GÖREVDE YÜKSELME YAZILI SINAVI

12. GRUP ŞUBE MÜDÜRÜ (BİLGİ TEKNOLOJİLERİ) DERS NOTU

DEVLET HAVA MEYDANLARI İŞLETMESİ
GENEL MÜDÜRLÜĞÜ

İÇİNDEKİLER

1. BİLGİ TEKNOLOJİLERİ DAİRESİ BAŞKANLIĞI GÖREV FAALİYETLERİ

- İhtiyaç duyulan Bilgi İşlem Sistemlerinin Planlanması, Projelendirilmesi, Teknik şartnamelerinin hazırlanması temin edilmesi,
- Hizmette olan sistemlerin periyodik bakım, onarım planlarının hazırlanması, uygulanmasının sağlanması ve gerekli durumlarda sistem analizlerini yapmak veya yaptırmak üzere takibi.
- Hizmette olan Bilgi İşlem Sistemlerinin programlarının hazırlanması veya hazırlattırılması, ihtiyaç duyulan program ilave ve değişiklerinin yapılması veya yaptırılması,
- İhtiyaç duyulan yedek malzeme, test cihazlarının ve dokümanların temini hizmette olan sistemlerde çıkabilecek arızaların anında giderilebilmesi için gerekli tedbirlerin alınması,
- Bilgi İşlem Sistemleri ile ilgili uluslararası kuruluşların ve Networklerin çalışmalarını yakından takip etmek, hazırlanan ve kabul edilen planlarının zamanında yerine getirilebilmesi için ilgili birimlerle gerekli koordine ve işbirliğinin sağlanması, gerekli plan ve programların yapılması,
- Hizmetleri ile ilgili personelin gerek Yurtiçi, gerekse Yurtdışı Eğitim planlarının yapılması ve uygulanması,
- Hizmetlerinin daha iyi yürütülebilmesi için teknolojideki gelişmelerin yakından takip edilmesi ve bu gelişmelerin bünyeye uygulanmasının sağlanmasından yükümlüdür.
- Bilgi Teknolojileri Dairesi, Kuruluşumuzun bilgisayar teknolojisi ve kullanımı konusunda destek hizmeti yürüten bir birimidir. Esas olarak Yazılım Geliştirme, Bilgi Sistemleri Destek, Sistem ve İletişim, Bilişim Güvenliği, Bilgi Güvenliği Risk Yönetimi Şube Müdürlükleri olacak şekilde yapılanmıştır.
- Yazılım Geliştirme Şube Müdürlüğü, Kuruluşumuzun ihtiyaç duyduğu programların hazırlanması veya hazırlattırılması, ihtiyaca göre mevcut programlar üzerinde değişiklikler yapılması ya da yaptırılmasını, Database kurulumu yönetimi, Kuruluşumuz Web Sayfası ile Kurumsal Portalın yapılması ya da yaptırılmasını sağlamaktadır.
- Bilgi Sistemleri Destek Şube Müdürlüğü, Bilgisayar Sistemi ve Çevre donanımları Teknik Şartnamelerinin hazırlanması, temini kabul ve tahsis işlemleri, BT son kullanıcı sistem/cihaz ve yazılımları teknik kurulumlarının yapılması/yaptırılmasının sağlanması, Kullanıcıların karşılaştığı teknik alt yapı ile ilgili sorunlara destek sağlanması, meydana gelen arızalara müdahale edilmesi, son kullanıcı cihazlarının periyodik bakım ve temizleme işlerinin

yapılması/yaptırılması, BT cihazlarının Envanter kayıtları, Sigorta, garanti, benzeri hizmetlerinin yürütür.

- Sistem ve İletişim Şube Müdürlüğü ise DHMİ Merkez ve Taşra Birimleri ile bu birimlerde çalışan kullanıcıların Bilgi Teknolojileri Dairesi Sistem Merkezine bağlantısının sağlanması, bu bağlantılarda şifreleme ve güvenlik tedbirlerinin sürekli ayakta tutulması, BT hizmetlerinin verilebilmesi için gerekli sunucu/donanım alt yapısının ve işletim sistemlerinin yönetilmesi, bakım ve onarım ve idamelerinin yapılması, gelişen bilgisayar ağları teknolojilerinin yakından takip edilmesi ve uygun olanlarının Kuruluşumuza kazandırılması konularının iş ve işlemlerini yapar.
- Bilişim Güvenliği Şube Müdürlüğü, Kuruluşumuz güvenlik sistemlerinin (güvenlik sunucu donanımları, güvenlik sunucu işletim sistemleri ve yazılımları, güvenlik aktif ağ cihazları, güvenlik ağ ve sunucu kalibrasyon cihazları, güvenlik izleme cihazları vb.) temini, tesisi, tahsisi, bakım ve onarımının yapılması/yaptırılması, sistemler üzerindeki kurumsal bilgi güvenliği politikalarının oluşturulması ve buna ilişkin planlama, işletim, yönetim ve denetleme çalışmalarının yapılması/yaptırılması, her türlü zararlı yazılımlara ve siber saldırılara önlem olarak merkezden yönetilen güvenlik yazılımlarının/donanımlarının kullanılması ve güncellenmesi, sistemler üzerindeki güvenlik zafiyetlerinin tespitine yönelik güvenlik testleri ve araştırmalarının yapılması/yaptırılması, yazılım ve donanımlar ile ilgili olarak her türlü erişim, sorgulama ve kayıt değişikliği loglarının (kayıt izleri) 5651 sayılı kanun hükümleri doğrultusunda tutulması, Kuruluşumuz siber ortamlarına doğrudan ya da dolaylı olarak yapılan veya yapılması muhtemel siber saldırılara karşı gerekli önlemleri almak üzere, Ulusal Siber Olaylara Müdahale Merkezi(USOM) ve Sektörel Siber Olaylara Müdahale Ekibince (Sektörel SOME) ve Kurumsal Siber Olaylara Müdahale Ekibinin (SOME) oluşturulması, aktif, etkin ve sürekli bir şekilde çalışmasının sağlanması, Kuruluşumuzun bilgi varlıklarını, içerden veya dışarıdan gelebilecek bütün tehditlere karşı korumak amacı ile Bilgi Güvenliği Yönetim Sisteminin (BGYS) kurulması ve çalıştırılması, Güvenlik Duvarı (Firewall) politikalarının belirlenmesi ve yönetiminin yapılması hizmetlerini yürütür.
- Bilgi Güvenliği Risk Yönetimi Şube Müdürlüğü, Kuruluşumuzun KamuNet ağına bağlanmasına ilişkin yer alan asgari gereksinimleri karşılama ve kayıt altına alma, KamuNet'e bağlantı yapacak birimleri ve sistemlerini kapsayacak BGYS'sini kurma ve işletme, Kurmuş olduğu BGYS için, TS ISO/IEC 27001 veya ISO/IEC 27001 standardına göre belgesini alma ve güncelliğini sağlama, 2019/12 sayılı Cumhurbaşkanlığı Genelgesi ve Dijital Dönüşüm Ofisi

tarafından yayınlanan “Bilgi ve İletişim Güvenliği Rehberi” talimatlarına uyma/uyulmasını sağlama, Bilgi teknolojilerine ilişkin risk yönetim kültürünün oluşturulmasını sağlayacak politika ve prosedürleri belirleme, Kuruluşumuzun çalışanlarının belirlenen bilgi güvenliği politikaları çerçevesinde bilinçlendirilmesi için çalışmalar yapma hizmetlerini yürütür.

- Bilgi Teknolojileri Dairesi Başkanlığı, Genel Müdürlüğümüz amaç ve hedeflerine uygun olarak, Genel Müdürlüğümüz ana statüsü ile yürürlükte bulunan yönetmelik ve mevzuatlara göre yürütülmekte olan işlerin; yeni teknolojiler kullanılarak her yönden hizmet kalitesinin yükseltilip, bunun paralelinde Kuruluş gelirini arttırmak ve Kuruluşumuzun gerek yurt içi, gerekse yurt dışında ilişkili olduğu Kurum ve Kuruluşlar ile sorunsuz bilgi alış verişi yapabilmesi amacı ile DHMİ Bilişim alt ve üst yapı modernizasyon çalışmalarını yürütür.

Bilgi Teknolojileri Dairesi Başkanlığının Destek Verdiği ve Geliştirdiği Projeler

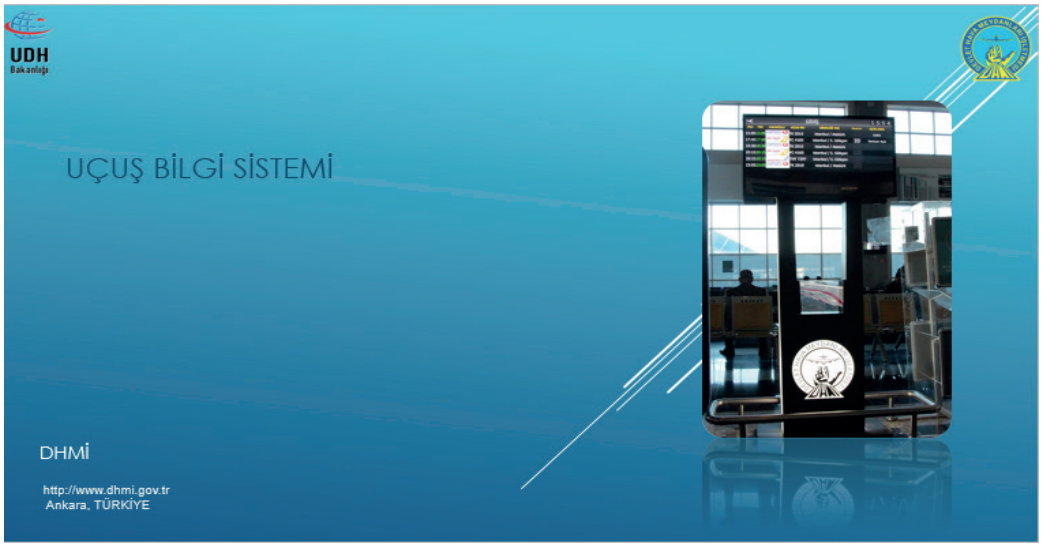
FIDS (Uçuş Bilgi Sistemi)

Bilgi Teknolojileri Dairesi Başkanlığı Yazılım Geliştirme Şube Müdürlüğü tarafından geliştirilen Uçuş Bilgi Sistemi Endüstriyel Monitörler aracılığı ile yolculara, karşılayıcılara, uğurlayıcılara ve yer hizmet birimlerine uçuş durum bilgilerini gerçek zamanlı olarak verebilmek için kullanılan görsel bir yazılım sistemidir. Bu sistemde kullanılan monitörler 7/24 gün/saat çalışma koşullarına uygun olarak tasarlanmaktadır ayrıca dış mekânlar için kullanılan monitörlerde nem ve sıcaklık şartlarına dayanaklı ve IP koruma sınıfı kabin ve monitörler tercih edilmektedir. Kullanım yerleri aşağıdaki gibidir.

- **Check-in Banko Monitörleri:** Tipik olarak 32 inç boyutunda ve check-in bankosun yer alan firmanın check-in işlemi yapılan uçuşuna ait bilgiler yer almaktadır.
- **Giden Yolcu Salonu Monitörleri:** Tipik olarak 40 ve 46 inç boyutlarında yatay ve dikey olarak konumlandırılan İç veya Dış Hat yakın zamanda uçuş gerçekleşmiş ve gerçekleşecek uçuş bilgilerini göstermektedir.
- **Arındırılmış Salon Monitörü (Gate):** Tipik olarak 32 ve 40 inç boyutlarında yatay ve dikey olarak konumlandırılan gidilecek olan uçuşun bilgileri ile kapı bilgisi yer almaktadır.
- **Bagaj Alım Monitörü:** Tipik olarak 32” boyutunda gelen yolcuların bagajlarının hangi konveyörden alacağına dair bilgilerin yer aldığı monitörlerdir.
- **Şut Bölgesi Monitörü:** Tipik olarak 32” boyutunda ve dış mekân koşullarına uygun hangi bagajın hangi konveyörden verileceği bilgisi olan monitörlerdir.

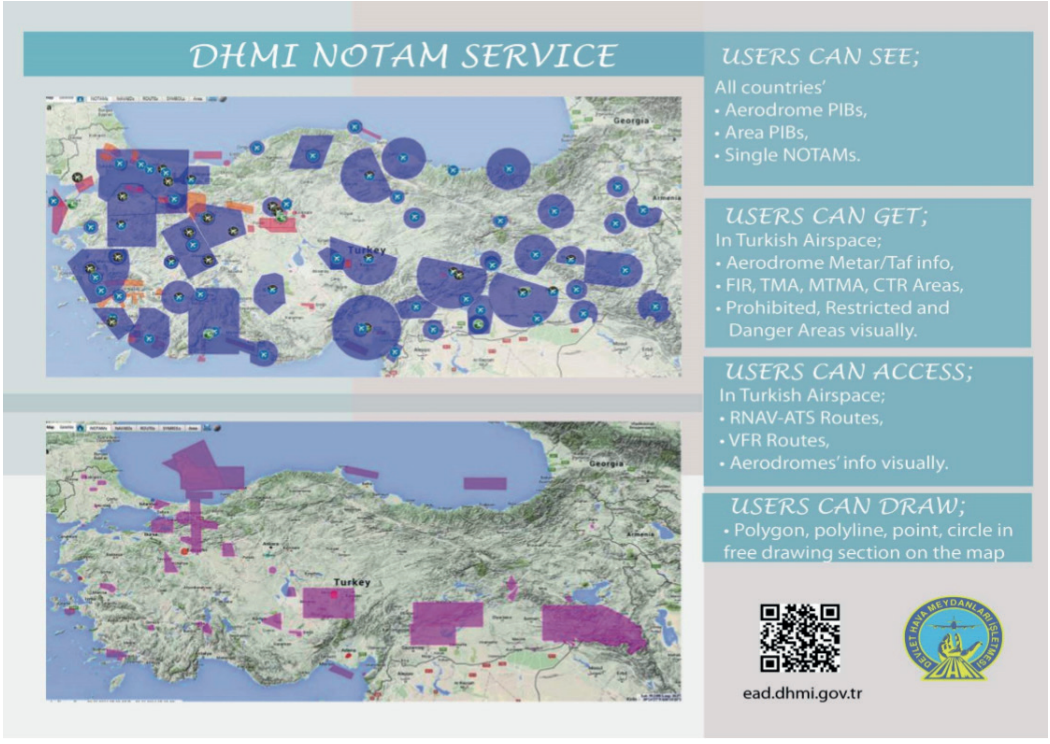
- **Dış Mekân Monitörü:** Tipik olarak 40 ve 46 inç boyutlarında yatay ve dikey olarak konumlandırılan Dış Mekân koşullarına uygun İç veya Dış Hat yakın zamanda uçuşu gerçekleşmiş ve gerçekleşecek uçuş bilgilerini göstermektedir.

Uçuş Bilgi Sisteminin 2022 yılı Ocak ayı itibarı ile 40 Havalimanına kurulumu tamamlanmış olup, hali hazırda Uçuş Bilgi Sistemi kurulu olmayan diğer Havalimanlarına da kurulum planlamaları yapılmaktadır. Geliştirilen uygulama, teknolojisi itibarı ile şu an kullanılmakta olan birçok Uçuş Bilgilendirme Sisteminden daha üstün teknolojik özelliklere sahip olup Ulusal ve Uluslararası Teknoloji Fuarlarında da ülkemiz ve Devlet Hava Meydanları İşletmesi adına tanıtımı yapılmaktadır.



EAD-Notam Servisi

Başkanlığımız Yazılım Geliştirme Şube Müdürlüğünce geliştirilen en son uygulamada Hava Sahamız için yayınlanan NOTAM'ların EAD Sistemi üzerinden çekilerek Ülke Haritamız üzerinde ilgili alanları kapsayacak şekilde görsellik sunan DHMİ AIS Portal uygulamasıdır. Bu uygulamadan hem Kurum Personelimiz hem de Pilotlar yararlanmaktadır. Bu uygulama; geliştirmesi tamamlanan ve Web üzerinden Uçuş Planı doldurulmasına imkan verecek Uçuş Planı Portalı ile entegre edilmiştir.



Oracle Exalytics İş Zekâsı Sunucu ve Yazılımı

Bilgi Teknolojileri Dairesi Başkanlığı bünyesinde geliştirilen uygulamalar aracılığı ile dijital ortamda biriken Kurumsal verilerimizin yorumlanabilir bilgiye dönüştürülmesi ve veri görselleştirilmesi için Veri Madenciliği ve İş Zekâsı Platformu kurulmuştur.

Veri Madenciliği ve İş Zekâsı Platformu üzerinde İş Zekası, Forecast (Tahminleme), Predictive (Ön Görü) ve Analitik raporlar hazırlanabilmekte ve hazırlanan raporlar Veri Madenciliği Portalı üzerinden yayınlanarak özellikle Birim Yöneticileri ve Üst Yönetimin sağlıklı ve hızlı karar alabilmesi sağlanabilmektedir.

Kuruluşumuz Web Siteleri

Kuruluşumuz WEB sitelerinin sürekli olarak faal tutulması, WEB Sitelerimizin kapsamının genişletilmesi, güncel tasarım kriterlerine uygun ve yeni nesil teknolojilerle uyumlu güçlü bir içerik yönetimi sağlanmaktadır.

Eğitim Portalı

Havacılık Eğitim Dairesi Başkanlığımızın DHMİ-Akademi seviyesinde; Personelimiz ile Sektör Çalışanlarına yönelik eğitim hizmetlerini çağdaş ve her noktadan erişebilir bir Eğitim Portali Uygulaması ile yapabilmesini teminen proje hazırlanmıştır. Hazırlanan proje kapsamında Uygulama ile Kurs Planlaması ve Duyuruları ile Kursiyer ve Eğitmen talepleri toplanarak takibi yapılabilecek, ilaveten uzaktan eğitim, Sanal POS ile ücret tahsilatı yapılabilecektir.

E-Arşiv Projesi (Kurum Arşivinin Dijitalleştirilmesi)

Arşivler Kurumların ve Devletlerin hafızalarıdır. Arşivlerin zarar görmesi halinde bu hafızanın yitirilmesi sonucu ortaya çıkar. Hem bu yaklaşımla Hafızamızı koruma altına almak hem de kolay ve hızlı bir erişim sağlanmak amacı ile Kuruluşumuz arşivinin (Belge, Doküman, Harita, Pafta, Kitap, Resim, vb.) dijitalleştirilmesi çalışmalarına başlanmıştır. Bu çalışma kapsamında Dijital Arşiv Yönetim Sistemi tesis edilerek Kuruluşumuz Elektronik Belge Yönetim Sistemi ile entegrasyonu sağlanacaktır. Türk Hava Sahası EN-ROUTE ve lokalinde gerçekleşen uçuş bilgilerinin EUROCONTROL CRCO (Centeral Route Charge Office) 'ya bildiriminin yapılabilmesi için ihtiyaç duyulan yazılımların geliştirilmesi Yazılım Geliştirme Şube Müdürlüğün tarafından yapılmıştır. Bu Uygulama ile EUROCONTROL CRCO 'ya bildirilmek üzere toplanan tüm uçuş bilgilerinin DEBI (Data Exchange By Internet) bağlantısı kullanılarak gönderilebilmesi yapılmaktadır.

Ayrıca;

- EUROCONTROL nezdinde ülkemizin uçuş birim fiyatının tespiti için oluşturulan Milli

Maliyet veri tabanına yansımak üzere Kuruluşumuzun yapmış olduğu yatırım ve harcama bilgilerinin toplanması ve EUROCONTROL Müdürlüğüne bildirilmesi için ihtiyaç duyulan yazılımların geliştirilmesi Yazılım Geliştirme Şube Müdürlüğü tarafından yapılmıştır.

- AIT yazılımı kullanılarak AFTN mesajlaşma trafiği Genel Müdürlüğümüz ve muhtelif taşra teşkilatlarında Bilgi Teknolojileri Dairesi Başkanlığı tarafından temin ve tesis ettiği veri iletişim alt yapıları yapılmaktadır.

- Ülkemizin sivil uçuşa açık hava sahasında uçuş güvenliğinin emniyetini artırmak amacıyla geliştirilen SMART projesinin ihtiyaç duyduğu operasyonel veri iletişim alt yapısının projelendirme çalışmaları Bilgi Teknolojileri Dairesi Başkanlığı tarafından yapılmaktadır.
- Sivil uçuşa açık hava sahasının güvenliği açısından öncelikli konulardan biri hava ve meydan **SLOT** tahsislerinin yapılması ve izlenmesi konusudur. Bununla ilgili **Slot Koordinasyon Merkezi, Sivil Havacılık Genel Müdürlüğü ve Radar FDP'nin** entegre olduğu uygulama Yazılım Geliştirme Şube Müdürlüğü tarafından yapılmıştır.
- **Hava Seyrüsefer Dairesi Başkanlığı Muhabere** birimi tarafından Kuruluşumuz adına kiralanan Telekom hatlarının takibi sağlamak amacıyla ihtiyaç duyulan yazılım, donanım ve iletişim alt yapısının temini, tesisi ve idamesi,
- **Hava Trafik Kontrolörlerinin** tüm lisans ve personel hareketlerinin takibi amacıyla ihtiyaç duyulan yazılım, donanım ve iletişim alt yapısının temini, tesisi ve idamesi,
- Türk Hava Sahasının güvenliği için ülkemizin muhtelif bölgelerinde kurulu bulunan **seyrüsefer yardımcı sistemlerinin (VOR, DME, NDB) uzaktan izlenmesi ve yönetimi** için ihtiyaç duyulan yazılım, donanım ve iletişim alt yapısının temini, tesisi çalışmaları,
- Ülke çapında Kuruluşumuzun tüm üniteleri arasında sesli ve görüntülü olarak iletişimine olanak sağlayacak **IP Telephony/VOIP (Voice Over IP)** iletişim alt yapısının oluşturulması çalışması,

Personel(İnsan Kaynakları) Projesi

- İzin, İstirahat, Rapor, Mükâfat ve Mücazat İşlemleri,
- Tayin ve Terfi İşlemleri,
- Sicil İşlemleri,
- Tahakkuk ve Harcırah İşlemleri

Muhasebe ve Envanter projesi

- Meydan muhasebesi
- Merkez muhasebesi
  - Yurt içi, yurt dışı Gelir-Gider takibi
  - Ödenek işlemleri
  - Bilanço
  - Mizan
  - Bütçe
  - Envanter işlemleri

Malzeme ve Stok Takip Projesi

- Malzeme-Stok Takibi
- Depo İşlemleri
- Demirbaş ve hurdalık takip işlemleri
- İhale İşlemleri
- Sigorta İşlemleri
- Ödenek Tahakkuk İşlemleri
- İstatistiki Bilgi Alma İşlemleri

Hizmet ve Gelirler Projesi

- Uçuş Kayıtlarının sisteme girilmesi ve güncellenmesi,
- Permi ve Slot takibi,
- Yer Hizmetlerinin uçuş kayıtlarına güncellenmesi,
- Uçak Hizmetleri, Terminal Hizmetleri ve Sözleşmeli İşler Tahakkuk ve Faturalarının alınması,
- Uçuş istatistiklerinin alınması,
- Elektronik olarak Kule, Apron ve Köprü raporlarının alınması

Sosyal İşler Projesi

- Kamp
- Lojman
- Tabldot
- Misafirhane
- Kütüphane
- Kurslar
- Sağlık

Yönetim Bilgi Sistemi Projesi

Mevcut yazılım projelerinde oluşan bilgi özetlerinin üst yönetimce izlenmesi ve takip edilmesi

Evrak Otomasyon Sistemi Projesi

Kuruluşumuz Evrak Akışının Elektronik ortamda yapılması amacı ile geliştirilmiştir.

CUTE/BRS SİSTEMİ

CUTE Sistemi (Common Use Terminal Equipment)

CUTE Sistemi havayolu şirketlerinin kullandıkları DCS sisteminin havalimanının ortak kullanılan alanlarında bulunan sistemleri (Bilgisayar, Printer, Bagaj etiketi yazıcı, Bilet Yazıcı vb) ortak olarak kullanmalarına imkân verir. Aynı zaman da kısıtlı bulunan Check-in kontuarlarının ve Gate'lerin optimum şekilde kullanılmasını sağlar. Bu sayede Check-in kontuarları havayollarına daimi tahsis yerine saatlik olarak da tahsis edilebilir. Yani CUTE sistemi olmamış olsa idi her havayolu şirketine daimi bir check-in kontuarı tahsis etmek gerekecek, her havayolu da hem bilgisayar ve çevre donanımlarını ve de network altyapısını ayrı ayrı kurmak durumunda kalacak buda havalimanında altyapı kirliliğine neden olacaktır.

Günümüzde Dünyada yaygın olarak havalimanlarında; **SITA, RESA, ARINC, ULTRA, AMADEUS** firmalarına ait CUTE/CUPPS sistemleri kullanılmakta olup, Ülkemizdeki havalimanlarında ise **SITA, RESA**, **BRIDGE ve TRAVSYS** firmalarına ait CUTE/CUPPS Sistemleri kullanılmaktadır.

BRS (Baggage Reconciliation System) Bagaj Eşleştirme Sistemi

Bagaj eşleştirme sistemi öncelikli olarak ICAO'nun sahipsiz bagajın taşınmaması kuralını uygulayabilmek için kullanılan sistemdir. Sistem aynı zamanda;

- Doğru bagajın doğru uçuşta ve sahibinin de aynı uçuşta olduğunu garantilemek,
- Uçağa binmeyen yolcu olduğunda yolcuya ait bagajın belirlenip indirilmesini sağlamak,
- Bagaj operasyonunu havalimanı dâhilinde ve birden çok havalimanı boyunca sağlamak
- Gerçek zamanlı bagaj yönetim çözümü sağlamaktadır.
- BRS sistemi kullanımı sayesinde;
- Yolcu ve bagajlarının beraber yolculuk etmesi sağlanarak güvenlik arttırılır,
- Bagaj yükleme/yönlendirme hatalarının azaltılması ve ihtiyaç duyulduğunda gerçek zamanlı bilgi sağlanabilmesi ile müşteri servis kalitesi arttırılır,

2. BİLGİSAYAR DONANIMI VE İŞLETİM SİSTEMLERİ

Bilgisayar; kendine önceden yüklenmiş program gereğince çeşitli bilgileri-verileri uygun ortamlarda saklayan ve istenildiğinde geri getiren, çeşitli aritmetik ve mantıksal işlemler yapan; çok hızlı çalışan elektronik bir cihazdır. Bilgisayarın elektronik kısmına donanım (hardware), program kısmına ise yazılım (software) denir.

Bilgisayarın gelişiminde şu 4 unsur hiç değişmemiştir.

1. Bilginin Girişi (Giriş birimleri: Klavye, Mouse, Kamera, Scanner, Fax-Modem vb.)
2. Bilginin saklanması (Hafıza: Hard disk, disket, cd-rom vb.)
3. Bilginin işlenmesi (Beyin: Merkezi işlem birimi-Central Processing Unit-CPU)
4. Bilginin çıkışı (Çıkış birimleri: Monitör/ekran, Printer/yazıcı, plotter/çizici, modem)

Donanım bilgisayarı oluşturan her türlü fiziksel parçaya verilen addır. Donanım bir merkezi işlem biriminden (Central Processing Unit-CPU) ve bu birime bağlı çevre birimlerinden oluşur. Çevre birimleri de ayrıca giriş birimleri (input devices) ve çıkış birimleri (output devices) olmak üzere iki kısma ayrılır.

Bir bilgisayar; Anakart (Motherboard), Merkezi İşlem Birimi (CPU), Bellek (RAM), Sabit Disk (Hard Disk), Donanım Kartları (Ekran Kartı, Ses Kartı, Ethernet Kartı vb.), Monitör, Kasa, Klavye, Mouse vb. bileşenlerden meydana gelir.

Anakart (Mainboard) : Anakart, bir bilgisayarın tüm parçalarını üzerinde barındıran ve bu parçaların iletişimini sağlayan elektronik devredir. Bir bilgisayarın temel devre kartıdır. Bilgisayardaki tüm elektriksel bileşenler ana karta bağlanmıştır.

Bir anakart; Yonga Seti (Chipset), Veri Yolları (BUS), İşlemci Yuvası, Bellek Yuvaları, Genişleme Yuvaları, Güç Kaynağı (Power Supply), Bios ve Bios Pili ve Giriş/Çıkış Portlarından meydana gelmektedir.

Merkezi İşlem Birimi (CPU) : Merkezi işlem birimi (CPU - Central Processing Unit), bilgisayarın en önemli parçasıdır. Mikro işlemci diye de anılır. Komutları işler, hesaplamaları yapar, bilgisayarın içindeki bilgi akışını kontrol eder ve yönetir. CPU, kullanıcı tarafından verilen komutları yorumlar, komutlara uygun programları çalıştırır ve isteklerimizi yerine getirir.

Ana Bellek (RAM) : Ana bellek veya rastgele erişimli bellek (Random Access Memory-RAM), bir giriş cihazından veya bir ikincil depolama cihazından okunan veri ve programların, çalıştırılan programlardan elde edilen sonuçların ve bir ikincil depolama cihazına veya bir çıkış cihazına gönderilmeye hazır olan çıktıların tutulduğu yerdir. DRAM, SRAM, SDRAM, DDRRAM, DRDRAM, PSRAM, RLDRAM, SGRAM gibi Ana Bellek (RAM) türleri mevcuttur.

BIOS (Basic Input Output System) : BIOS yongası (entegresi), bilgisayarın açılışı sırasında parçaları kontrol eden ve onları çalışmaya hazır duruma getiren bir program içerir. ROM (Read Only Memory) türündeki bellek üzerinde kaydedilmiş bir programdır. Bu tür bellekteki bilgiler bilgisayarı kapattığınızda silinmez.

Sabit Disk (Harddisk) : Bilgiler bilgisayarın belleğinde işlenip değerlendirilmektedir. Bilgisayarın kapatılması veya elektriğin kesilmesi halinde bellekteki bilgiler silinmektedir. Bellekte geçici olarak saklanan bilgileri kalıcı olarak saklamak için bilgilerin manyetik bir ortama aktarılması gerekir. En çok kullanılan manyetik ortamların başında ise hard disk gelmektedir. Hard (sabit) disk sürücü bir bilgisayarın bilgi depolamak için kullandığı en temel birimdir. Veriler bir dizi dönen diskte manyetik olarak saklanır(Kaydedilen bilgiler Dosya adını alır).

Çevre Birimleri : Bilgisayara bağlı olan fakat bir kasa içerisinde yer almayan ama daha sonra çeşitli portlar yardımıyla bağlanan donanımlara Çevre Birimleri denir. Başlıca çevre birimleri şunlardır:

Ekran (Monitör), Klavye (Keyboard), Fare (Mouse), Yazıcı (Printer), Çizici (Plotter), Tarayıcı (Scanner), Modem :

Koruyucu Bakım

Herhangi bir koruyucu bakım programının amacı, pahalı bilgisayar, Switch, Sunucu vb. onarımlarının önüne geçmektir.

Koruyucu bakım, sistemler zarar görmeden önce alınacak önlemleri içerir. Bu önlem ve tedbirleri aşağıdaki gibi sıralayabiliriz:

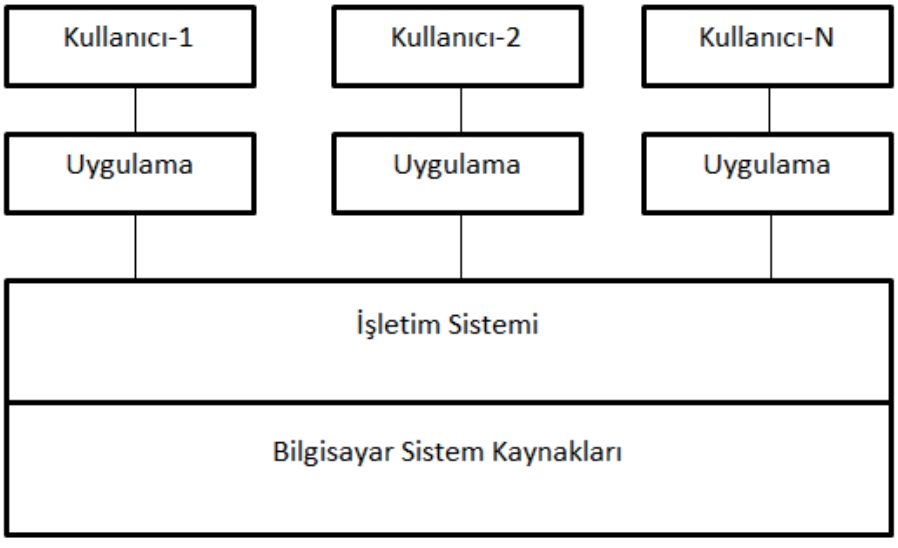
1. Sunucu odası ve bilgisayar laboratuvarının fiziksel olarak güvenlik önlemleri alınmalıdır.
2. Yetkisiz ve sorumlu olmayan kişilerin girişine izin verilmemelidir.
3. Ortam sürekli temiz ve bakımlı tutulmalıdır.
4. Çevresel yönergeler, anlatılacak olan ortam ile ilgili hususlara dikkat edilmelidir.
5. Bakım zaman çizelgesinde belirlenen zamanlarda donanımların ve yazılımların bakımı yapılmalıdır.

6. Bilgisayar çevre birimlerinin bakım ve kontrolü yapılmalıdır.
7. Sistemlerde bulunan aygıtların kendi sürücüleri yüklenmeli ve güncel tutulmalıdır.
8. Sistemlere gereksiz yazılımların yüklenmemesi için tedbirler alınmalıdır.
9. Lisanssız yazılımların kullanılması önlenmelidir.
10. Güncel olmayan yazılımlar sistemden kaldırılmalıdır.
11. Sistemler sürekli virüs taramasından geçirilmelidir.
12. Virüs programı güncel tutulmalıdır.
13. Sistemde bulunan önemli verilerin yedeği periyodik olarak alınmalıdır.

İŞLETİM SİSTEMLERİ

İşletim Sistemi Nedir?

Bilgisayarlarda işletim sistemi, donanımın doğrudan denetimi ve yönetiminden, temel sistem işlemlerinden ve uygulama programlarını çalıştırmaktan sorumlu olan sistem yazılımıdır. En yaygın olarak kullanılan işletim sistemleri iki ana grupta toplanabilir: Microsoft Windows grubu ve UNIX benzeri işletim sistemlerini içeren grup (bu grup içinde pek çok Unix versiyonu, Linux ve Mac OS sayılabilir). İşletim sistemi, bütün diğer yazılımların belleğe, girdi/çıktı aygıtlarına ve dosya sistemine erişimini sağlar. Birden çok program aynı anda çalışıyorsa, işletim sistemi her programa yeterli sistem kaynağını ayırmaktan ve birbirleri ile çakışmamalarını sağlamaktan da sorumludur.



İşletim Sistemlerinin Temel İşlevleri

1. “Kullanıcı arabirimi” tanımlamak,
2. Sistem açılışını sağlamak,
3. Donanımı, kullanıcılar arasında paylaştırmak,
4. Kullanıcıların verileri paylaşmasını sağlamak,
5. Giriş / çıkış işlemlerini gerçekleştirmek,
6. Hataları düzeltmek,
7. Programlama arabirimi(API: Application Program Interface) sağlamak.

Bir İşletim Sisteminin Bileşenleri

Bir işletim sistemi, kavramsal olarak, üç grupta toplanabilecek bileşenlerden oluşur: kullanıcı arayüzü (bu bir grafik kullanıcı arayüzü ve/veya komut satırı yorumlayıcısı ["kabuk" da denir] olabilir), dosya yönetim sistemi ve bir çekirdek.

Kullanıcı Arabirimi

Genel olarak arayüz, herhangi bir şeyin kullanımını ya da onda etkileşimi sağlayan kısım olarak düşünebilirsiniz Bir araba, gaz ve fren pedalları ile aracı yönlendirmeyi sağlayan direksiyonu da içeren daha karmaşık bir arayüze sahiptir. Bir bilgisayarın arayüzü klavye ve fare ile monitörde gözüken ve bilgisayarı birçok farklı iş için kullanabilmemizi sağlayan yazılımlardan oluşur. Macintosh bilgisayarların çıkışı ve ardından Microsoft’un Windows yazılımının geliştirilmesinden beri birçok insan, arayüz dendiğinde otomatik olarak grafiksel kullanıcı

arayüzünü (GUI –Graphic User Interface, grafik kullanıcı arayüzü-) düşünmektedirler. Bilgisayar kullanımını daha kolay hale getirmede görsel nesneler kullanımı gittikçe gelişiyor olsa da bu nesneler bilgisayar ve kullanıcı arasında etkileşimi sağlayan seçenekler topluluğunun sadece bir parçasıdır.

Çekirdek

Çekirdek, diskteki dosyaların izlerini tutar, programları başlatır ve yürütür, belleği ve çeşitli süreçlerin kaynaklarını düzenler, ağdan paketleri alır ve gönderir, vb... Çekirdek kendi başına çok az iş yapar, fakat diğer servislerin kullanabileceği araçları sağlar. Ayrıca donanımlara doğrudan ulaşan kişileri önleyerek, onları kendi sunduğu araçları kullanmaya zorlar. Bu yolla çekirdek, kullanıcıları diğer kullanıcılara karşı koruyacak bir yol izler. Çekirdek tarafından sağlanan bu araçlar sistem çağrıları üzerinden kullanılır. Sistem programları işletim sisteminin ihtiyacı olan çeşitli servisleri yerine getirmek için çekirdek tarafından sağlanan bu araçları kullanırlar. Çekirdek, işletim sisteminin kalbidir. Adından da anlaşılabileceği gibi, "kabuk", çekirdeğin çevresini sararken, donanımla iletişim kurmak da çekirdeğin işidir.

İşletim Sisteminin İşlevleri

Dosya ve Klasör Yönetimi

Dosyaları ve klasörleri yönetme, kaynakları saklama ve güvenliğini sağlamayı, bu kaynakları ağ kullanıcılarının kullanımına sunmayı ve yine bu kaynaklardaki değişiklikleri yönetmeyi içerir.

Bilgisayarda bulunan işletim sistemleri, tüm programlar, oyunlar, bizim hazırladığımız belgeler dosyalar halinde saklanır. Bu dosyalar bilgisayarımızda harddisk adını verdiğimiz fiziksel bir aygıtta saklanır ve bu dosyaları kendi aralarında gruplamak içinde klasörler kullanılır. Yani verilerin bir arada tutulduğu ortamlara dosya denir.

Sürücü: Dosya ve klasörlerin saklanabileceği fiziksel ortamlardır ve alfabede bulunan harfler ile temsil edilirler. Disket sürücüler A veya B harfi ile Harddiskler ise C ve sonrasında gelen harfler ile temsil edilirler. CD-ROM, DVD-ROM ve Tape Backup üniteleri vb. diğer aygıtlar ise Harddiskten sonra gelen harfler ile temsil edilirler.

Klasör: Sürücüler içerisinde bulunan ve dosyaları gruplamak amacı ile kullanılan program grup isimleridir. Klasörler dosyaları yaptıkları işlere göre gruplandırırlar, bu sayede aradığımız herhangi bir dosyayı bulmamız kolaylaşır.

Dosya: Bilgisayarda yaptığımız her işlem dosyalar aracılığı ile yapılmaktadır. Bir oyun oynayacaksak onun için gerekli dosyalar ekran görüntüleri dosyalarda saklanır. Kullandığımız bir muhasebe programında girdiğimiz faturalar, çekler, senetler ilgili dosyalara kaydedilir.

Yazdığımız belgeler, hesap tabloları, sunular vb. dosyalarda saklanır. Bu sayede yaptığımız çalışmaları istediğimiz herhangi bir zamanda açıp okuyabilir gerekli güncellemeleri yapabiliriz. Bilgisayarda bulunan bütün dosyalar "dosyaadı.uzantı" şeklinde saklanır. Dosyaadı o dosyanın yaptığı işe göre verilmiş mantıksal bir isimdir ve toplam 255 karakter uzunluğunda olabilir, uzantı ise o dosyanın işlevine göre bilgisayar tarafından daha önceden belirlenmiş bir isim olabilir ve genelde 3 harf uzunluğundadır. Uzantılar sayesinde o dosyanın hangi programla hazırlandığını ve hangi programlarla açılabileceğini anlayabiliriz.

Uzantı	Açıklama
Exe	Uygulama dosyaları
Bat	Toplu iş dosyaları
Txt	Metin dosyaları
Bmp	Resim dosyaları
Jpg	Resim dosyaları
Doc	Microsoft Word dosyaları
Xls	Microsoft Excel dosyaları
Ppt	Microsoft Powerpoint dosyaları
Zip	Sıkıştırılmış dosyalar

Dosya Uzantıları

Uygulamaların Yönetimi

Kullanıcı bir program çalıştırmak istediğinde, işletim sistemi uygulamanın yerini sabit diskten tespit eder ve uygulamayı RAM'e yükler. Bu işlem etkileşimli işlem olarak adlandırılır. Etkileşimli işlem kullanıcılara, uygulamaları dinamik biçimde yönetme, çalıştırılan programların sonuçlarını doğrudan elde edip, her an müdahale edebilme olanağı sağlayan çalışma türüne ilişkin bir özelliktir. Bu çalışma türünde kullanıcılar, bir işin çalışma süreci boyunca işe, monitör ve klavye vasıtası ile her an müdahale edebilmektedirler. Yani bir başka söylemle, ekran başında oturan bir kullanıcının bilgisayara bir komut vermesi ve o komuta bilgisayardan yanıt alması türünde, bir nevi karşılıklı konuşma yapar gibi çalışma biçimine "Etkileşimli İşlem" denir. Bu tanımdan da anlaşılacağı gibi, kullanıcılar program geliştirme, metin dosyaları oluşturma, program derleme ve test etme, veri tabanı sorguları işletme, bilgisayar ağı komutları girme, internet servislerini kullanma gibi kısa süreli işlerini Etkileşimli İşlem olarak yürütürler.

Yardımcı Programları Destekleme

İşletim sistemi yardımcı programları, problemleri giderebilmek ve sisteminin sağlıklı işlemesini sürdürebilmek amaçlı kullanır. Silinmiş, hasarlı dosyaları bulabilmek, verilerin yedeğini

alabilmek gibi işlemlerde kullanır. İşletim sistemi, üzerinde yer alan bazı yazılımlar "Sistem Yazılımı" olarak anılır. Örneğin derleyiciler (compilers) ; yazdığımız programı makine diline çeviren ara program, editörler (editors), yararlı programlar (utility) ; virüs temizleyen programlar gibi gerçek iş için yardımcılardır, veri tabanı yönetim sistemleri (database management system) ve bilgisayar ağı yazılımları (network software) yine birer sistem yazılımlarıdır. Ancak bu yazılımlar işletim sisteminin kendi öz parçaları değildir.

İşletim Sistemi Tipleri

Çoklu Kullanıcı (Multiuser) İşletim Sistemleri

İki veya daha fazla kullanıcının programlar veya paylaşılan aygıtlar üzerinde çalışabilmesidir. Bu konuya en güzel örnek paylaştırılan yazıcılardır. Birçok kullanıcı aynı anda yazıcıya belge gönderir ve de sıra ile bu belgeler yazıcıdan çıktı alınır.

Çoklu İşlem (Multiasking) İşletim Sistemleri

Kullanıcılar sistemde aynı anda birden fazla işlem (process) çalıştırabilirler. Bu, siz bir işlemi başlattıktan sonra, o başlattığınız işlem çalışmaya devam ederken başka bir işlem de başlatabilirsiniz demektir. Çoklu görev, bir işletim sisteminde bir kullanıcının, birden fazla sayıda işlemi aynı anda işletime alınabilmesi özelliğidir. Yani çoklu görev, bellekteki birkaç veriyi aynı anda işlemesi ve işlemci ile I/O ünitelerinin de bunlar arasında aynı anda kullandırılması ortamının yaratılmasıdır. Ancak bir bilgisayar sisteminde, işletim sisteminin kendisine ait birden fazla işlemin aynı anda çalıştırılması, bu sistemde "çoklu görev (multitasking)" özelliği olduğunu göstermez. Bu nedenle bir işletim sisteminde çoklu görev özelliği, ancak bir kullanıcının birden fazla sayıdaki işlemi aynı anda işletebiliyorsa vardır. Çoklu görev birçok uygulamanın (programın) aynı anda çalıştırılmasıdır. Bunun sağlanması için, görevler (uygulamalar) kısa zaman dilimleri içinde işlemcide çalıştırılır. Bu zaman dilimlerinin oldukça küçük zaman dilimleri olması nedeniyle yapay da olsa bir eş zamanlılık söz konusu olur. (İşlemci aynı anda iki işi yapamaz.)

Çoklu İşlemci (Multiprocessing) İşletim Sistemleri

Gittikçe yaygınlaşan bir durum da bir basit sistemin içerisine birçok CPU bağlayarak çok önemli hesaplamaları yapmaktır. Her işletim sistemi birden fazla işlemciyi destekleyemiyor. İşletim sistemi, yapılacak olan işlemleri iki veya daha fazla işlemci üzerine dağıtmayı bilmeli ve bunları kontrol edebilmelidir. Bu özelliğe sahip olan işletim sistemleri arasında Windows 2000,

Windows NT, Linux, Unix, BeOS bulunuyor. Microsoft'un diğer işletim sistemleri (Win9x - ME) çok işlemcili sistemleri desteklemiyor.

Çoklu Görev (Multithreading) İşletim Sistemleri

Program ihtiyaç halinde işletim sistemi tarafından küçük parçalara ayrılır ve çalıştırılabilir. Bu özellik aynı zamanda çoklu kullanıcı sistemleri de destekler. Aynı programın parçaları farklı kullanıcılar tarafından da kullanılabilir.

Windows Sunucu(Server) İşletim Sistemleri

- Windows NT
- Windows 2000
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2016

Disk Yapılandırılması (RAID)

Günümüzde bilgisayarlar yüksek işlem hızlarına ulaşmışlar ve bu hız artarak devam etmektedir. İşlem hızın öncelikle önemli olduğu durumlarda ise sabit disklerin önemi daha da artmaktadır. İşletim sistemleri, performansı artırmak için çeşitli araçlar sunuyor olsa da disklerin fiziksel sınırları vardır. Birkaç tane diski, eş zamanlı olarak kullanmak bu fiziksel sınırlamanın olumsuz etkilerini gidermek açısından oldukça önemlidir.

Temel olarak veri okuma ve yazma hızlarını artırmak ve güvenliği sağlamak amacıyla birden fazla diskin bir arada kullanılmasına RAID (Redundant Array of Indepented Disk Drives-Bağımsız Disklerin Artıklıklı Dizisi) adı verilmektedir. RAID oluşturulmasının amacı; hata toleransı sağlamak, daha fazla depolama alanı sağlamak ve performansı yükseltmektir. RAID denetçi kartları ile yapılandırılan RAID teknolojisine, “Donanımsal RAID” adı verilir. Artık son kullanıcılar da, işletim sistemleri ile birlikte gelen araçlar yardımıyla RAID teknolojilerini kullanabilmektedirler. Buna “Yazılımsal RAID” denir

HOT SPARE: RAID grubunun içerisinde bulunan ancak boşta yedek olarak bekleyen diske denir. RAID grubundaki bir disk arızalandığı zaman normal şartlarda diskin değiştirilmesi ve verinin tekrar yazılması beklenir. Ancak Hot Spare olması durumunda arızalanan disk yerine Hot Spare geçer ve veri bu diske yazılmaya başlar.

HOT SWAP: RAID grubundaki bir diskin arızalanması halinde sunucuyu kapatmadan disk değişiminin yapılması işlemine verilen isimdir.

DUPLEXİNG: İki RAID kartının yedekli çalışması işlemidir.

RAID ile ilgili olarak bilinmesi gereken bazı hususlar;

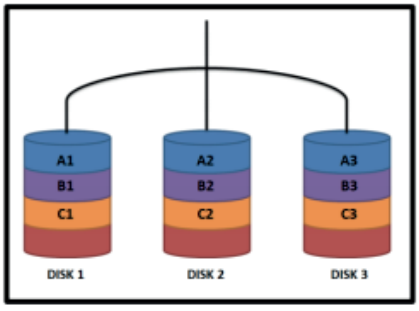
* RAID yapısında disklerin aynı RPM'de veya aynı boyutta olması gerekmiyor. Sunucunuzun desteklediği tüm diskleri kullanabilirsiniz. Ancak şunu bilmeniz gerekiyor RAID yapısında olan diskler içerisinde en düşük RPM'li ve en düşük kapasiteye sahip diskiniz hangisi ise RAID ona göre hareket eder. Yani 500 gb 7200RPM 1 disk ile 1 tb 15000 RPM 2 diskiniz olduğunu düşünün bu disklerden RAID 0 yaptığınız takdirde her diskin 500 gb kapasitesini kullanabilirsiniz. RAID yapısındaki tüm diskler ise 7200 RPM'miş gibi davranırlar.

* RAID Controller kartlarının arızalanması durumunda RAID kartınızı değiştirebilirsiniz. RAID kartının arızalanması disk yapısının tamamen bozulduğu anlamına gelmemektedir. RAID kartını değiştikten sonra yeni raid kartınız sunucu boot olurken disklerdeki RAID yapısını okuyacak ve RAID yapısını kendi üzerine alması için onay isteyecektir.

* RAID Controller kartlarında Battery pili yazılan verilerin disklere iletilmesinden ve güvenliğinden sorumludur. Olası bir anlık kesinti halinde veriler battery üzerinde tutulur ve sunucunun tekrar aktif olması halinde veriler disklere yazılır. Battery olmaması durumunda büyük veri kayıpları yaşanabilir. Ayrıca battery performansıda etkilemektedir. RAID5 Controller üzerinde battery olmadan saatte 8 gb civarında bir yazma söz konusuyken Battery ile bu 70 gb'lara kadar çıkabilmektedir. Bu ciddi bir fark olduğundan dolayı Battery kesinlikle kullanılması tavsiye edilir.

RAID 0

RAID 0, disk şeritleme olarak adlandırılır. RAID 0 yapılandırmasını gerçekleştirmek için en az 2 diskin olması gerekir. 3 diskten oluşan RAID 0 yapısını aşağıda görebilirsiniz.



Bu yapılandırmada, veriler 3 diske paylaştırılarak yazılır. Windows yazılacak veriyi, şerit adı verilen bloklara ayırır ve kümedeki tüm disklere, bu şeritleri sırayla yazar. Yani kümede üç disk varsa, verinin bir kısmını Disk 1'e, bir kısmını Disk 2'ye ve bir kısmını da Disk 3'e yazar. Bu işleme şeritleme adı verilir. Bu yapılandırma ile hız artar, ancak herhangi bir diskte sorun olması durumunda veri bütünlüğü kaybolacağı için veri anlamını yitirir. Disk Yönetimi, şeritleme kümesinin genel boyutu olarak en küçük disk biriminin boyutunu alır. Örneğin, en küçük birim boyutu 1 GB ise üç diskten oluşan şeritleme kümesinin boyutu 3 GB'tır.

RAID 1

RAID 1, disk yansıtma olarak adlandırılır.

- RAID 1 için, iki birim iki sürücüde aynı biçimde yapılandırılmalıdır.
- En az 2 dinamik diskin olması gerekir.
- Veriler her iki diske de yazılır.
- Disklerden biri arızalanırsa, veriler diğer diskte de bulunduğu için kaybedilmez.
- RAID 1 ile depolama alanı boyutu yarı yarıya azalır. Örneğin 60 GB boyutundaki bir diski yansıtmak için bir 60 GB disk daha gerekir. Bu 60 GB bilgiyi saklamak için 120 GB alan kullanılacağı anlamına gelir.
- RAID 1, genellikle sistem dosyalarının yedeklerini tutmak için kullanılır.

Aynı veri iki diske yazıldığı için hız yaklaşık olarak %50 düşer. Fakat disklerin birinde herhangi bir sorun olduğunda diğeri kaldığı yerden devam eder, veri kaybı yaşanmaz.

RAID 5

RAID 5, eşlikli disk şeridi olarak adlandırılır. RAID 1 ile karşılaştırıldığında, hataya dayanıklılığının yanı sıra daha az yük ve daha iyi okuma performansı sağlar. RAID 5'i yapılandırmak için RAID 0'da olduğu gibi en az üç disk kullanılır. Ancak RAID 0'dan farklı olarak, tek bir diskin arızalanması halinde, tüm sürücü kümesinin kullanılamaz olmasını engellemek için eşlik hata denetimi özelliği bulunur.

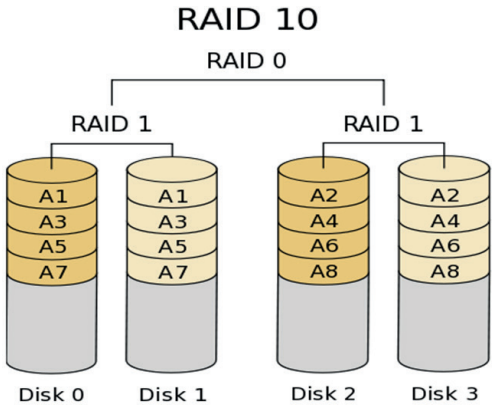
Bir algoritma ile bilgiler disklere sırası ile yazılırken, her defasında bir diske yazılan bilgilerin algoritması kaydedilir. Bu şekilde devam eden veri yazma işlemi ile RAID 5 sistemindeki herhangi bir diskin arızalanması durumunda sistemin çalışmaya devam etmesi, arızalı diskin sistem kapanmadan değiştirilmesi ve RAID 5 yapının tekrar oluşturulmasını sağlamaktadır. Burada tek bir disk güvenlik için kullanılmaktadır. Bu yüzden toplam kapasite, bir disk eksik olacaktır.

RAID 6

Bu model RAID 5 ile hemen hemen aynıdır. Tek farkı Parity diskinin 1 tane değil de 2 tane olmasıdır. Parity diskinin 2 tane olmasından dolayı okuma hızı RAID 5 ile aynı olmasına rağmen yazma hızı RAID 5'e göre daha kötüdür. Ancak güvenlik bakımından RAID 5'ten daha iyidir. Aynı anda 2 diskinizin arızalanması bu yapıya zarar vermeyecektir. Kapasite olarak ise 2 disk kaybınız bulunmaktadır. RAID 6 yapısını kullanabilmeniz için RAID kartınızın RAID 6 modelini desteklemesi gerekmektedir. Her RAID kartının desteklediği bir model olmamakla birlikte bazı RAID kartlarında ekstra lisans ile bile verilebilmektedir. Yüksek güvenlik ve iyi performans sağladığından dolayı tercih sebebidir.

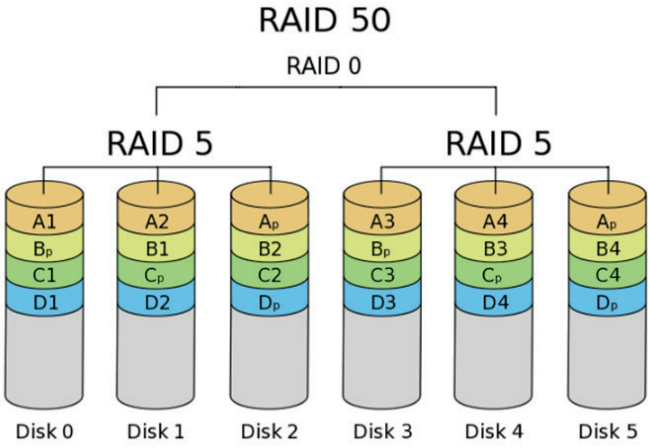
RAID 10

RAID 1 ve RAID 0 birleşmesi ile oluşan bir RAID modelidir. Performans olarak oldukça yüksektir. İki farklı RAID 1 yapısının RAID 0 ile birleşmesinden oluşur. Bu yapı için en az 4 disk gerekmektedir. Sadece çift sayıda diskler ile çalışır ve disk sayısını ne kadar arttırırsanız arttırın disk kapasitesi disk sayısı / 2 kadardır. Güvenlik olarak RAID 1 sağladığı güvenlik ile aynıdır. Tek bir RAID grubundaki 2 diskin arızalanması RAID yapısını bozar.



RAID 50

Bu RAID modeli en az 6 diskten oluşur. RAID 5 disklerin RAID 0 altında birleşmesi ile yapılır. Hem performanslı hem de güvenlidir.



Kuruluşumuzda Kullanılan İşletim Sistemleri

Kuruluşumuz Bilgi Teknolojileri Daire Başkanlığı merkezinde bulunan sunucularda Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016 ve Linux işletim sistemleri kullanılmaktadır.

Kişisel bilgisayarlarda ise; Windows XP, Windows 7, Windows 8 ve Windows 10 kullanılmaktadır.

3. YAZILIM GELİŞTİRME VE SÜREÇLERİ

YAZILIM NEDİR?

En yalın tanımıyla ***yazılım;*** elektronik bir donanımın, belirli bir işi yapması için derlenmiş komutların bütünüdür. Bu komutlar işlemcilerde işlenerek bir olaya dönüştürülür. **Türk Dil**

Kurumu Sözlüğü' ne göre **yazılım "***Bir bilgisayarda donanıma hayat veren ve bilgi işlemde kullanılan programlar, yordamlar, programlama dilleri ve belgelemelerin tümü.* (TDK Sözlük)" olarak tanımlanır.

Yazılım aslında hayatımızın her alanındadır ve her alanda hayatımızı kolaylaştırabilir. Bilgisayarlar, telefonlar, televizyonlar, mobil teknoloji, internet, sanayide kullanılan yeni nesil cihazların neredeyse tamamı, otomotiv, inşaat, eğitim, reklam, pazarlama, iletişim, medya, eğlence, sağlık başta olmak üzere hemen hemen tüm sektörlerde, uzay sanayisinde, günlük hayatta kullanılan bazı teknik aksesuarlarda kısacası "yazılım" gerçekten de yaşamın her alanındadır.

YAZILIM ÇEŞİTLERİ NELERDİR?

Pek çok kaynakta yazılım iki ana başlık altında incelenir:

- Bilgisayar Yazılımları
- Elektronik Yazılımları

Bilgisayar, temelde elektronik bir cihaz olsa da içindeki yazılım mantığı temel elektronik cihazlardan biraz daha farklı olduğu için bunları ayrı iki kategoriye ayırmak daha doğru olur. Mobil cihazlar da bilgisayar ile aynı kategoride anlatılabilir, aralarında pek fark yoktur.

BİLGİSAYAR YAZILIMLARI

Bilgisayar yazılımları da kendi içerisinde işlev olarak üçe ayrılır. Bunlar;

- Uygulama Yazılımları
- Sistem Yazılımları
- Çevirici Yazılımlar

Uygulama Yazılımları

Bilgisayarda kullanılan, bir görevi yapmak için yazılmış yazılımlardır. Mesela; *Web programları, Ofis Programları, Resim ve Video Düzenleme Programları, Oyunlar, Muhasebe Programları, İnsan Kaynakları, Stok Programları* gibi birçok kategoride uygulamalar bulunmaktadır. Kısacası uygulama yazılımları; insanların çalışmalarını hızlandırmak, bir işlemi bir veya birkaç tuşla yapabilmek için yazılmış yazılımlardır. DHMİ Bilgi Teknolojileri Dairesi Başkanlığı Yazılım Geliştirme Şubesinin ana görevi de, Kurumun ihtiyacı olan uygulama yazılımlarını geliştirmek veya geliştirilmesini sağlamaktır.

Sistem Yazılımları

Sistem yazılımları bilgisayar kullanımı için gerekli ana fonksiyonları sağlar ve bilgisayar donanımına ve sistemin yürütülmesine yardımcı olur. Şu kombinasyonları içerir:

- Aygıt sürücüleri
- İşletim sistemleri
- Sunucular
- Hizmet programları
- Pencere sistemleri

Sistem yazılımı çeşitli bağımsız donanım bileşenlerinin uyum içinde çalışmalarından sorumludur.

Sistem yazılımı bilgisayar donanımının işletilmesi ve uygulama yazılımının çalıştırılması için bir platform sağlamak için tasarlanmış bir bilgisayar yazılımıdır.

En temel sistem yazılımı türleri şunlardır:

- Bilgisayar BIOS'u ve aygıt yazılımı: Bilgisayara bağlı veya bilgisayar içindeki donanımı çalıştırmak ve kontrol etmek için gereken temel işlevselliği sağlar.
- İşletim sistemi (önde gelen örnekler; Microsoft Windows, Mac OS X ve Linux olmak üzere): Bilgisayar parçalarının; hafıza ile diskler arasında veri alışverişi veya monitöre görüntü sağlamak gibi görevleri uygulayarak birlikte çalışmasına olanak sağlar. Ayrıca üst düzey sistem yazılımı ve uygulama yazılımlarının çalıştırılması için bir platform oluşturur.
- Yardımcı yazılım: Bilgisayarın analiz edilmesine, yapılandırılmasına, yönetilmesine ve optimize edilmesine yardımcı olur.

Sistem yazılımları için uygulama yazılımlarından daha derin bir bilgisayar ve yazılım bilgisi gerekmektedir.

Çevirici Yazılımlar

Bu yazılımlar, herhangi bir dilde yazılan kodları makine diline (0 ve 1 lerden oluşan dile) çevirerek donanımlara ne yapması gerektiğini söyler. Bu sayede de bilgisayar/makine bu uygulamaları çalıştırabilir. Eğer yazılım diliyle, kullanılan programlama aracı uyuşmuyorsa veya doğru işletim sistemine ait değilse o program o cihazda çalışmayacaktır. Bunu Türkçe bilmeyen birine Türkçe bir şeyler anlatmak gibi düşünebilirsiniz.

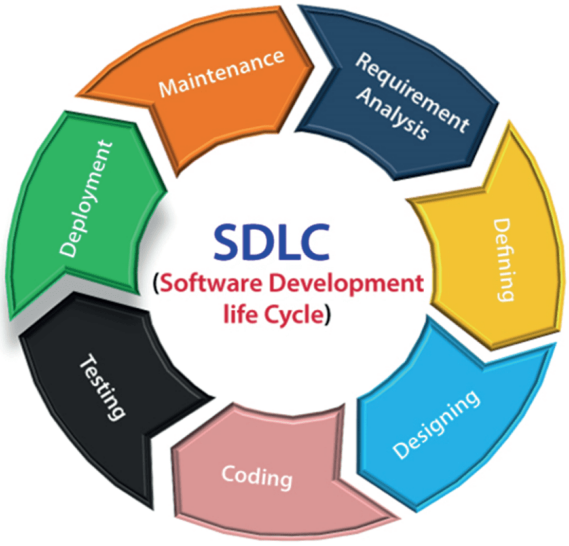
ELEKTRONİK YAZILIMLARI

Bir veya birkaç görevi yapması için yazılan, genellikle işlemcinin pin giriş-çıkışlarına bağlı sensörlerden veri okumak ve işlemek, giriş-çıkışlara bağlı olan motor veya led gibi elektronik cihaza bir iş yaptırmak amacıyla yazılan yazılımlardır. Bu yazılımlar küçük projelerden, sanayide kullanılan büyük cihazlara kadar her alanda kullanılmaktadır.

Bu arada elektronik yazılım dilleri ile bilgisayar dilleri aslında fark yoktur. Yani birçok ortak yazılım dili bulunmaktadır.

Elektronik yazılımının bilgisayar yazılımından farkı; elektronik yazılımlarda, programlanan işlemciyi mutlaka bir elektronik devre ile gerekiyorsa da mekanik tasarım ile birleştirilip kullanmak gerekmektedir. Yani elektronik yazılımlarda; kimi zaman kamera, kimi zaman ise motor gibi fiziksel bir karşılık mutlaka bulunmalıdır.

YAZILIM GELİŞTİRME YAŞAM DÖNGÜSÜ SÜRECİ (SDLC)



SDLC (Software Development Life Cycle), yüksek kaliteli bir ürün sunmak için yazılımın geliştirilmesiyle ilgili çeşitli aşamaları tanımlayan bir süreçtir. SDLC aşamaları, bir yazılımın, yani ürünün başlangıcından kullanımdan kaldırılmasına kadar olan tüm yaşam döngüsünü kapsar. Yazılım yaşayan bir organizma olduğu için bu süreci bir döngü olarak düşünmemiz gerekir.
SDLC sürecine bağlılık, yazılımın sistematik ve disiplinli bir şekilde geliştirilmesine yol açar.
SDLC, aşamaları pek çok kaynakta bazı aşamalar birleştirilerek veya farklı isimlendirmeler ile belirtilse de temel olarak 4 ile 10 aşamadan oluşan bir süreçtir. Farklı kaynaklarda farklı isimler ile belirtilse de genel olarak anlatılmak istenilen aynıdır. En Temel hali ile yazılım geliştirme yaşam döngüsünü aşağıda belirtilen 6 aşama ile tanımlayabiliriz:

1.Gereksinim Toplama ve Analiz (Requirement Analysis/Defining)
2.Tasarım (Designing)
3.Kodlama (Coding)
4.Test (Testing)
5. Dağıtım (Deployment)
6. Bakım (Maintanence)
Olaya Güvenliği de dahil edersek bu aşamalara ilave bir takım süreçler daha eklememiz gerekebilir.

Güvenli Yazılım Geliştirme Yaşam Döngüsü (Secure-Software Development Life Cycle)

1) Gereksinim Toplama ve Analiz
Planlama kısmını da bu aşamada ele alabiliriz. Yazılım yaşam döngüsünün başlangıç noktasıdır. Temel ihtiyaçların belirlendiği, proje için fizibilite çalışmalarının yapıldığı ve proje planlamasının oluşturulduğu dönemdir. Bu aşamada, beklentilerine göre bir ürün geliştirmek

için müşteriden ilgili tüm bilgiler toplanır. Herhangi bir belirsizlik yalnızca bu aşamada çözülmelidir.
İş analisti ve Proje Yöneticisi, müşterinin inşa etmek istediği, son kullanıcı kim olacak, ürünün amacı gibi tüm bilgileri toplamak için müşteri ile toplantılar yaparak anlamaya çalışır. Bir ürünü oluşturmadan önce, ürünle ilgili temel bir anlayış veya bilgi çok önemlidir.
İhtiyaç toplama yapıldıktan sonra, bir ürünün geliştirilmesinin fizibilitesini kontrol etmek için bir analiz yapılır. Herhangi bir belirsizlik olması durumunda, daha fazla tartışma için gerekirse daha fazla toplantılar yapılır.
Müşteriden alınan bilgiler ile yapılan analiz, Gereksinim analizi olup sonucunda Gereksinim Tanımları Dokümanı oluşturulur. Oluşturulan bu dokümanın müşteri tarafından da incelenip onaylanması çok faydalı olacak ve yanlış anlaşılan konuların en baştan düzeltilmesine olanak sağlayacaktır.
Sistem Analizini de bu aşamada ele almak gerekir. Analist bu aşamada iş akış şemalarını oluşturarak, sistem girdileri ve çıktılarının tanımlamalarını yapar.

2) Tasarım

Bu aşamada, Analiz aşamasında toplanan gereksinim girdi olarak kullanılır ve sistem geliştirmeyi gerçekleştirmek için kullanılan yazılım mimarisi türetilir.
Analiz çalışması sonucu ortaya çıkartılan proje detayları baz alınarak proje gerekli durumlarda bileşenlerine ayrılırlar, proje içerisinde yapılacak işlemler adım adım belirlenir ve proje planı oluşturulur. Proje planının yanısıra tasarım dokümanı da oluşturulmalıdır. Tasarım dokümanında proje bilgileri (amaç, kapsam vs), sistem tasarım bilgileri, tasarım detayları, veri modeli, kullanıcı arayüz tasarımları, UML Diagramları yer almalıdır. Tasarım dokümanının amacı, yazılım geliştiricinin yazılımını geliştirirken referans alacağı ve proje sürecinde/sonrasında projeye dahil olacak yeni yazılımcıların projeyi daha kolay anlayabilmesini sağlayacak teknik bir dokümantasyona sahip olması gerekliliğidir.

3) Uygulama veya Kodlama

Planlama, analiz ve tasarımı tamamlanıp yapılacak işlemleri detaylı olarak belirlenen projenin geliştirme aşamasıdır. Uygulama / Kodlama, kod geliştirici Tasarım dokümanını aldığında başlar. Yazılım tasarımı kaynak koduna çevrilir. Yazılımın tüm bileşenleri bu aşamada uygulanır. Üretim aşamasında yazılımcı alfa testlerini de gerçekleştirmektedir.

4) Test Etme

Test, kodlama tamamlandıktan ve modüller test için yayınlandıktan sonra başlar. Bu aşamada, geliştirilen yazılım kapsamlı bir şekilde test edilir ve bulunan tüm kusurlar, düzeltmeleri için geliştiricilere atanır. Test aşamasının test ekibi tarafından test araçları kullanılarak yapılması idealdir.
Yeniden test, regresyon testi, yazılımın müşterinin beklentisine göre olduğu noktaya kadar yapılır. Test uzmanları, yazılımın müşterinin standardına uygun olduğundan emin olmak için Gereksinim Tanımları Dokümanına başvurur.
Güvenlik testleri ve stres testleri gibi test adımları da bu aşamada ele alınabilir. Yazılım dağıtılmadan önce güvenlik açıklarının da tespit edilerek kapatılması önemli bir konudur.

5) Dağıtım

Ürün test edildikten sonra, üretim ortamında veya ilk olarak devreye alınır. Kullanıcı Kabul Testi de müşteri beklentisine göre bu aşamada yapılabilir.

Kullanıcı Kabul Testi için, üretim ortamının bir kopyası oluşturulur ve müşteri, geliştiricilerle birlikte testi yapar. Müşteri uygulamayı beklendiği gibi bulursa, müşteri tarafından yayına alınması için onay alınır.
Müşteri onayı alındıktan sonra, dağıtım aşamasında geliştirilen yazılım gerçek ortama yüklenir. Bu aşamada kullanıcı yetkilendirmeleri ve kullanıcı eğitimleri de gerçekleştirilir. Gerektiğinde kullanıcı kılavuzları hazırlanır.

6) Bakım

Yazılım yaşadığı sürece devam eden bir aşamadır. Bir yazılımın gerçek ortamına yüklenmesinden sonra bakımı, yani herhangi bir sorun ortaya çıkarsa ve düzeltilmesi gerekiyorsa veya herhangi bir iyileştirme yapılacaksa geliştiriciler tarafından yapıldığı aşamadır. Proje yayına alındıktan sonra oluşabilecek hataların giderilmesi, yazılımın iyileştirilmesi ve yeni işlevlerin eklenmesi süreçleridir. Bu süreç zarfında kullanıcılardan gelen bilgiler doğrultusunda bu istekler gerçekleştirilmektedir. Proje analizleri sırasında olmayan yeni bir istek gelecek olursa bu aşamada, süreç en başa yani analiz aşamasına tekrar döner ve diğer aşamalar sırası ile takip edilir. Yazılım Yaşam Döngüsü denilmesinin asıl sebebi de budur. Yazılım yaşadığı sürece döngü devam eder.

YAZILIM GELİŞTİRME SÜREÇ MODELLERİ

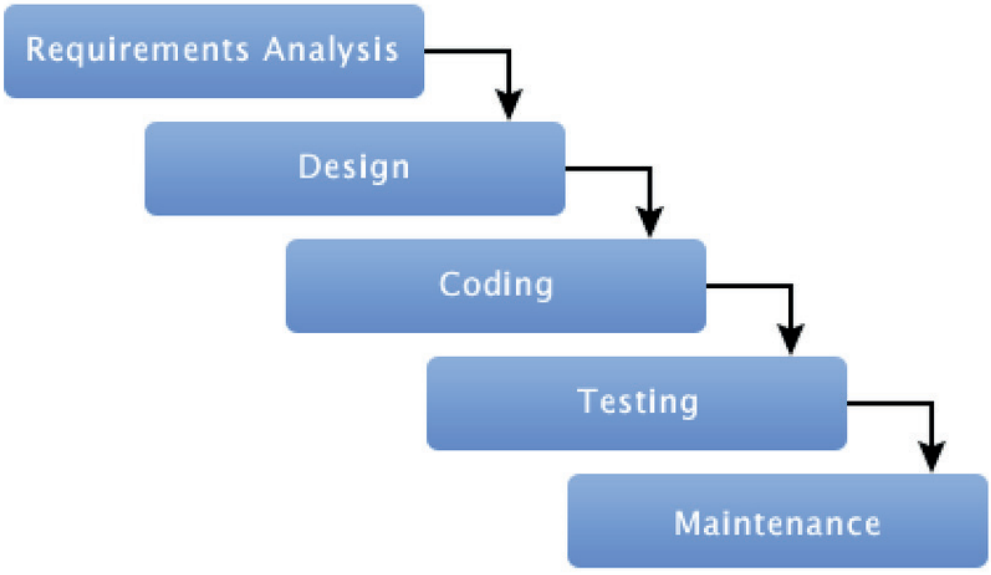
Sistem geliştirmenin zorluklarıyla baş edebilmek için, geliştirmeyi sistematik hale getirmeyi hedefleyen çeşitli süreç modelleri ortaya çıkmıştır. Bu modellerin temel hedefi; proje başarısı için, sistem geliştirme yaşam döngüsü (SDLC) boyunca izlenmesi önerilen mühendislik süreçlerini tanımlamaktır. Modellerin ortaya çıkmasında, ilgili dönemin donanım ve yazılım teknolojileri ile sektör ihtiyaçları önemli rol oynamıştır. En bilinen süreç modelleri:

- Çağlayan (Waterfall) Modeli
- Evrimsel (Evolutionary) Model
- Artırımlı (Incremental) Model
- Döngüsel (Spiral) Model
- Çevik (Agile) Model

ÇAĞLAYAN (WATERFALL) MODELİ:

Aşamaları:

Gereksinim Tanımlama: Gerçekleştirilecek sistemin gereksinimlerinin belirlenmesi işidir. Müşteri ne istiyor? Ürün ne yapacak, ne işlevsellik gösterecek?
Tasarım: Gereksinimleri belirlenmiş bir sistemin yapısal ve detay tasarımını oluşturma işidir. Ürün, müşterinin beklediği işlevselliği nasıl sağlayacak?
Gerçekleştirme ve Birim Test: Tasarımı yapılmış bir sistemin gerçekleştirilmesi işidir. Yazılım ürünü, tasarımı gerçekleştirecek şekilde kodlandı mı?
Tümleştirme ve Test: Gerçekleştirilmiş sistemin beklenen işlevselliği gösterip göstermediğini sınama işlemidir. Ürün, müşterinin beklediği işlevselliği sağlıyor mu?
İşletme ve Bakım: Müşteriye teslim edilmiş ürünü, değişen ihtiyaçlara ve ek müşteri taleplerine göre güncelleme işidir. Ürün müşteri tarafından memnuniyetle kullanılabiliyor mu?



Zorluklar:

Bir sonraki aşamaya geçmeden, önceki aşama neredeyse tümüyle tamamlanmış olmalıdır (örneğin, gereksinim tanımlama aşaması bitmeden tasarım aşamasına geçilemez.) Bu şekilde geliştirme boyunca değişen müşteri isteklerinin sisteme yansıtılması zorlaşır. Önceki nedenle bu model, gereksinimleri iyi tanımlı ve değişiklik oranı az olacak sistemler için daha uygundur. Çok az sayıda iş sisteminin gereksinimleri başlangıçta iyi şekilde tanımlanabilir. Bu zorluğu aşmak için; gereksinim tanımlama aşamasından önce iş gereksinimlerinin anlaşılması ve tanımlanması faydalı olabilir. Daha çok, geniş kapsamlı sistem geliştirme projeleri için tercih edilir.

EVRİMSEL (EVOLUTIONARY) MODEL:

Sistem, zaman içinde kazanılan anlayışa göre gelişir. Amaç, müşteriyle birlikte çalışarak taslak bir sistem gereksinimleri tanımından, çalışan bir sisteme ulaşmaktır. En iyi bilinen gereksinimlerle başlanır ve müşteri tarafından talep edildikçe yeni özellikler eklenir. Öğrenme amacıyla, sonradan atılabilecek prototipler (throw-away prototyping) geliştirilir. Amaç, sistem gereksinimlerini anlamaktır. En az bilinen gereksinimlerle başlanır ve gerçek ihtiyaç anlaşılmaya çalışılır.

Zorluklar:

Geliştirme süreci izlenebilir değildir. Her seferinde eklemelerle çalışan sistem, müşteriyle gözden geçirilir. Zaman içinde kazanılan anlayışa göre geliştirilen sistemler, sıklıkla kötü tasarlanır. Küçük- ve orta-ölçekli, etkileşimli (interactive) sistemler için uygulanabilir.

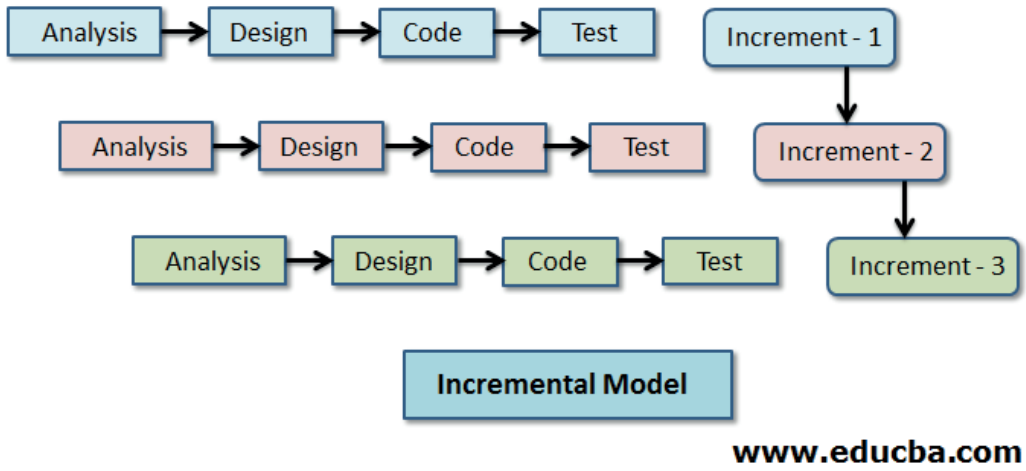
ARTIRIMLI (INCREMENTAL) MODEL:

Sistemi tek seferde teslim etmek yerine geliştirme ve teslim parçalara bölünür. Her teslim beklenen işlevselliğin bir parçasını karşılar.

Kullanıcı gereksinimleri önceliklendirir ve öncelikli gereksinimler erken teslimlere dahil edilir.

Bir parçanın geliştirilmesi başladığında, gereksinimleri dondurulur. Olası değişiklikler sonraki teslimlerde ele alınır.

Kazançları:
Her teslimle birlikte müşteriye görünen bir değer döndüğünden, sistemin işlevselliği erken erken aşamalarda ortaya çıkar.
Erken teslimler, sonraki teslimler için gereksinimleri çıkarmada prototip vazifesi görür.
Projenin tümden batması riskini azaltır.
Öncelikli gereksinimleri karşılayan sistem işlevleri daha çok test edilir.

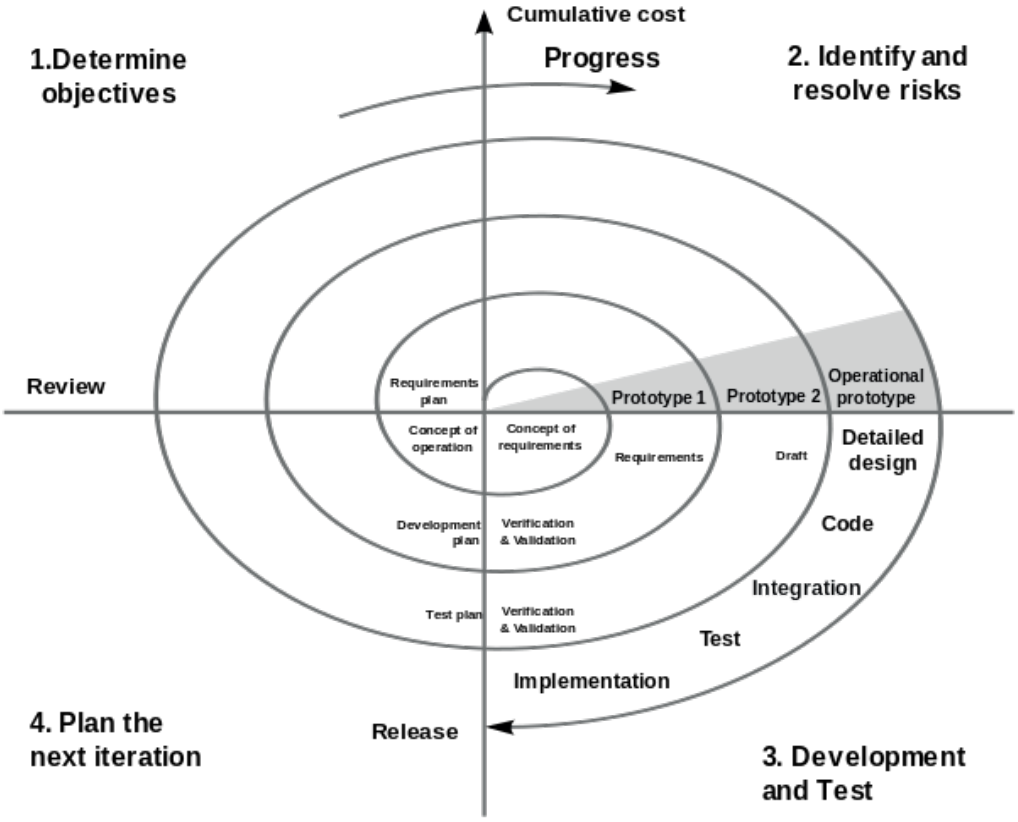


DÖNGÜSEL (SPIRAL) MODEL:

Süreç, geri dönüşümlü etkinlikler zinciri yerine döngüsel olarak ifade edilir.
Her döngü süreçteki bir aşamayı ifade eder.
4 sektörden oluşur:

- Hedef Belirleme: Aşamanın başarımı için somut hedefler belirlenir.
- Risk Değerlendirme ve Azaltma: Riskler adreslenerek azaltıcı eylemler gerçekleştirilir.
- Geliştirme ve Doğrulama: Genel modeller içinden geliştirme için bir model seçilir.
- Planlama: Proje gözden geçirilir ve bir sonraki aşama planlanır.

Riskler süreç boyunca özel olarak ele alınır ve çözümlenir.
Tanımlama ve tasarım gibi alt aşamalar yoktur; her döngü ihtiyaca göre seçilir.



ÇEVİK (AGILE) MODEL:

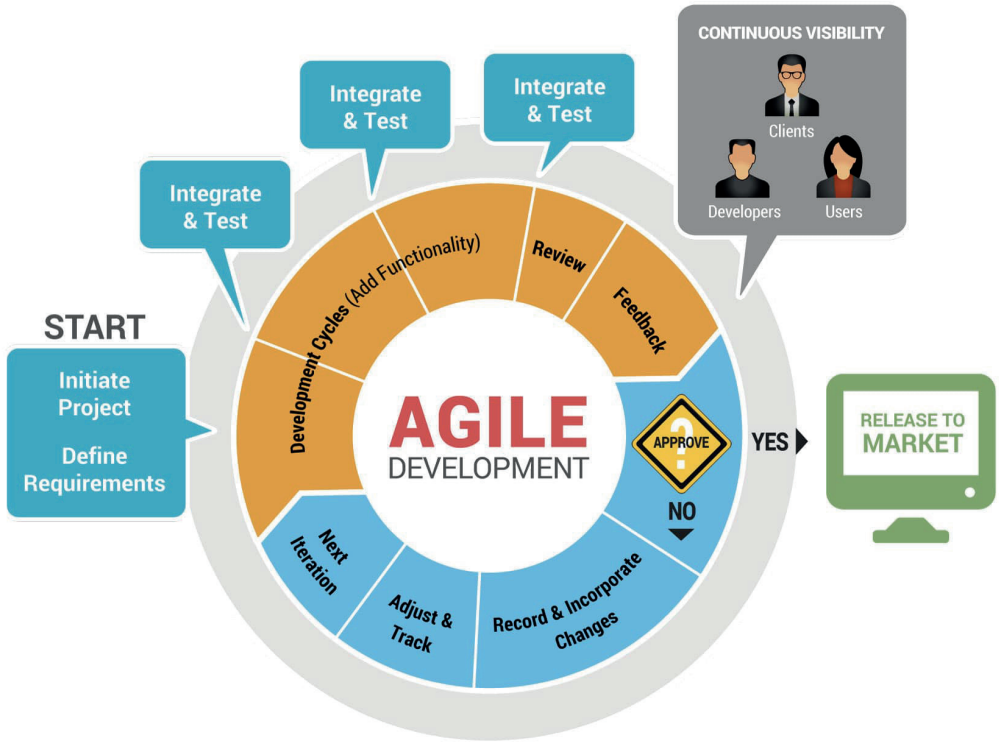
Mevcut geleneksel modellere alternatif olarak, 1990' larda ortaya çıkmaya başlamıştır.
Çevik Modeller kapsamında; yazılım sistemlerini etkili ve verimli bir şekilde modellemeye ve belgelendirmeye yönelik, pratiğe dayalı yöntemler yer alır.
Bu modelleme biçiminin; kapsadığı değerler, prensipler ve pratikler sayesinde geleneksel modelleme metotlarına göre yazılımlara daha esnek ve kullanışlı biçimde uygulanabileceği savunulmaktadır.
2001 yılında, dünyanın önde gelen çevik modellerinin temsilcileri, ortak bir zeminde buluşabilmek adına bir araya gelerek **"Çevik Yazılım Geliştirme Manifestosu"** nu yayınlamışlardır. Bu manifestoya göre:

- Bireyler ve aralarındaki etkileşim, kullanılan araç ve süreçlerden,
- Çalışan yazılım, detaylı belgelerden,
- Müşteri ile işbirliği, sözleşmedeki kesin kurallardan,
- Değişikliklere uyum sağlayabilmek, mevcut planı takip etmekten daha önemli ve önceliklidir.

Çevik Yazılım Geliştirme Manifestosu maddelerinin altında yatan temel prensipler şunlardır:

- İlk öncelik; sürekli, kaliteli yazılım teslimatı ile müşteri memnuniyetini sağlamaktır.
- Proje ne kadar ilerlemiş olursa olsun değişiklikler kabul edilir. Çevik yazılım süreçleri değişiklikleri müşteri avantajına dönüştürür.

- Mümkün olduğunca kısa zaman aralıkları ile (2-6 hafta arası) çalışan, kaliteli yazılım teslimatı yapılır.
- Analistler, uzmanlar, yazılımcılar, testçiler vs. tüm ekip elemanları bire bir iletişim halinde, günlük olarak birlikte çalışır.
- İyi projeler motivasyonu yüksek bireyler etrafında kurulur. Ekip elemanlarına gerekli destek verilmeli, ihtiyaçları karşılanarak proje ile ilgili tam güvenilmelidir.
- Ekip içerisinde kaliteli bilgi akışı için yüz yüze iletişim önemlidir.
- Çalışan yazılım, projenin ilk gelişim ölçütüdür.
- Çevik süreçler mümkün olduğunca sabit hızlı, sürdürülebilir geliştirmeye önem verir.
- Sağlam teknik alt yapı ve tasarım çevikliği arttırır.
- Basitlik önemlidir.
- En iyi mimariler, gereksinimler ve tasarımlar kendini organize edebilen ekipler tarafından yaratılır.
- Düzenli aralıklarla ekip kendi yöntemlerini gözden geçirerek verimliliği arttırmak için gerekli iyileştirmeleri yapar.



VERİ TABANI

Veritabanı, genellikle bir bilgisayar sisteminde elektronik olarak depolanan yapılandırılmış bilgi veya veriden oluşan düzenli bir koleksiyondur. Veritabanı genellikle bir veritabanı yönetim sistemi (DBMS) ile kontrol edilir. Veri ve DBMS (Data Base Management System) ve aynı

zamanda bunlarla ilişkili uygulama yazılımları bir araya getirildiğinde sıklıkla yalnızca veritabanı olarak kısaltılan veritabanı sistemi olarak ifade edilir.
Günümüzde operasyonda kullanılan en yaygın veritabanı türlerindeki veri genellikle işlemeyi ve veri sorgulamayı verimli hale getirmek üzere bir dizi tablodaki satırlarda ve sütunlarda modellenir. Böylece veri kolayca erişilebilir, yönetilebilir, değiştirilebilir, güncellenebilir, kontrol edilebilir ve organize edilebilir hale getirilir. Çoğu veritabanında veri yazma ve sorgulama için yapılandırılmış sorgu dili (SQL) kullanılır.

SQL Nedir?

SQL verileri sorgulamak, değiştirmek ve tanımlamak ve aynı zamanda erişim kontrolü sağlamak üzere neredeyse tüm ilişkisel veritabanlarında kullanılan bir programlama dilidir. SQL ilk olarak 1970'li yıllarda Oracle'ın büyük katkıları ile IBM'de geliştirilmiş ve daha sonra SQL ANSI standardı uygulanmış ve SQL IBM, Oracle ve Microsoft gibi şirketlerden pek çok uzantının temelini atmıştır. SQL günümüzde oldukça yaygın bir şekilde kullanılsa da yeni programlama dilleri geliştirilmeye başlandı.
Veritabanları, 1960'lı yılların başlarında ortaya çıkmalarından bu yana radikal bir evrim sürecinden geçmiştir. Hiyerarşik veritabanı gibi navigasyonel veritabanları (ağaç benzeri bir modeli temel alır ve yalnızca bir kaynaktan çoklu alıcıya doğru ilişkiye olanak sağlar) ve ağ veritabanı (çoklu ilişkilere olanak sağlayan daha esnek bir model), verileri depolamak ve değiştirmek üzere kullanılan orijinal sistemlerdi. Bu ilk sistemler kolay olsa da esnekti. 1980'li yıllarda ilişkisel veritabanları popüler oldu ve ardından 1990'lı yıllarda nesne odaklı veritabanları ortaya çıktı. Daha yakın bir zamanda ise, internetin büyümesine ve yapılandırılmamış verilerin daha hızlı bir şekilde işlenmesine duyulan ihtiyaca yanıt olarak NoSQL veritabanları kullanılmaya başlandı. Günümüzde ise bulut veritabanları ve kendi kendini yöneten veritabanları veri toplama, depolama, yönetme ve kullanma konusunda çığır açıyor.
Hem veritabanları hem elektronik tablolar (ör. Microsoft Excel) bilgi depolamak için uygun yöntemlerdir. Aralarındaki temel farklar şu şekilde sıralanabilir:
Veri toplama ve değiştirme yöntemi
Verilere erişebilen kişiler
Depolanabilecek veri miktarı
Elektronik tablolar orijinal olarak tek kullanıcı için tasarlanmış olup özellikleri bu amacı yansıtmaktadır. Muazzam düzeyde karmaşık veri manipülasyonuna ihtiyaç duymayan tek veya az sayıda kullanıcı için harika bir seçenektir. Diğer yandan veritabanları ise çok daha yüksek miktarda, kimi zaman devasa miktarlarda bilgi koleksiyonlarını barındırmak üzere tasarlanmıştır. Veritabanları, oldukça karmaşık bir mantık ve dil kullanımıyla aynı anda birden fazla kullanıcının hızlı ve güvenli bir şekilde verilere erişmesine ve veri sorgulamasına olanak sağlar.

Veri Tabanı Türleri:

Çok sayıda farklı veritabanı türü bulunur. Belirli bir kurum için en iyi veritabanı, söz konusu kurumun verileri nasıl kullanmayı amaçladığına bağlı olarak değişiklik gösterir.
İlişkisel Veritabanları: İlişkisel veritabanları 1980'li yılların sonlarında piyasada hakimiyet kazandı. İlişkisel veritabanındaki öğeler, sütunlar ve satırlardan oluşan bir tablo kümesi şeklinde organize edilir. İlişkisel veritabanı teknolojisi, yapılandırılmış bilgilere en verimli ve esnek şekilde erişme olanağını sağlar.
Nesne Odaklı Veritabanları: Nesne odaklı bir veritabanındaki bilgiler, tıpkı nesne odaklı programlamada olduğu gibi nesneler biçiminde temsil edilir.

Dağıtılmış Veritabanları: Dağıtılmış veritabanı, farklı yerlerde bulunan iki veya daha fazla dosyadan oluşur. Veritabanı, farklı ağlara yayılan ya da aynı fiziksel konumda yer alan birden fazla bilgisayarda depolanabilir.
Veri Ambarları: Merkezi bir veri havuzu olan veri ambarı, özel olarak hızlı sorgulama ve analiz amaçlarıyla tasarlanmış bir veritabanı türüdür.
NoSQL Veritabanları: Bir NoSQL veya ilişkisel olmayan veritabanı yapılandırılmamış ve yarı yapılandırılmış verilerin depolanmasına ve değiştirilmesine olanak tanır (veritabanına girilen tüm verilerin nasıl düzenleneceğini tanımlayan ilişkisel veritabanının aksine). NoSQL veritabanları, web uygulama yazılımlarının daha yaygın ve daha karmaşık hâle gelmesi ile birlikte popülerlik kazandı.
Grafik Veritabanları: Grafik veritabanı, verileri birimler ve birimler arasındaki ilişkiler açısından depolar.
OLTP Veritabanları: OLTP veritabanı, birden fazla kullanıcı tarafından çok sayıda işlemin gerçekleştirilmesi için tasarlanmış hızlı ve analitik bir veritabanıdır.
Günümüzde onlarca veritabanı türü kullanılmaktadır. Daha az yaygın olan diğer veritabanları bilimsel, finansal ya da diğer işlevlere özel olarak tasarlanmıştır. Farklı veritabanı türlerine ek olarak, bulut ve otomasyon gibi radikal ilerlemeler ve teknoloji geliştirme yaklaşımlarındaki değişiklikler veritabanlarının rotasını yepyeni yerlere çeviriyor. En yeni veritabanlarından bazıları şu şekilde sıralanabilir:
Açık Kaynak Veritabanları: Açık kaynak veritabanı sistemi, kaynak kodu açık kaynak olan bir sistemdir. Bu tür veritabanları SQL veya NoSQL veritabanları olabilir.
Bulut Veritabanları: Bir bulut veritabanı özel, genel veya hibrit bulut bilgi işlem platformunda bulunan yapılandırılmış veya yapılandırılmamış bir veri koleksiyonudur. İki tür bulut veritabanı modeli bulunur:
Geleneksel ve Servis Olarak Veritabanı (DBaaS): DBaaS sayesinde yönetim görevleri ve bakım işlemleri servis sağlayıcı tarafından gerçekleştirilir.
Çoklu Model Veritabanı: Çoklu model veritabanları, farklı veritabanı türlerini tek bir entegre arka uçta buluşturur. Buna göre çeşitli veri türlerini içerebilirler.
Belge/JSON Veritabanı: Belge odaklı bilgilerin depolanması, alınması ve yönetilmesi için tasarlanan belge veritabanları, verileri satırlar ve sütunlar yerine JSON biçiminde depolamak için modern bir yöntem sunar.
Kendi Kendini Yöneten Veritabanları: En yeni ve en ezber bozan veritabanı türü, kendi kendini yöneten veritabanları (aynı zamanda otonom veritabanları olarak bilinir), geleneksel olarak veritabanı yöneticileri tarafından gerçekleştirilen ince ayar, güvenlik, yedekleme, güncelleme ve diğer rutin yönetim görevlerini otomatikleştirmek üzere makine öğreniminden yararlanan bulut tabanlı çözümlerdir.

Veritabanı Yazılımı:
Veritabanı yazılımı dosya ve kayıt oluşturmayı, veri girişini, veri düzenlemeyi, güncellemeyi ve raporlamayı kolay hale getirerek veritabanı dosyalarını ve kayıtları oluşturmak, düzenlemek ve muhafaza etmek için kullanılır. Yazılım veri depolama, yedekleme ve raporlama, çok erişimli denetleme ve güvenlik de sağlar. Hırsızlık olayları artığından, güçlü veritabanı güvenliği günümüzde özellikle önem kazanmıştır. Veritabanı yazılımı bazen "veritabanı yönetim sistemi" (DBMS) olarak da adlandırılmaktadır.
Veritabanı yazılımı veri yönetimini daha kolay hale getirir ve kullanıcıların yapılandırılmış bir forma veri depolamalarına ve sonra buna erişmelerine olanak tanır. Genellikle veri

oluşturmaya ve yönetmeye yardımcı olan bir grafiksel arayüzdür ve bazı durumlarda kullanıcılar veritabanı yazılımı kullanarak kendi veritabanlarını oluşturabilir.

Veritabanı Yönetim Sistemi (DBMS)

Veritabanları tipik olarak veritabanı yönetim sistemi (DBMS) olarak bilinen kapsamlı bir veritabanı yazılım programını gerektirir. DBMS, veritabanı ve son kullanıcıları ya da programlar arasında bir arayüz işlevi görerek kullanıcıların bilgilerin nasıl organize ve optimize edildiğini yönetmesine, bilgileri almasına ve güncellemesine olanak sağlar. DBMS aynı zamanda veritabanlarına ilişkin gözetim ve kontrol faaliyetlerini kolaylaştırarak performans izleme, ince ayar ve yedekleme ve kurtarma gibi çeşitli yönetim operasyonlarının gerçekleştirilebilmesini sağlar.

Popüler veritabanı yazılımlarına ya da DBMS'lere MySQL, Microsoft Access, Microsoft SQL Server, FileMaker Pro, Oracle Database ve dBASE örnek olarak gösterilebilir.

PROGRAMLAMA DİLLERİ

Programlama dili, programcının belli bir algoritmayı ifade etmek için kullandığı standartlaşmış bir notasyondur. Bir programcı komutları yazmak için farklı programlama dilleri kullanabilir. Programlama dilleri, programcının bilgisayara hangi veri üzerinde işlem yapacağını, verinin nasıl depolanıp iletileceğini, hangi koşullarda hangi işlemlerin yapılacağını tam olarak anlatmasını sağlar. Şu ana kadar 2500'den fazla programlama dili yapılmıştır.

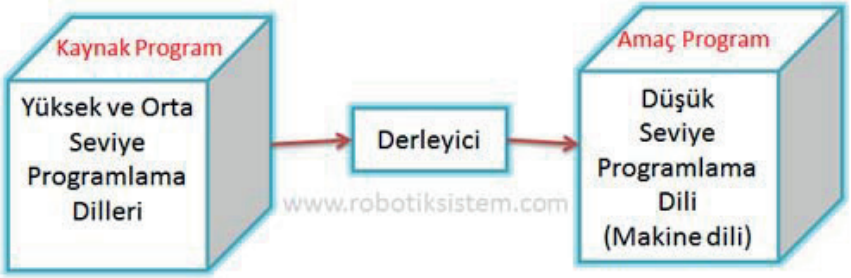
Programlama dilleri insanların algılamasına yakın olmasına göre 3 gruba ayrılır.

Alt Seviye Programlama Dilleri: Makine koduna oldukça yakın programlama dilleridir. Makina hakimiyeti oldukça gelişmiştir. Bu programlama dillerini bilen kişilerin mikro işlemciler hakkında bilgi sahibi olması gereklidir. (Assembly programlama dili gibi)

Orta Seviye Programlama Dilleri: Oldukça esnek olan bu diller hem üst hem alt seviye programlama yapabilirler. Alt seviye dillere oranla biraz daha anlaşılırdır. (C programlama dili gibi.)

Üst Seviye Programlama Dilleri: Olay tabanlı programlama dilleri olarak da adlandırılırlar yalnız bu programlama dilleri sadece belirli fonksiyonlar etrafında çalışırlar ve programlama hakimiyetini azaltırlar. En hızlı ve en etkili programlama dilleri bu kategoridedir. (visual basic ve pic basic pro gibi) Diğer programlama dillerine kıyasla daha kolay öğrenildiği ve uygulandığı için yeni başlayanlara en uygun diller üst seviye programlama dilleridir.

Yüksek seviyeli programlama dillerinde yazılan programın çalışabilmesi için makine diline çevrilmesi gerekir. Bunun için program hangi yüksek seviyeli dil ile yazıldıysa o dilin derleyicisi kullanılır. Böylece yüksek seviyeli programlama dili ile yazılmış olan kaynak program, makine dilindeki amaç programa dönüştürülür. Kaynak programın içeriğinin değiştirilmesi mümkündür, ancak derlenmiş olan amaç programın içeriğine müdahale etme imkanı yoktur.



En Çok Kullanılan Programlama Dilleri:

1. Python

2. C
3. Java
4. C++
5. C#
6. R
7. JavaScript
8. PHP
9. Go
10. Swift
11. Arduino
12. Ruby
13. Assembly
14. Scala
15. Matlab
16. HTML
17. Shell
18. Perl
19. Visual Basic
20. Cuda

Bu diller web, mobil ve elektronik gibi uygulamalarda kullanılan programlama dilleri olarak da ayrıca sınıflandırılmaktadır.

Web Tabanlı Programlama Dilleri:

Web programlama, web sunucular içerisinde yer alan sitelerin ara yüzlerinde çalışan tüm fonksiyonların programlanmasıdır. Örneğin bir web sitesinin tasarımı da dahil olmak üzere içerisindeki tüm yazılım, web programlama dilleri ile yazılır.

Listede yer alan popüler web programlama dillerinin sırası aşağıdaki gibidir.

1.Python
2.Java
3.C#
4.JavaScript
5.PHP
6.Go
7.Ruby
8.Scala
9.HTML
10.Perl
11.Lua
12.Rust
13.Processing
14.D
15.Clojure
16.Ocaml
17. Actionscript

Elektronik için Programlama Dilleri:

1. **C**

2. **C++**
3. **C#**
4. **Python**
5. **Java**

Makine diline en yakın olan assembly programlama dili dışında başka diller ile de elektronik programlama yapılabilmektedir. Elektronik programlama dilleri sayesinde elektronik donanıma sahip cihazların kontrolü sağlanır.

Mobil Programlama Dilleri:

Günümüzün en popüler mobil programlama dilleri:

1. **Java**
2. **C++**
3. **Objective-C**
4. **C#**
5. **HTML5**
6. **Swift**

Günümüzün en büyük girişimleri ve teknoloji devlerinin en büyük ürünleri mobil uygulamalardan oluşuyor. Böylelikle mobil uygulama geliştirmek için sağlanan platformlar ve mobil programlama dilleri de gün geçtikçe değer kazanıyor. Mobil programlama dilleri ile Android, Windows Phone, iOS gibi mobil işletim sistemlerine uyumlu uygulama geliştirmek mümkündür.

4. BİLGİSAYAR AĞLARI VE İLETİŞİM (NETWORK)

Network Nedir, Ne İşe Yarar?

Birden fazla bilgisayarın çeşitli sebeplerden dolayı bir iletişim aracı üzerinden(kablolu veya kablosuz), tüm iletişim, yazılım ve donanım bileşenleri ile birbirlerine bağlandığı yapıya network denir.

Bilgisayarların birbirine bağlanma sebepleri temel olarak aşağıda verilmiştir;

- Kaynakları paylaşmak (dosyalar, modemler, yazıcılar ve faks cihazları),
- Uygulama yazılımlarını paylaşmak (Kelime işlemci programı),
- Verimliliği artırmak (Verilerin kullanıcılar arasında paylaşımını kolaylaştırmak).

Kurumumuzu örnek verecek olursak. DHMI ağında ki tüm bilgisayar kullanıcıları ağ üzerinden bağlandığı sürece tüm lokasyonlarda dosya paylaşabilir, elektronik posta gönderebilir veya alabilir, ip telefon ile görüşme yapabilir, faks gönderebilir veya yazıcıdan çıktı alabilirler.

Bilgisayar ağları temel olarak bilgisayarların kaynaklarını paylaşır. Sistem olarak bilgisayar ağı (network), sunucu ve istemci bilgisayarlardan oluşur. Üzerindeki herhangi bir kaynağı paylaşan bilgisayara sunucu (server), bu kaynağa erişen cihaza da istemci (client) adı verilir. Bir bilgisayarı sunucu yapan şey, üzerindeki donanım miktarı, hatta özel bir donanım olup olmaması değil, üzerindeki bir kaynağı paylaştırmasıdır. Doğal olarak üzerindeki kaynağı paylaştıran ve birçok kullanıcının hizmetine sunan bir bilgisayar, talebi karşılamak için daha güçlü olmalıdır. Ancak bir bilgisayara sunucu özelliğini veren üzerindeki donanım değil, kaynaklarını paylaştırmasını sağlayan yazılımdır (çoğunlukla işletim sistemi veya işletim sistemi içindeki bir yazılım modülü).

Yapılarına Göre Bilgisayar Ağları

Yapısal olarak bir bilgisayar ağı; **peer to peer(P2P)** ve **İstemci/Sunucu mimarisi** başlıkları altında incelenebilir.

Peer to peer(P2P) Bütün bilgisayarlar eşit haklara sahiptir. Sunucu ve istemci olarak birbirlerinden ayrılmazlar. Her bilgisayar yerine göre istemci gibi yerine göre sunucu gibi davranabilir.

İstemci/Sunucu yapısında ise; adından da anlaşılacağı üzere yazılımsal ve donanımsal olarak bir bilgisayar ana bilgisayar olarak tanımlanır. Çok sayıda kullanıcı olması, güvenliğin ve işlem

yoğunluğunun belli bir kapasiteyi aşması gibi durumlarda, sunucu tabanlı ağ sistemine gereksinim duyulur. Sunucu tabanlı ağlarda bir bilgisayar daha güçlü ve özel bir bilgisayardır. Buna sunucu (server) denir. Sunucu bilgisayar genellikle ağ işlemlerine atanır ve ağ yöneticisi tarafından ağ yönetimi işlemleri için kullanılır. Genellikle diğer rutin işlemler için kullanılmaz. Sunucu tabanlı ağ sistemlerinde genel olarak aşağıdaki sunucular kullanılabilir.

- Dosyalama ve yazdırma sunucuları, kullanıcıların dosya ve yazıcı kaynaklarına erişimini düzenlerler.
- Uygulama sunucuları, uygulamaların istemci/sunucu tarafından çalıştırılmalarını sağlar.
- Posta sunucuları, (mail server) kullanıcılar arasında posta alışverişini sağlar.
- Faks sunucuları, kullanıcılar arasında faks alışverişini sağlar.

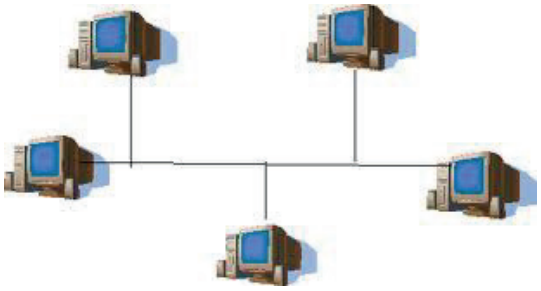
Yapılarına göre bilgisayar ağları 3 temel özellik gösterirler:

- Doğrusal veya BUS yapı (linear veya BUS topology)
- Halka yapı (ring topology)
- Yıldız yapı (star topology)

Doğrusal veya BUS Yapı (Linear veya BUS Topology)

Doğrusal yapı da sunucu (server) ve iş istasyonları (workstation) bir hat üzerinde sıralanırlar. Bu yapıya 'BUS Topology' de denmektedir. Bütün bilgi alış verişleri bu hat üzerinden olmaktadır. Hat kalitesi ile doğru orantılı olarak sinyal transfer hızı da değişmektedir. Hat da bir arıza olduğu zaman çalışan hattın dışında kalan uçlar çalışamaz duruma düşmektedirler. Bu yapıda olan yerel ağlar ETHERNET yapı olarak tanımlanırlar. Ağı kurabilmek için iş istasyonlarında ETHERNET kartı olmalıdır. Pek çok küçük ve orta büyüklükteki kuruluşlarda kullanılan bir yerel ağ yapısıdır. Kapasite olarak düşük olmakla birlikte yeni teknolojik ürünler ile hızları arttırılmaktadır.

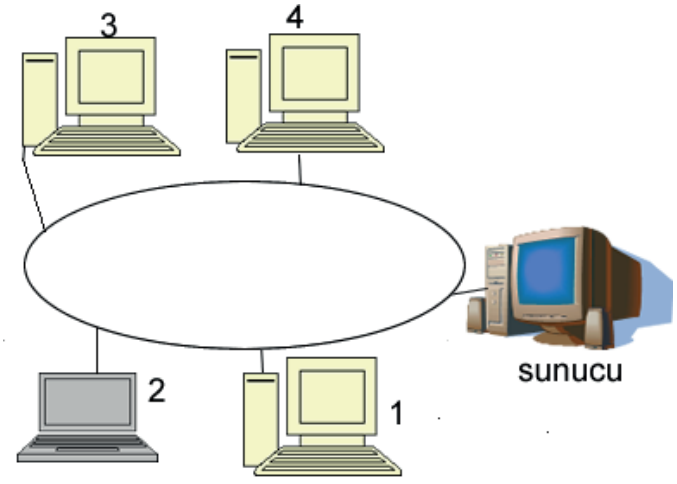
En büyük olumsuz yönü iletişim hattında bir arıza olduğu zaman çalışan hattın dışında kalanların çalışamaz olmasıdır. Bunu karşılık maliyeti düşük bir ağ yapısıdır.



Doğrusal veya BUS Yapı

Halka Yapı (Ring Topology)

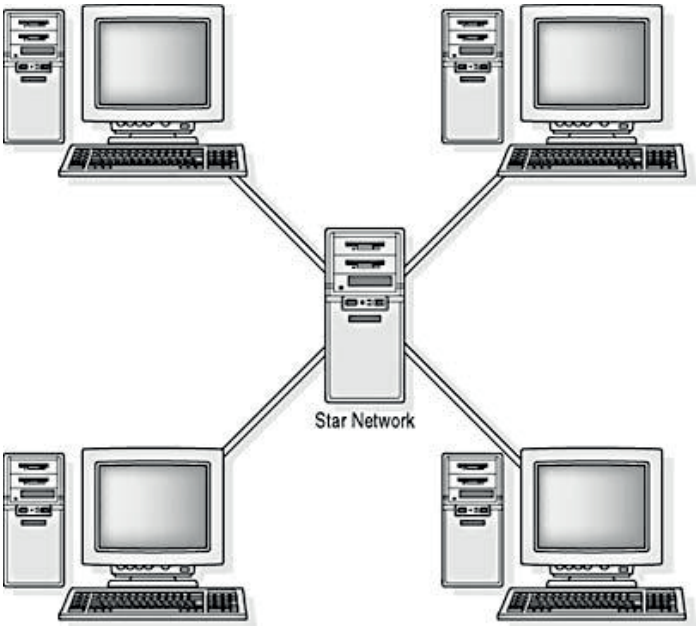
Halka yapıda ise sunucu ve diğer bağlantılı cihazlar bir dairenin kenarlarında yer alırlar. Bütün bilgi ve iletiler bu daire üzerinden gider.



Halka yapı ağlar maliyet bakımından diğer yerel ağlara göre biraz daha pahalıdır. İletişim hızları kablolama sisteminize bağlıdır. Halka yapının bir üstün yönü iletişim hattında bir arıza olunca kullanıcılara verebileceği bir seçenektir. Yukarıdaki örneği inceleyelim. Varsayalım 4 numaralı iş istasyonunda bir arıza olunca sinyaller 1 numaralı iş istasyonu üzerinden gider ve geri döner. Bu yöntem ile sinyal akışı kesilmemiş olur.

Yıldız Yapı (Star Topology)

Yıldız yapı da ise ağa bağlı tüm çevre birimleri doğrudan sunucuya bağlıdır. Bu yapı en eski yerel ağ yapısıdır. Bütün sinyal transferini merkezi yerdeki sunucu yapar. Sunucuda kendisine bağlı her iş istasyonu için bir ağ kartı olması gerekir.



Ağ Çeşitleri

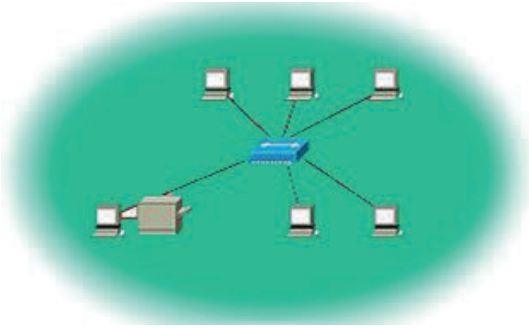
Bilgisayar ağ yapı çeşitlerini gördük. Bu ağ yapı çeşitlerine uyumlu olarak bilgisayar ağ çeşitleri bulunmaktadır. Bu ağlar:

- Yerel Ağlar (Local Area Networks)
- Geniş Alan Ağları (Wide Area Networks)
- Metropolitan Ağlar (Metropolitan Area Networks)

Yerel Ağlar (Local Area Networks - LAN)

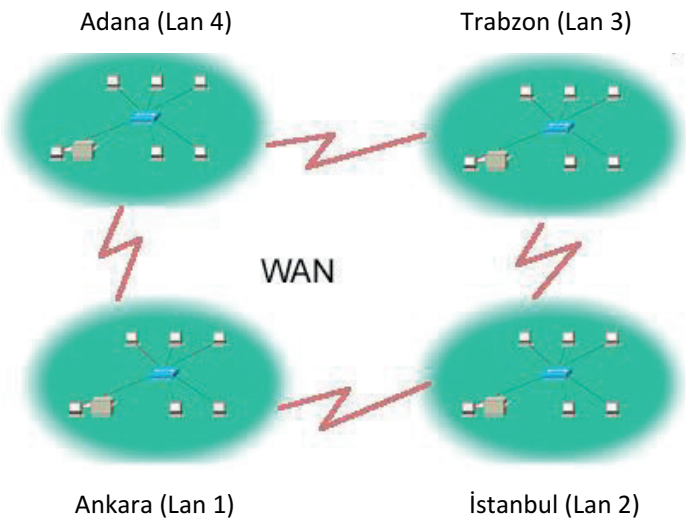
Bir sunucuya belirli bir uzaklıkla bağlanan gerek doğrusal, gerek halka ve gerekse yıldız yapıya sahip, mekân olarak küçük alanı kaplayan ağlara yerel ağlar denir.

Bir ilköğretim okulunda bulunan ağ yerel ağdır veya çok katlı bir binada hizmet veren bir şirketin oluşturduğu yapı yerel ağdır veya bir üniversitenin, bir fakültesinin kendi içerisinde kullandığı ağ yerel ağdır. Bu gibi örnekleri çoğaltabiliriz. Yapının nasıl olacağını kuruluşun amaçları ve finansal yapısı belirleyecektir. Yerel ağlar birbirleri ile bağlanabilirler.



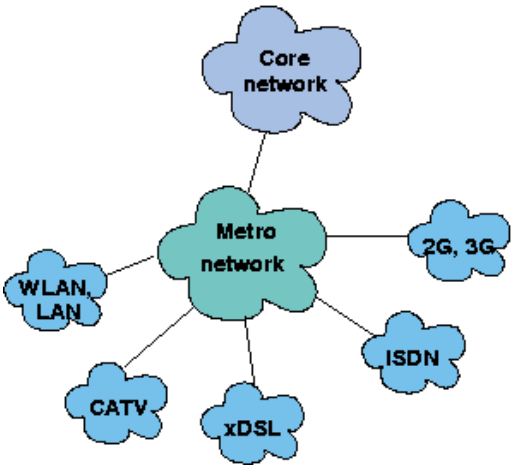
Geniş Alan Ağları (Wide Area Networks - WAN)

Yerel ağlar küçük ölçekli alanlar için oldukça kullanışlıdır. Ama iletişim teknolojisindeki gelişmeler uzaklıkları yakınlaştırdığı için gelişme yerel ağlardan çok daha büyük ve geniş alanları içeren bilgisayar ağlarına doğru olmaktadır. Geniş alan ağları bir ülke içerinde olabildiği gibi ülkeler, kıtalararası bile olabilmektedir.



Metropolitan Ağlar (Metropolitan Area Networks - MAN)

Metropolitan ağ da aslında bir geniş alan ağıdır. Ama temel bir özelliğinden dolayı geniş alan ağlarından ayrılmaktadır. Eğer bir geniş alan ağında(WAN) ağdaki tüm iletişim hatları aynı ise bu yapı “geniş alan ağı” dır. Ancak iletişim hatlarından bazıları yüksek kapasiteli ise (Metro Ethernet gibi) bu durumda bu ağ metropolitan ağdır.



Günümüzde tüm ülkelerin kullandıkları ağlarının içerisindeki bazı ağlar metropolitan ağ yapısında olan geniş alan ağlarıdır.

(Metro Ethernet, Türk Telekom tarafından sunulan yeni nesil erişim şebekesidir. Yerel alan ağında kullanılan Ethernet teknolojisinin metropole uygulanmasıdır. Fiber optik kablo bağlantısı ile gigabit seviyesine kadar bağlantı imkanı sunmaktadır.)

Ağ Kabloları ve Kablo Çakımı

Bilgisayarlar kablo aracılığıyla birbirine bağlanır. Değişik kablolama teknikleri ve kablo türleri vardır.

Bilgisayar ağlarında kullanılan kablo tipleri şunlardır:

- Çift Bükümlü Kablo (Twisted Pair Cable)
  - Korumasız Çift Bükümlü Kablo (Unshielded Twisted Pair-UTP)
  - Korumalı Dolanmış Çift (Shielded Twisted Pair-STP)
- Koaksiyel Kablo (Coaxial Cable)
- Fiber Optik Kablo (Fiber Optic Cable)

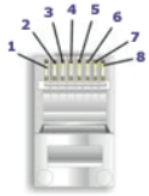
Bilgisayarlar ağa bağlanırken çoğunlukla UTP kablo kullanılır ve UTP kablolar kendi içinde güvenli olarak aktarabileceği veri miktarına göre kategorilere ayrılır. Bilgisayar ağlarında önce 10 Mbit ethernet döneminde CAT3 kablo yoğun olarak kullanılmış, 100 Mbit ethernetin geliştirilmesiyle CAT5 kablolar üretilmeye başlanmış ve kullanılmaktadır. UTP kablolar dış görünüş olarak birbirine çok benzer. Ancak her kablonun üzerinde kategorisi yazmaktadır. Kablonun kategorisi üretim kalitesiyle ilgilidir. Yapılan çeşitli testler ile kablonun belirtilen hızlarda elektrik sinyalini ne kadar sağlıklı ve az kayıpla iletebildiği, manyetik alan etkisine karşı

sinyali ne kadar koruyabildiği ölçülür. Testler ile ortaya konan değerler kategorinin kriteridir. Bu kriterleri tutturabilen kablo bu kategoriyi almaya hak kazanır. CAT5 ile 100 Mbit hızında veri aktarımı yapılabilir. Bir sonraki standart CAT5e (Enhanced CAT5, gelişmiş CAT5) standardıdır. Bu CAT5 ile aynı yapıda olup, daha üst seviye değerlere erişebilen bir kablodur. CAT5e ile gigabit hızına ulaşılabilir. Gigabit ethernet'te CAT5 kullanılabilmekle beraber CAT5e tavsiye edilir. CAT6'da da aynı durum söz konusu CAT5e'den de daha yüksek değerlere erişebilir. CAT6 şu anda 568A standardına eklenmiş yani resmen kullanıma sunulmuştur. 1000Mhz hızı için, yani Gigabit ethernet için en uygun kablodur.

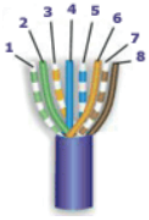
Category	Speed	Frequency
CAT 1	Carry only voice	1MHz
CAT 2	4Mbps	4MHz
CAT 3	10Mbps	16Mhz
CAT 4	16Mbps	20Mhz
CAT 5	100Mbps	100Mhz
CAT 5e	1000Mbps	100Mhz
CAT 6	1000Mbps	250MHz
CAT 7	10Gbps	600MHz
CAT 7a	10Gbps	1000Gbps
CAT 8	25Gbps	2000Mhz

Full Dublex Ethernet (Kablo) aynı anda hem data iletimini hem de data alınmasını sağlar. Half Dublex çalışmalarda bant genişliğinin %50-60 kullanılırken full dublex yapılarda bant genişliğinin tamamı kullanılabilir.

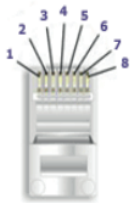
Bilgisayar ağlarında çift bükümlü ağ kabloları RJ–45 adı verilen konektöre 568-A veya 568-B standartlarında bağlanırlar.



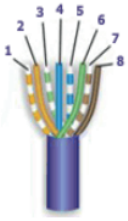
1	Yeşil	Beyaz
2	Yeşil	
3	Turuncu	Beyaz
4	Mavi	
5	Mavi	Beyaz
6	Turuncu	
7	K.Rengi	Beyaz
8	K.Rengi	



568-A bağlantısı



1	Turuncu	Beyaz
2	Turuncu	
3	Yeşil	Beyaz
4	Mavi	
5	Mavi	Beyaz
6	Yeşil	
7	K.Rengi	Beyaz
8	K.Rengi	



568-B bağlantısı

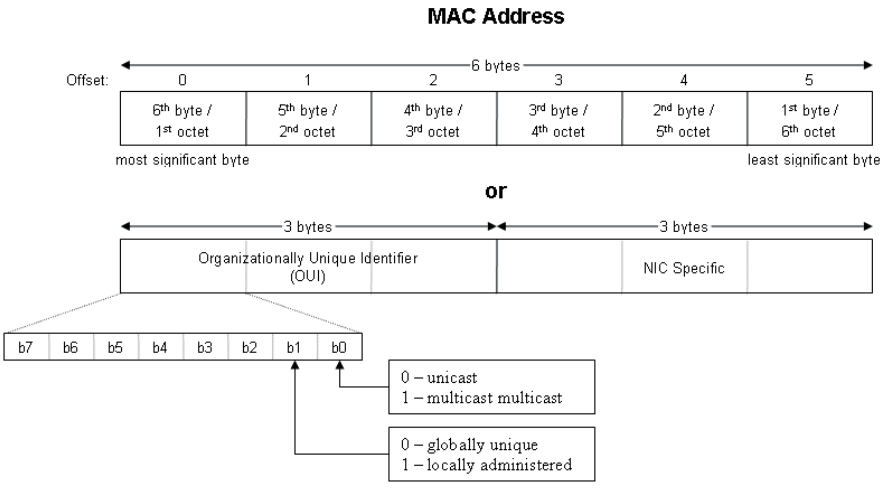
İki bilgisayarın birbirine bağlantısında çapraz (crossover) kablolama yapılır. Bunun anlamı ağ kablosunun bir ucunun 568-A, diğer ucunun da 568-B standardına göre bağlanmasıdır. İkiden fazla bilgisayarın birbirine bağlantısında anahtar (switch) kullanılır. Bu tür bağlantıda ise düz (straight) kablolama yapılır. Düz kablolamada kablonun her iki ucu da 568-A veya 568-B standardında göre bağlanır.

Network Cihazları

Ethernet Kartı

Bilgisayarların bir networke bağlanıp veri alış verişinde bulunabilmesini sağlayan elektronik devrelerdir. Farklı yerlerde Ethernet kartı, ağ kartı ya da NIC şeklinde isimlendirmeleri yapılmıştır. NIC Network Interface Card'ın kısaltmasıdır.

Her Ethernet kartının kendine ait bir numarası vardır ve buna MAC (Media Access Control) adresi denilmektedir. Bu adres 6 oktet 8 bitten oluşur. Bu 6 oktetin ilk 3 okteti IANA (Internet Assigned Numbers Authority) tarafından belirlenir. Bir firma Ethernet Kartı üretirken IANA'ya başvuru yapar IANA firmaya firmayı belirten 3 oktetlik bir adres verir kalan oktetleride firma tamamlar ve Ethernet kartını üretir. Bu standat sayesinde aynı MAC adresi taşıyan kartlar üretilmez. MAC adres için dünyada bir tane olmaktan başka belirleyici bir özelliği yoktur.



Bir bilgisayarın MAC adresini komut satırına **ipconfig /all** yazarak öğrenilebilir.

```
C:\Users\user>ipconfig /all

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : dhmi.root
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265
   Physical Address. . . . . . . . . : F8-34-41-F7-36-D1
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::745d:dcd:c95e:e68f%16(Preferred)
```

Hub

Ağ elemanlarını birbirine bağlayan çok portlu bir bağdaştırıcıdır. En basit ağ elemanıdır. Hub kendisine gelen bilgiyi gitmesi gerektiği yere değil, portlarına bağlı bütün bilgisayarlara yollar. Bilgisayar gelen bilgiyi analiz ederek kendisine gelmişse kabul eder. Ağı yorar.

Switch

Anahtar (switch) akıllı bir hub cihazıdır. Hub'ın yaptığı görevin aynısını yapar, ancak ağı yormaz. Aynı anda birden fazla iletim yapma imkânı sağlar. Böylece aynı anda bir bilgisayar yazıcıyı kullanırken diğer ikisi kendi aralarında dosya transferi yapabilirler.

Anahtar, portlarına bağlanan bilgisayarları MAC adreslerine bakarak tanır. Anahtarlama işlemini gerçekleştirmek için MAC adreslerini yapısında bulunan tabloda tutar. Bu tabloda MAC adresinin hangi porta bağlı olduğu bilgisi bulunur. Kendisine ulaşan veri paketlerinin MAC adreslerini inceler ve her porta dağıtmak yerine, sadece hedef MAC adresine sahip olan bilgisayarın bağlı olduğu porta bırakır. Böylelikle veri paketi sadece hedef bilgisayara ait portu ve kabloyu meşgul eder. Çakışmalar engellenmiş olur ve ağ performansı artar.

Tekrarlayıcı (Repeater)

Tekrarlayıcı alıcısına ulaşamama ihtimali bulunan veri paketlerini güçlendirmek amacıyla kullanılır. Uzaktaki bilgisayarlara ulaşmaya çalışırken veri paketleri yolda güç kaybederler. Tekrarlayıcı veri paketlerini güçlendirerek yollarına devam etmelerini sağlar. Tekrarlayıcı bir sinyali aldığında onu orijinal gücü ve durumuna getirir.

Köprü (Bridge)

Köprü temelde tekrarlayıcının yaptığı işi yapar. Tekrarlayıcı kendisine gelen veriyi güçlendirir ve hedefe bakmaksızın doğrudan yollar. Köprü ise, veri paketi o hedefe gitmiyorsa göndermez, yani gelen bilgiyi süzer. Köprü ayrıca birbirinden faklı ağları birbirine bağlar ve anlaşmalarını sağlar. Büyük ağların parçalanıp her biri bağımsız birer ağ niteliğini koruyacak biçimde daha küçük ağlara bölünmesinin ve bunların birbirine köprülenerek bağlanmasının (bridging) birçok faydası vardır.

Köprülemenin faydaları:

- Trafik yoğunluğu ayrıştırılmış olur; aynı ağı adresleyen trafik diğer ağları etkilemez.
- Herhangi bir ağda olabilecek bir hata veya arıza diğer ağlara yansıtılmamış olur.
- LAN'ların etkin uzunluğu artırılmış olur.

Yönlendirici (Router)

OSI başvuru modelinin ilk üç katmanına sahip aktif ağ cihazlarıdır. Temel olarak yönlendirme görevi yapar. LAN ve WAN arasında veya VLAN arasında bağlantı kurmak amacıyla kullanılır. Yönlendiricinin üzerinde LAN ve WAN bağlantıları için ayrı ayrı portlar bulunur. Bu portlar ile iki ağ arasında bağlantı sağlanır.

Bu işlem köprüler tarafından da yapılır. Aralarındaki fark ise köprüleme işlemi OSI 2. katmanında (data-link) gerçekleşirken, routing işlemi OSI 3. katmanında (network) gerçekleşir.

Yönlendirici görevini yaparken şu sırayı izler;

- Bir veri paketini okumak.
- Paketin protokollerini çıkarmak.
- Gideceği network adresini yerleştirmek.
- Routing bilgisini eklemek.
- Paketi alıcısına en uygun yolla göndermek.

Geçityolu (Gateway)

OSI başvuru modelinin 7 katmanının işlevlerini de içinde barındırır. Geçit yoluna gelen veri paketleri en üst katman olan uygulama katmanına kadar çıkar ve yeniden ilk katman olan fiziksel katmana iner. Geçit yolu farklı protokol kullanan ağlarda iki yönlü protokol dönüşümü yaparak bağlantı yapılmasını sağlar. Temel kullanım amaçları: Protokolleri birbirinden farklı iki ağı birbirine bağlamak ve aralarında geçit oluşturmak, IP yönlendirmek ve Güvenlik duvarı oluşturmaktır.

OSI Referans Modeli

Bilgisayarların ağ üzerinden haberleşmesini sağlamak için çeşitli protokollerin tanımlanması gerekir. OSI modeli 7 fonksiyonel katmandan oluşmaktadır. ISO bu katmanları ortak noktalarına ve kendi işlevlerine göre sınıflandırmıştır. OSI modelinin yapısında protokol katmanları vardır.

Fiziksel Katman

OSI referans modeli içinde tanımlanmış ilk katmandır. Görevi ise verilerin haberleşme kanalları boyunca sayısal veriler (bit) olarak iletilmesidir. Üst katmandan gelen sayısal paketleri kablolu veya kablosuz iletişim araçlarıyla ağ ortamına, ağdan gelen sayısal paketlerini ise üst katmana aktarma görevi yapar. Ethernet buna tipik bir örnektir. Üst katmandan 0 ve 1 olarak gelen sayısal verileri elektriksel sinyallere çevirir. Kablolar, hub, repeater cihazları bu katmanda yer alırlar

Veri Bağlantı (Data Link) Katmanı

Fiziksel katman sadece iletim ortamından gelen sinyalleri 0 ve 1'den oluşan bitlere çevirir. Fiziksel katman bitleri yorumlayamaz. Veri bağlantı katmanı gelen bitlerin anlamını yorumlar. İletişim kurulmak istenen bilgisayarın donanım adresini (MAC Adres) kullanarak iletişim kurar. Bilgisayar ağlarında kullanılan köprüler bu katmanda tanımlıdır. Adresleme için, MAC adresi, Unicast adresi, broadcast adresi ve multicast adresi örnek olarak verilebilir. Bu katman kullanılan protokollere HDLC, PPP, ATM, Frame Relay örnek verilebilir.

Ağ (Network) Katmanı

Bu katman bir paketin yerel ağ içerisinde ya da diğer ağlar arasında ki hareketini sağlayan katmandır. Bu hareketin sağlanabilmesi için hiyerarşik bir adresleme yapısı gerekmektedir. Gelişen teknolojiyle birlikte mevcut ağlarında büyüme eğiliminde olması adresleme yapısının hiyerarşik olmasını gerektirmektedir. Ayrıca hiyerarşik sistem dataların hedef bilgisayara en etkili ve en kısa yoldan ulaşmasını da sağlar. Bu katmanın bir özelliği olan Adresleme sayesinde

bu sağlanabilmiştir. Adresleme Dinamik ya dastatik olarak yapılabilir. Sabit adresleme el ile yapılan adreslemedir. Dinamik adresleme de iseotomatik olarak ip dağıtacak örneğin DHCP gibi bir protokole ihtiyaç vardır.

Ayrıca bu katmanda harekete geçen bir datanın hedefine ulaşabilmesi için en iyi yol seçimi de yapılır. Bu işleme Routing bu işlemi yerine getiren cihaza ise Router diyoruz. Router en basit tarif ile en iyi yol seçimini yapar ve broadcast geçirmediği için ağ performansını olumsuz etkilemez.

İletişim Katmanı

İletişim katmanının görevi, verilerin güvenli bir şekilde iletimini sağlamasıdır. İletişim katmanı üst katmanlardan gelen veriyi ağ paketi boyutunda parçalara böler. UDP, TCP ve ICMP gibi protokoller bu katmanda çalışır. Bu protokoller hata kontrolü gibi görevleri de yerine getirir.

Oturum Katmanı

Oturum katmanı, bir bilgisayar birden fazla bilgisayarla aynı anda iletişim içinde olduğunda, gerektiğinde doğru bilgisayarla yönlendirme yapar. Örneğin A bilgisayarı B üzerindeki yazıcıya yazdırırken, C bilgisayarı B üzerindeki diske erişiyorsa, B hem A ile olan hem de C ile olan iletişimini aynı anda sürdürmek zorundadır. Bu katmanda çalışan NET BIOS ve Sockets gibi protokoller farklı bilgisayarlarla aynı anda olan bağlantıları yönetme imkânı sağlar. Örnek olarak SMTP'yi (Simple Mail Transfer Protokol – Yalın Elektronik Posta İletim Protokolü) verebiliriz.

Sunum Katmanı

Sunum katmanının en önemli görevi yollanan verinin karşı bilgisayar tarafından anlaşılabilir halde olmasını sağlamaktır. Böylece faklı programların verilerini kullanabilmesi mümkün olur. Ayrıca sunum katmanı uygulama katmanında iletilen verilerin formatlarını tanımlar.

Uygulama Katmanı

OSI modelinin en üst katmanı olan uygulama katmanı kendisine sağlanan imkânları kullanarak protokoller ve uygulamalar oluşturulmasını sağlar. Kullanıcı düzeyinde OSI modelinde bulunan yapılara erişimi sağlar.

Katman	Kapsam & Protokoller
7. Uygulama	DNS, HTTP, FTP, SMTP, SNMP, TelNet
6. Sunum	MIME, SSL, TSL
5. Oturum	NamedPipes, NetBIOS, SAP
4. Taşıma Katmanı	TCP, UDP
3. Ağ Katmanı	IP, ICMP, IGMP
2. Veri Bağlantısı	MAC, ARP
1. Fiziksel Katman	Donanım; ethernet, fiber optik, token ring…

IP Adress ve Network Adress

Bilgisayar ağlarının oluşturulması sırasında yapılması gereken ilk görev ağ üzerinde bulunan tüm noktalara internet adreslerinin atanmasıdır. IP adreslerinin atanması çok kolay bir işlem olmasına karşın aynı adresin birden fazla bilgisayarda olmaması gerekir. Bununla birlikte IP adreslerinin ağ üzerinde bulunan diğer birimlerle tutarlılık göstermelidir.

Bir IP adres bilgisayarların anlayacağı 32-bitlik ikili sayı sisteminden oluşur. Bununla birlikte ikili sayı sistemini yorumlamak zordur. Bunun için 32 bitlik IP adres, 8 bitten oluşan dört bölüme ayrılmıştır. Her bir bölüm 0'dan 255'e kadar ondalık sayılardan oluşur. Bazı IP adreslerini network adresi ve Broadcast adresi olduğu için kullanamayız.

Broadcast adres; bilgisayarlar birbirleriyle iletişim kurmak için MAC adreslerine ihtiyaç duyarlar. Bunun için data link katmanında hazırlanan ethernet paketin hedef bölümüne 11111111 değeri (hegzadesimal FF) atanır. Bunun anlamı bu paket broadcast'tir ve ağdaki tüm bilgisayarlar bu paketi almak zorundadır. Bu paketle bilgisayar şu mesajı verir, "eğer IP adresin 10.1.8.10 ise bana MAC adresini bildir." Bu mesaj ağdaki tüm bilgisayarlara ulaşır. Her bilgisayar Broadcast mesajını alır ve inceler, eğer kendi IP adresi sorulan IP ise, MAC adresini Broadcast'i yollayan network kartına bildirir. Yoksa paketi imha eder.

Broadcast adresi: Broadcast teriminin anlamı, data paketinin bir noktadan diğer tüm noktalara belirtilen network üzerinden dağıtılmasıdır. Bu adres özellikle broadcasting için kullanılır.

	1st octet	2nd octet	3rd octet	4th octet
172.0.0.0	Network	Host	Host	Host
Subnet Mask: 255.0.0.0 or /8	255	0	0	0
192.4.0.0	Network	Network	Host	Host
Subnet Mask: 255.255.0.0 or /16	255	255	0	0
192.168.1.0	Network	Network	Network	Host
Subnet Mask: 255.255.255.0 or /24	255	255	255	0

	1st octet	2nd octet	3rd octet	4th octet
172.0.0.0	Network	Host	Host	Host
Subnet Mask	11111111	00000000	00000000	00000000
192.4.0.0	Network	Network	Host	Host
Subnet Mask	11111111	11111111	00000000	00000000
192.168.1.0	Network	Network	Network	Host
Subnet Mask	11111111	11111111	11111111	00000000

İlk şekilde subnet masklar ikinci şekilde o subnet masklarin Binary gösterimi mevcut. İlk resimdeki /8, /16, /24 gibi ifadeler görüyorsunuz. Bunlar Subnet Maski ifade eder, daha doğrusu Subnet Maskın Binary gösterimi içindeki toplam 1 sayısıdır.

Ornek Bazi Binary gosterimler:

```
192.168.1.0         11000000.10101000.00000001.00000000
255.255.255.0       11111111.11111111.11111111.00000000
192.168.1.255       11000000.10101000.00000001.11111111

192.168.0.0         11000000.10101000.00000000.00000000
255.255.0.0         11111111.11111111.00000000.00000000
192.168.255.255     11000000.10101000.11111111.11111111

192.168.0.0         11000000.10101000.00000000.00000000
255.255.255.0       11111111.11111111.11111111.00000000
192.168.0.255       11000000.10101000.00000000.11111111
```

Bir networkteki ilk ip adresi o networkün network adresini ve son ip adresi de Broadcast adresidir. Bu adresler network cihazlarına atanamaz.

Network Address		Subnet Mask	Broadcast Address
172.0.0.0		255.0.0.0	172.255.255.255
172.0.0.1	ve	172.255.255.254	
172.16.0.0		255.255.0.0	172.16.255.255
172.16.0.1	ve	172.16.255.254	
192.168.1.0		255.255.255.0	192.168.1.255
192.168.1.1	ve	192.168.1.254	
192.168.0.0		255.255.0.0	192.168.255.255
192.168.0.1	ve	192.168.255.254	
192.168.0.0		255.255.255.0	192.168.0.255
192.168.0.1	ve	192.168.0.254	

TCP/IP

TCP (Transmission Control Protocol), IP ise (Internet Protocol) ifadesinin kısaltmasıdır. Bilgisayar ağları alanında, TCP/IP en iyi ve en yaygın olarak kullanılan protokoldür. TCP, güvenilir ve sanal devre üzerinden çalışan bir protokoldür. Aynı ağ üzerinde ya da farklı ağlar üzerinde iki hostların birbirleriyle güvenilir bir şekilde haberleşmesini sağlar.

TCP 'nin başlıca Özellikleri:

- Bir bağlantının (connection) kurulması ve sonlandırılması
- Güvenilir (Reliable) paket dağıtımının sağlanması
- Akış kontrolü (flow control) olanağı ile hostlarda veri taşmasının (overflow) önlenmesi
- Bozulmuş ya da ikilenmiş verinin düzeltilmesi (error recovery)
- Alıcı host içerisinden birçok uygulama arasında demultiplexing yapılması

TCP, internet ortamında sağlar işlevler:

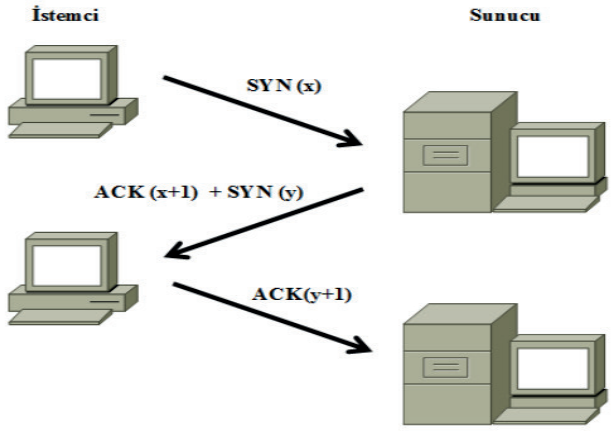
- Temel Veri Aktarımı(Basic Data Transfer)
- Güvenilirlik (Reliability)
- Uçtan uca Akış Kontrolü (End to end flow control)
- Çoğullama (Multiplexing)
- Bağlantılar (connections)
- Tam çift yönlü işlem (full duplex process)

TCP bağlantısının kurulması üç aşama (Three Way Handshake) sonucunda gerçekleşir:

1.Aşamada: Kaynak host bağlanmak istediği hosta bir istek paketi gönderir. Bu paketin TCP bağlantısında SYN = 1 ve ACK = 0 'dır. Gönderdiği paket içindeki segmente ait sıra numarası X'tir.

2.Aşamada: Bu paketi alan hedefe TCP bağlantısında SYN = 1, ACK = 1 bitlerini kurarak kendi paketini sıra numarasına SEQ Numarası=Y ve onay numarası, ACK Numarası = (X + 1) 'i gönderir.

3.Aşamada: isteğine karşılık bulan istemci son aşamada hedefe onay paketi gönderir ve bağlantı kurulmuş olur. Sonra kaynak, hedefe göndermek istediği veri paketlerini gönderir.



TCP ve UDP üst protokollerle bağlantıda portları kullanırlar. 65535 adet port vardır ve IANA (Internet Assigned Numbers Authority) ilk 1024 portu Well-known portlar olarak ilan etmiştir.

Well-Known Port	Application	Protocol
20	File Transfer Protocol (FTP) Data	TCP
21	File Transfer Protocol (FTP) Control	TCP
23	Telnet	TCP
25	Simple Mail Transfer Protocol (SMTP)	TCP
69	Trivial File Transfer Protocol (TFTP)	UDP
80	Hypertext Transfer Protocol (HTTP)	TCP
110	Post Office Protocol 3 (POP3)	TCP
194	Internet Relay Chat (IRC)	TCP
443	Secure HTTP (HTTPS)	TCP
520	Routing Information Protocol (RIP)	UDP

UDP (User Datagram Protocol)

UDP, TCP / IP protokol grubunun iki aktarım katmanı protokolünden birisidir. UDP, onay (acknowledge) gönderip alacak mekanizmalara sahip değildir. Bu yüzden veri iletiminde başarıyı garantileyemez. Yani güvenilir bir aktarım servisi sağlamaz. Uygulamalar güvenli ve sıralı paket dağıtımı gerektiriyorsa UDP yerine TCP protokolü tercih edilmelidir. Bazı UDP port numaraları; Who is: 43, DNS: 53, NTP: 123, SNMP: 161

ICMP (Internet Control Message Protocol)

ICMP (Internet Control Message Protocol) paketinin kullanım amacı şunlardır.

• TTL (yaşam) süresi dolduğu zaman paketin sahibine bildirim yapılması

• Herhangi bir durumda yok edilen paket hakkında bildirim sağlanması

• Parçalanmasın komutu verilmiş paket parçalandığında geri bildirim sağlanması

• Hata oluşumlarında geri bildirim sağlanması

• Paket başka bir yoldan gideceği zaman geri bildirim sağlanması

TFTP (Trivial File Transfer Protocol)

UDP tabanlı Cisco IOS tarafından desteklenen bir protokoldür. Router ve switch'lerde dosya transferi için kullanılır, daha az hafıza ve işlemci gücü gerektirir. UDP tabanlı olduğu için hızlı bir iletim söz konusudur fakat hata telafisi yoktur.

SMTP (Simple Mail Transfer Protocol)

Mail göndermek için sunucu ile istemci arasındaki iletişim şeklini belirleyen protokoldür. Sadece mail yollamak için kullanılan bu protokolde, basitçe, istemci bilgisayar SMTP sunucusuna bağlanarak gerekli kimlik bilgilerini gönderir, sunucunun onay vermesi halinde gerekli maili sunucuya iletir ve bağlantıyı sonlandırır.

SNMP (Simple Network Management Protocol)

SNMP protokolü ağlar üzerindeki birimleri denetlemek amacıyla geliştirilmiştir. Bir network cihazı üzerindeki sıcaklıktan o cihaza bağlı kullanıcılar, internet bağlantı hızından sistem çalışma süresine kadar birçok bilgi SNMP protokolünde tanımlanmış bir yapı içerisinde tutulur.

DHCP (Dynamic Host Configuration Protocol)

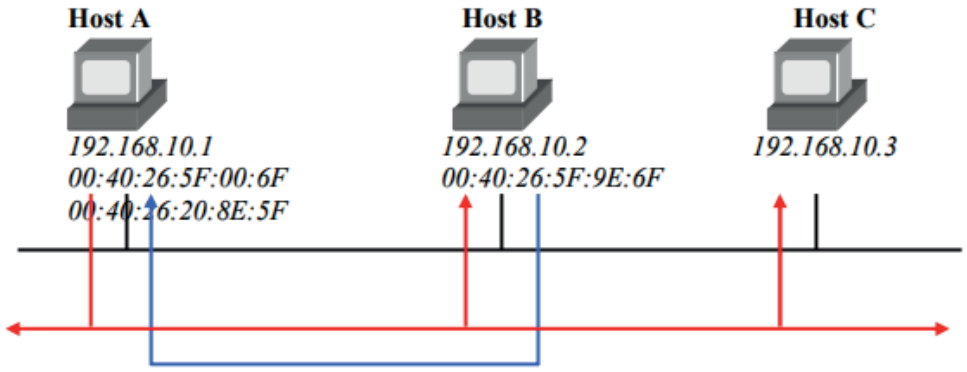
Bu protokol ile tam dinamik ip konfigürasyon dağıtımı yapabilir. Sunucu – istemci ortamında çalışırlar ve istemcilerde ip adreslerini otomatik olarak alacaklarına dair bir konfigürasyon yapılmalıdır. DHCP ile belirlenen ip adresleri, subnet masklar, dns server adresleri, varsayılan ağ geçidi gibi adresler dağıtılabilir, ip adresleri MAC adreslerine reserve edilebilir veya bazı ip adresleri tamamen kullanıma kapatılabilir. DHCP' den alınan ip adresleri DHCP server

tarafından istemciye belirli sürelerle kiralanır ve istemci belirli aralıklara ile DHCP serverdan kira süresini yenilemesini ister. Yenilenme kira süresine dolana kadar yapılamazsa DHCP server tarafından istemciye yeni bir ip adresi verilir.

Adres Çözümleme Protokolü (ARP)

ARP (Address Resolution Protocol) IP adresinden MAC adresi elde eden bir protokoldür. IP adresinden MAC adresi elde etmek için aşağıda gösterilen sıra izlenir. Örneğin, Host A (192.168.10.1) Host B (192.168.10.2) ile haberleşmek istemektedir.

- Host B'nin MAC adresini elde etmek için, Host A ARP istek paketini broadcast yapar.
- ARP istek paketi Host B'nin IP adresini (192.168.10.2) içerir.
- Host B ARP istek paketini alır. sonra Host B Host A'ya MAC adresinin bulunduğu ARP cevap paketini gönderir.



Sık sık tekrarlanan ARP paketleri network üzerinde yoğunluğa sebep olur. Bu problemi çözmek için her bilgisayar, IP adreslerinin ve MAC adreslerinin bulunduğu ARP tablosunu geçici bir süre hafızasında tutar. Bir host ARP tablosunda bulunana IP adresleri için ARP isteği yapmaz. MAC adresleri belli zaman aralıklarıyla ARP tablosundan silinir. İnternet katmanında hazırlanan ve hedef bilgisayarın IP adresini içeren veri paketi, MAC adres kullanılmadan data link katmanı üzerinden gönderilemez. Bu nedenle IP paket gönderilmeden önce internet katmanı hedef bilgisayarın MAC adresini sorar. Bunun için ARP istek paketi gönderilerek hedefin MAC adresini öğrenilir. Buna adres çözümleme denir ve ARP olarak isimlendirilir. ARP amacıyla kullanılan pakete ARP paket denir.

IP HESAPLARI VE SUBNETTING

TCP/IP protokolünde tüm bilgisayarlar 32 bitlik "özgün" bir IP numarasına sahip olacak şekilde adreslenirler.

IP adresleri sınıflara ayrılmıştır, bu sınıflar;

Class A: 0.0.0.0 - 127.255.255.255 arasındaki ip adresleri.

Class B: 128.0.0.0 - 191.255.255.255 arasındaki ip adresleri.

Class C: 192.0.0.0 - 223. 255.255.255 arasındaki ip adresleri.

Class D: 224.0.0.0 - 239. 255.255.255 arasındaki ip adresleri.

Class E: 240.0.0.0 – 255. 255.255.255 arasındaki ip adresleri.

Her ip sınıfının subnet maskıda belirlenmiştir buna göre;

A sınıfı için subnet mask: 255.0.0.0,

B sınıfı için subnet mask: 255.255.0.0,

C, D, E sınfları için subnet mask: 255.255.255.0 'dır.

Bazı ip aralıkları iç networkte kullanılmak üzere ayrılmıştır ve herhangi bir şekilde dış networkte (internette) kullanılamaz.

Bu ip aralıkları şunlardır:

10.0.0.0 – 10.255.255.255

172.16.0.0 -172.31.255.255

192.168.0.0 – 192.168.255.255

İnternet ortamında bu ip adresleri kesinlikle kullanılmaz, iç network kullanıcıları internete çıkarken, ISP tarafından sağlanan static veya dynamic bir ip adresine dönüşürler. İşte bu ip adresi tüm dünya da tek olacaktır.

Ip adreslerinin dağıtılması sırasında subnet maskların standar verilmesi ciddi sorunlara sebep olacaktı. Örneğin bir ISP firması söz gelimi 150 adet ip adresi almak istiyorsunuz. Bu durum standart subnet mask kullanılarak size verilebilecek minimum ip sayısı 255'dir. Daha vahim bir senaryo ise siz söz gelimi 500 tane ip adresi isteseniz ortaya çıkar çünkü o zaman size verilebilecek minimum ip sayısı 255*255 = 65025 ' dir. Bunun önüne geçebilmek için yapılabilecek tek şey ise subnet masklar ile oynamaktan geçer. Bu sayede networkler sub-networklere bölünebilir ve ip israfın biraz olsun azalabilir.

Örnek:

Elinizde adresi 192.168.1.0 olan C Class bir network var ve bunu 4 subnetworke bölmek istiyorsunuz;

Bu durumda 256/4 = 64 'er tane ip adresiniz olacak.

Subnet Maskın son oktetini 256-64 yaparsanız bunu gerçekleştirmiş olursunuz. Bu durumda subnet mask=255.255.255.192 olacaktır ve elimizde subnet maskı 255.255.255.192 ve network adresleri sırasıyla;
192.168.1.0
192.168.1.64
192.168.1.128
192.168.1.192

Olan 4 adet networkümüz, her networkte 64'er tane ip adresimiz olacak.

Bir networkün ilk ip adresi network adresini, son ip adresi broadcast adresini gösterdiği için kullanılamaz dolayısıyla bir networkte "useable" olarak adlandırılan, yani kullanılabilecek ip sayısı toplam ip sayısından 2 eksiktir.

Useable Ip sayısı = toplam ip sayısı – 2

Network adresleri örneğin /24 şeklinde gösterilebilirler. /24 ip adresinin binary yazılımında soldan sağa 24 tane 1 olduğu anlamına gelir. Bu şekilde yazılımına CIDR denir. (Classless)

Örneğin;

255.255.255.0 binary olarak
11111111.11111111.11111111.00000000 'e eşittir ve 24 tane 1 den dolayı /24 olarak gösterilebilir.

Yukarıdaki örneğimizdeki subnet mask ise binary olarak;
11111111.11111111.11111111.11000000 'a eşit olacak dolayısıyla /26 olarak gösterilebilecektir.

Örnekler:

Subnet Mask	Binary Yazılım	CIDR İfade
255.255.128.0	11111111.11111111.100000000.00000000	/17
255.255.255.128	11111111.11111111.111111111.01000000	/25
255.255.255.252	11111111.11111111.111111111.11111100	/30

Elimizde bir ip adresi ve onun subnet maskı varsa ikisinin binary yazılışını AND' leyerek network adresini bulabiliriz.

Örneğin elimizde subnet maskı 255.255.255.128 olan 192.168.1.141 gibi bir ip var.

192.168.1.141 = 11000000.10101000.00000001.10001101
255.255.255.128 = 11111111.11111111.11111111.10000000

AND (çarpıyoruz) = 11000000.10101000.00000001.10000000
Network Adresi = 192. 168. 1. 128

5. BİLİŞİM GÜVENLİĞİ (SİBER GÜVENLİK)

TEMEL SİBER GÜVENLİK KAVRAMLARI

Personelimiz; sahip olduğu Bilgi ve Bilgi varlıklarını; 2018 yılında alınan ISO-27001 Bilgi Güvenliği Standartları Belgesi, 657, 5651, 5237 ve 6698 sayılı yasalar gereği korumakla sorumlu tutulmuştur.

Personelimizin kendisine teslim edilen Bilgi ve Bilgi Varlıkları ile adına tahsis edilmiş ve Kuruluşumuz Bilgi Teknolojileri kaynaklarına erişim için kullandığı tüm hesapların muhafazası ve kullanım usul ve esaslarını kapsayan "Personel Bilgi Güvenliği Taahhütnamesi'ni imzalamaları ve İnsan Kaynakları Dairesi Başkanlığı tarafından bu taahhütnamelerin Personelin kişisel dosyalarında saklanmaları uygun görülmüştür.

Bilgi ve İletişim Teknolojileri, Ülkemizde ve Dünyada Kamudan Özel Sektöre, kritik altyapıların yönetimi ve idamesinden bireylerin kişisel kullanımına kadar birçok alanda ekonomik ve sosyal hayatın vazgeçilmez birer parçası haline gelmiştir. Bu teknolojiler bir yandan ülkeler için sürdürülebilir büyüme ve kalkınma yolunda anahtar rol oynarken, diğer yandan Siber Güvenlik Risklerini de beraberinde getirmektedir. Siber tehditler başta haberleşme, ulaşım, enerji, bankacılık, finans ve sağlık gibi kritik altyapılar olmak üzere tüm sektörleri olumsuz yönde etkileme potansiyeli taşımaktadır. Sayısı ve niteliği bakımından hızla artış gösteren siber tehditlerle mücadele kapsamında, Ulusal seviyede gerekli önlemlerin alınmasına yönelik stratejik hedeflerin belirlenmesi ve bu hedeflere ulaşmak için eylem planı hazırlanmış ve 2020/15 sayılı Cumhurbaşkanlığı Genelgesi ile Resmi Gazetede yayımlanarak duyurulmuştur.

Ulusal Siber Güvenlik Stratejisi ve Eylem Planında sektörümüz "Kritik Altyapı" olarak tanımlanmaktadır. Kuruluşumuz ana faaliyetleri kapsamında İşletme ve Seyrüsefer hizmetleri kritik öneme haiz operasyonel süreçleri ihtiva etmektedir. Bu operasyonel süreçlere yönelik siber saldırılar başta insan yaşamı olmak üzere Ülkemiz ve Kuruluşumuz ali menfaatlerine yıkıcı etkileri olan sonuçlar doğuracaktır.

Olası ve yıkıcı etkileri büyük siber saldırılara karşı koymak için Kuruluşumuz;

- 2019/12 Sayılı ve "Bilgi ve İletişim Güvenliği Tedbirleri" konulu Cumhurbaşkanlığı Genelgesi,
- 2020/15 Sayılı ve "Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" konulu Cumhurbaşkanlığı Genelgesi,
- 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla

İşlenen Suçlarla Mücadele Kanunu (Kuruluşumuz ilgi yasa kapsamında Yer Hizmet Sağlayıcısı olup bu konuda BTK tarafından belgelendirilmiştir),

- 6698 Sayılı Kişisel Verilerin Korunması Kanunu,
- 5809 Sayılı Elektronik Haberleşme Kanunu,
- Sektörel SOME ve USOM talimat ve yönergeleri,
- Sahip olduğumuz ISO 27001 Bilgi Güvenliği Yönetim Sistemi Sertifikası standartları,

gereği Bilgi ve İletişim Altyapısını güçlü ve güncel tutmaya gayret göstermektedir.

Güvenliğin her türünde olduğu gibi Bilgi ve İletişim Güvenliğinde de "tedbir alma ve karşı getirilmeli ve güncel tutulmalıdır.

TANIMLAR

Bilgi: Sizin için önemli olan, bu yüzden uygun şekilde korunması gereken varlıklardır.

Tehdit: Kuruluşa veya sistemlere zarar verebilecek istenmeyen bir olayın potansiyel sebebidir.

Zafiyet: Bir varlığa ya da kontrole ait, bir veya birden fazla tehdit tarafından sömürülebilecek zayıflıktır.

Risk: Bir zafiyetin bir tehdit tarafından kullanılması sonucu ortaya çıkacak olayın oluşma olasılığı ile yaratacağı etkinin birleşimidir.

Siber Güvenlik: Manyetik ortamda bulunan ve iletişim halinde olan her bilginin güvenliğidir. Siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesini,

Siber Ortam: Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan ortamı ifade eder.

Siber Güvenlik Olayı: Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesi veya teşebbüste bulunulmasıdır.

Kritik altyapılar: İşlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda,

- Can kaybına,
- Büyük ölçekli ekonomik zarara,
- Ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapıları kapsar.

Siber Güvenlik Olayı: Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesi veya teşebbüste bulunulmasıdır.

Hacker: Hacking olayını gerçekleştiren kişidir.

Bilgisayar Virüsü: Kullanıcının izni ya da bilgisi dahilinde olmadan bilgisayarın çalışma şeklini değiştiren ve kendini diğer dosyaların içerisinde gizlemeye çalışan bir tür zararlı bilgisayar programıdır. Virüsün temel iki görevi kendini çoğaltması ve kendini çalıştırmasıdır.

Solucan: Genellikle e-posta ile gönderilen ekler, çeşitli web siteleri ve ağ üzerinde paylaşılan dosyaları kullanarak yayılan zararlı yazılımlardır. Solucanlar, bir sistemi ele geçirdiklerinde, kullanıcının başka bir eylemine ihtiyaç duymadan, kullanıcının veri kaynaklarını kullanarak (e-posta adres listesi gibi) kendi kaynak dosyalarını hızlı bir şekilde diğer kullanıcılara da ulaştırmayı denerler ve bu yolla kendilerini çok fazla sayıda çoğaltabilirler. Solucanlar bunu yaparken kullanıcıların bant genişliklerini ve ağ kaynaklarını kullandıklarından ağların kilitlenmesine, e-posta sunucularının aşırı yüklenmesine veya web kaynaklarına erişim hızının düşmesine sebep olabilmektedirler.

Truva atı: Zararlı kod içeren yazılım demektir. Örneğin: "ücretsiz pdf dosya okuyucu yazılımını yükleyin" gibi bir ifade ile karşılaştığınızda bilinen pdf okuyucular dışındaki bir yazılım sizi bu tuzağa çekebilir.

Ransomware (Fidye Yazılımları): Fidye yazılımı, şantaj yazılımı veya fidye virüsü olarak bilinen yazılımlardır. Ransomware bulaştığı bilişim sistemleri üzerinde dosyaları erişimi engelleyerek kullanıcılardan fidye talep eden zararlı yazılımlardır.

Sektörel SOME (Siber Olaylara Müdahale Ekibi): Ulusal Siber Güvenlik Stratejisi ve Eylem Planı kapsamında kritik altyapı sektörü düzenleyici/denetleyici kurumlarında kurulması zorunlu kılınmış yapılardır. Bu ekiplere temel;

- Sektörleri kapsamında alınması gereken siber güvenlik önlemlerini belirleme,
- Siber güvenlik mevzuatları oluşturma,
- Mevzuatlar kapsamında denetimler gerçekleştirme görevleri verilmiştir.

Kurumsal SOME(Siber Olaylara Müdahale Ekibi): Faaliyet gösterdikleri sektörlerin Sektörel SOME'leri tarafından zorunlu kılınan siber güvenlik önlemlerini işletmelerinde almak/aldırmak ile görevli ekip.

Varlık: Bir kurum için değeri olan ve bu nedenle uygun olarak korunması ve işletilmesi gereken fiziksel ve dijital tüm unsurlardır.

Kişisel Veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi ifade eder.

LOG YÖNETİMİ

Özellikle de siber saldırıların tespiti ve olay yönetimi için loglama kritik önem taşımaktadır. Bir siber saldırının tespiti ve aydınlatılması için log kayıtları siber güvenlik uzmanları tarafından incelenerek ortaya çıkartılır. Log kayıtları siber saldırının niteliğinden, güvenlik açığının tespitine kadar birçok noktada siber güvenlik uzmanlarına yön gösterir nitelikte olmalıdır.

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlemesine Dair Usul ve Esaslar Hakkındaki Yönetmelik Kanunu, ISO 27001 gibi bilişim sektörünün en önemli kanun ve standartları log tutmayı esas zorunluluk olarak şart koşmaktadır.

5651 sayılı kanun gereğince ve Telekomünikasyon İletişim Başkanlığı yönetmelikleri gereği her kurum, bu erişim kayıtlarını tutmakla yükümlüdür. Aynı zamanda tutulan log kayıtları için en az iki yıl saklamakla yükümlüğü getirilmiştir.

Yasanın çıkarılmasının iki temel amacı bulunmaktadır. Birincisinde içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumluluklarını belirlenirken İkinci esasta İnternet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usulleri düzenlemektir.

5651 sayılı kanın kurumunuzun güvenliği için zorunlu kılınmıştır. Bir siber suç işlendiği takdirde log kaydı tutmayan bir Kurum bu suçtan sorumlu olur. Eğer log kaydı tutuluyorsa internete kim, hangi saat ve tarihte, hangi IP adres ile bağlandığı ortaya çıkartılarak işletmenizin sorumluluğunu ortadan kaldırır. Bu sayede siber suçlar tespit edilerek doğru kişiler yargılanır. Aksi takdirde altını çizerek belirtmek isteriz ki, bu hizmeti veren kurum ya da kuruluş sorumlu tutulur.

Kurumsal iş ortamlarında yaşanan siber saldırıların tespiti için ülkemizde 5651 sayılı kanun yürürlüğe girmiş ve uygulanma zorunluluğu konulmuştur. Kurumların en önemli güvenlik projelerinden biri olan log toplama, log yönetimi ve analizi siber güvenlik uzmanlarının olmazsa olmazlarımız arasına girmiştir.

FİZİKSEL GÜVENLİK UNSURLARI

Siber tehditler denince akla ilk gelen tehdit aktörlerin dijitale dayalı olması, tehditlerin dış dünyada da var olduğu gerçeğinin göz ardı edilmesine yol açmaktadır.

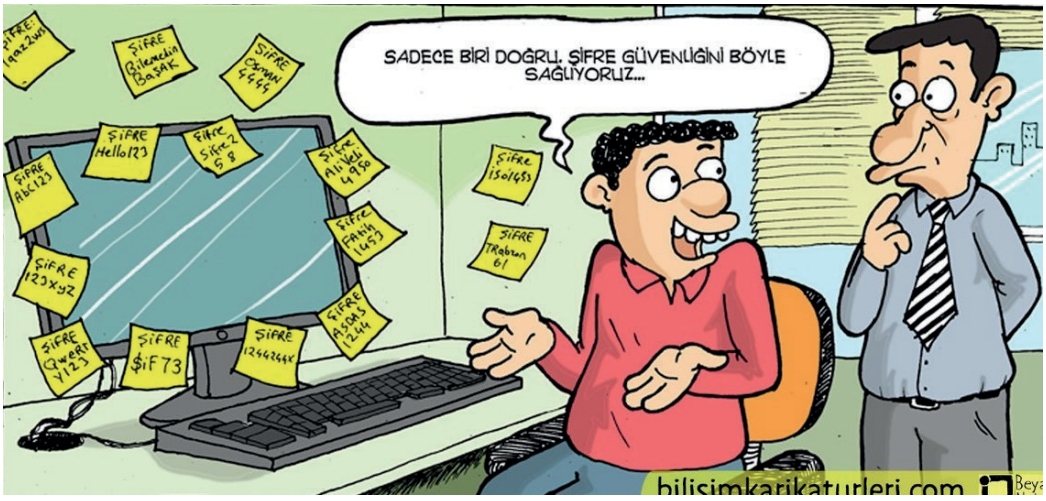
Araştırmalar her beş veri sızıntısından birinin siber saldırılardan, her dört veri sızıntısından birinin ise cihaz kaybı veya çalınmasından kaynaklandığını ortaya koymakla birlikte, etkili bir veri koruma stratejisinin önemli bir bileşenini oluşturan fiziksel güvenliği kötü niyetli yazılımlarla savaşmak gibi problemler nedeniyle arka plana atan şirketler, cihazlarını ve verilerini kaybederek kriz yaşadığı sıklıkla görülmektedir. Siber saldırılar kadar, ofisin ön kapısından içeri giren ya da havaalanının kafesinde bulunan bir çalışanın yanında oturan herhangi bir kişinin de büyük bir tehdit olabileceği ihtimali göz ardı edilmemelidir.

Kapı ve Geçişler: Saldırganların, yemek molaları, vardiya değişimleri veya kısa aralar gibi zamanları öğrenerek büyük bir insan kalabalığı arasında dikkat çekmeden hedeflerine sızabildiği bilinmektedir. Bu kapsamda kurum/kuruluş içi kısımların geçiş güvenliğini öncelik sırasıyla belirleyerek ona göre güvenli bir insan akışı sağlamak ve çalışanlar ile ziyaretçilere ait giriş çıkış kartları vermek gibi uygulamalar belirlenmesi ve söz konusu risklerin azaltılması gerekmektedir.

Çalışanlar Tarafından Unutulan Cihaz ve Yazılı/Dijital Dokümanlar: Teknolojinin gelişmesi sonucu yaşadığımız bu dijitalizasyon çağında kullanmakta olduğumuz akıllı telefon, cep telefonu, laptop benzeri mobil cihazlar ve unutulan yazılı/dijital veriler kurum/kuruluş ve şahıslar açısından ciddi anlamda güvenlik zafiyeti oluşturabilmektedir. Umuma açık yerlerde unutulan mobil cihazlar ve yazılı/dijital dokümanların tehlikeli kişilerin eline geçme olasılığına karşı gerekli önlemleri almak kurum/kuruluşlarda görev yapan çalışanlarındır.

Temiz Masa Temiz Ekran ve Bilgisayar Ekranlarının Kitlenmesi: Çalışanlar, çalışma ortamlarında olmadıkları süre içinde bilgisayar ekranlarını kitlemeli ve parola, yazılı doküman

vb. gibi yetkisiz erişim sağlanması halinde kurum/kuruluşlar açısından ciddi güvenlik riski oluşabilecek hiçbir dijital/yazılı bilgiyi çalışma ortamlarında erişime açık halde bırakılmamalıdır.



Zayıf Parola Kullanımı ve Parola Paylaşımı: Çalışanların kurum/kuruluşları tarafından belirlenen parola güvenliği standartlarına uymaları ve hiçbir şart altında kullandıkları parolaları çalışma arkadaşları ile paylaşmamaları gerekmektedir.

Aynı parolanın farklı hesaplarda kullanılması güvenlik zafiyeti oluşturabilir. Bu nedenle; çalışanlar iş hayatlarında kullandıkları mail Kurumsal mail hesaplarını ve parolalarını sosyal medya vb. ortamlarda kullanmamalıdır.

SOSYAL MÜHENDİSLİK VE SON KULLANICILARA YÖNELİK DİĞER TEHDİTLER

Sosyal mühendislik, insanların zafiyetlerinden faydalanarak çeşitli ikna ve kandırma yöntemleriyle istenilen bilgileri elde etmeye ve/veya işlemleri yapmaya çalışman saldırı türlerinin tamamını kapsayan saldırı çeşididir.

Saldırgan hedeflerinden bilgi elde etme ve/veya bir aksiyon alarak sonucunda kendisinin ve/veya kurumunun zarar görmesini amaçlar. Sosyal mühendislik için saldırganlar tarafından en etkin kullanılan yöntem eposta ve telefondur.

Saldırganların hedefleri kurumunuzda çalışan Sistem yöneticileri, üst düzey yöneticileri, IT çalışanları ve diğer yardım sever personeller yani siz dahil herkes olabilir !!!

Sosyal Mühendislik Saldırıları Neden etkilidir?

- İnsan güvenlik zincirindeki en zayıf ve şüpheli faktördür.
- Bu tarz saldırıları tespit etme diğerlerinden daha zordur.
- Bu ataklardan tamamen kurtulmak için bir metot bulunmamaktadır.
- Bu tür siber atakları %100 engelleyen donanım veya yazılım çözümü bulunmamaktadır.

Sosyal Mühendislik Saldırı Fazları Nelerdir?

1. Hedef Firma Hakkında Araştırma Yapılması(Çöp karıştırma, Web sitesi, Linkedn, Facebook vb.)
2. Kurbanın Belirlenmesi
3. Kurban ile ilişki kurulması ve geliştirilmesi(E-mail, telefon, yerinde ziyaret vb.)
4. İlişkinin saldırgan tarafından istismar edilmesi

Başlıca Sosyal Mühendislik Saldırı Çeşitleri

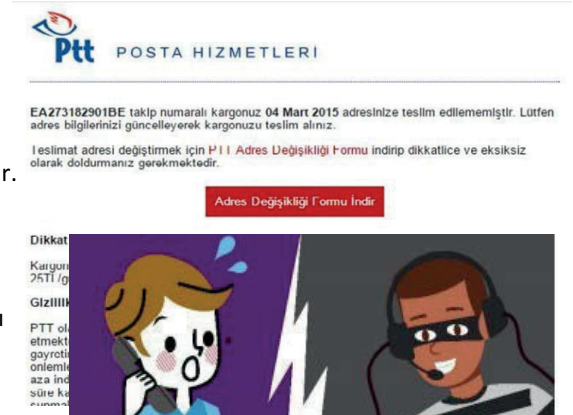
Phishing(Oltalama) Mailleri

Phishing Mailleri; saldırgan tarafından önceden hazırlanmış bir senaryo ile hedefi emailin güvenilir bir kaynaktan geldiğine inandırıp kendisine zarar verecek bir aksiyon almasını sağlamaya çalışan saldırı türüdür.

-En yaygın kullanılan saldırı türüdür.

-Çok yüksek teknik bilgi gerektirmediği için saldırganlar tarafından oldukça sık tercih edilmektedir.

-Bilgi işlem tarafından donanımsal ve yazılımsal belli başlı önlemler alınabilse de bu atak türünü %100 engellemek mümkün değildir.



Telefon ile Oltalama(Phone Phishing)

-Bu saldırı türünde saldırgan hedefi ile telefon yardımı ile iletişime geçerek istediği aksiyonları aldırmaya çalışır.

Sivil Havacılık Genel Müdürlüğü tarafından 2018 yılı içerisinde gerçekleştirilen 1.Havacılık Sektörü Siber Güvenlik Tatbikatında telefon ile oltalama saldırıları %75 oranında başarı ile en yüksek zafiyet olduğu tespit edilen saldırı çeşidir. Bu saldırı türünü %65 oranında başarı ile phishing mailleri takip etmektedir.

Omuz Sörfü

-Günlük hayatın her anında karşılaşılması mümkün bir saldırı türüdür.

-Gizli Bilgi, erişim kısıtlı sistem ve/veya varlıklara erişim sırasında kurbanın izlenmesi ve saldırgan tarafından bilgi edinilmesi yöntemidir.

Baiting

Bu tür sosyal mühendislik saldırısında saldırgan hedefinde kurbana cazip gelecek bir yem ile hedefe zarar vermeye çalışır. Örneğin; Saldırgan hedef veya hedeflerinin bulunduğu bir yere usb bırakarak hedefleri kandırıp bilgisayarlarına zararlı bir yazılım yüklemelerine sebep olabilir.

ABD tarafından İran Nükleer programına yönelik yapıldığı iddia edilen Stuxnet saldırısı bir baiting sosyal mühendislik saldırısıdır. Basit bir usb ile ne kadar büyük bir zarar verilebileceğinin en güzel göstergesidir.

Quid Pro Quo

-Örneğin; Kötü niyetli bir şahıs, BT hizmeti olduğunu iddia eden çeşitli BT şirketlerini arar ve kendini BT departmanından bir çalışan olarak tanıtır. En sonunda saldırgan, sunulan hizmeti gerçekten gerektiren bir çalışan veya şirketle karşılaşacak ve hedefi için saldırısına devam edecektir.

SON KULLANICILAR TARAFINDAN ALINMASI GEREKEN ÖNLEMLER

1. Kaynağı Değerlendir: Son Kullanıcılar buldukları bir usb'yi bilgisayarlarına takmadan ya da kendilerine gelen şüpheli buldukları bir e-mail ekindeki dosyayı açmadan önce kaynağı değerlendirmelidir. Şüpheli bir durumda aksiyon almamalı ve ivedi bir şekilde Kurumsal SOME ekipleri ile irtibata geçmelidir.
2. Sakin Ol: Saldırganlar genellikle hedeflerini telaşa düşürerek yapmamaları gereken bir eylemi gerçekleştirmeye çalışırlar. Bu yüzden son kullanıcılar olası bir siber saldırı karşısında sakin olmalıdır.
3. Gerçek olamayacak kadar güzelse: Bir Nijerya Prensi sizinle irtibata geçip yardım istiyorsa bir siber saldırıya kurbanı olarak seçilmiş olmanız kuvvetle muhtemeldir.
4. Antivirüs Kullanımı: Laptop, cep telefonu, tablet gibi mobil cihazlarda kullanıcıların bir antivirüs programı bulundurması ve söz konusu bu antivirüs programının güncel tutulması önemlidir.
5. Şüphe Duy: Sosyal Mühendislik saldırılarına karşı alınabilecek en güzel önlem risklerin farkında olarak her daim tetikte olmaktır.

SOSYAL MEDYA KULLANIMI

Sosyal Medya kişilerin internet üzerinde yaptığı diyaloglar ve paylaşımların bütünüdür. Bu platformlarda gerçekleşen diyaloglar ve paylaşımlar arttıkça bu tür içerikler bir değer haline gelmekte ve bilgi toplama amacı ile saldırganlar tarafından kullanılmaktadır.

-Sosyal Medya hesaplarınız üzerinden saldırganlar tarafından bilgi toplanarak phishing türü saldırılar için kullanılabilir.

-Sosyal Medya hesaplarınız ele geçirilerek şahsınızı ve kurumunuzu etkileyecek paylaşımlar yapılabilir.

-Lokasyon tespitiniz yapılabilir.

Sosyal Medya Hesaplarının Güvenliği Nasıl Alınır?

- Kurum ile ilgili hiçbir detay, bilgi, belge ve paylaşım yapılmamalıdır. Şirketin kurumsal bilgi güvenliği politikasına uygun hareket edilmelidir.
- Gelen direk mesajlara kesinlikle tıklanmamalıdır. (t.co/adres gibi benzeri bağlantıların sizi nereye gönderdiğini bilemezsiniz.)
- Takipçi sayılarını artırmak için servislere hesabınız üzerinde gereksiz haklar verilmemelidir.
- Hesaplara erişimi olan uygulamaları kontrol ederek risk yaratabilecek uygulamalara erişim izni verilmemelidir.
- Kurumunuz ve işleriniz ile ilgili fotoğraf, bilgi-belge, konum gibi paylaşımlarda bulunulmamalıdır. Bu bilgiler aleyhinizde kullanılabilir ve arama motorları bu verileri indekslenmektedir.
- Kimlik bilgileri paylaşılmamalı ve doğru bilgiler verilmemelidir.
- Sosyal platformların telefon rehberine veya maildeki kişilere ulaşarak sizin adınıza paylaşımlar yapmasına izin verilmemelidir.
- Şifremi unuttum sorusu için alakasız sadece sizin bileceğiniz bir cevap seçilmelidir. Örneğin ne zaman doğdun sorusunun cevabı doğum tarihiniz olmamalı bu soruya alakasız başka bir cevap verilmelidir.
- Sosyal medya hesaplarından özel bir konuyu, kişiyi veya olayı hedef alan yorum ve yazılardan kaçınması tavsiye edilmektedir.

MOBİL CİHAZLARIN GÜVENLİĞİ

Mobil sistemlerin yaygınlaşması ve akıllı cep telefonlarının yoğun kullanımı hackerların dikkatini bu yöne çekmektedir.

Mobil Cihaz Güvenliğinde Dikkat Edilmesi Gereken Hususlar

- Mobil Cihazlar üzerine kurulan programların gereken kaynak ve izinden fazlasına erişim hakkı talep etmemesine dikkat edilmelidir.
- Arka planda çalışan yazılım ve servislerin incelenmelidir.
- Güvenlik ayarları üzerinden bilinmeyen kaynaklı yazılım ve servislerin yüklenmesi engellemelidir.
- İşletim sistemi güncel tutulmalıdır.

- Mobil cihaz üzerinde güncel bir antivirüs kullanılmalı ve periyodik olarak tarama yapılmalıdır.
- Bir uygulama indirilmeden mobil market üzerinde uygulama yayıncısının doğrulaması yapılmalıdır.
- Kurumsal bilgiler ve dökümanlar mobil sistemlerde şifreli olarak tutulmalıdır.
- Mobil Cihazlar üzerinden bilinmeyen ağlar kullanılarak internete çıkılmamalıdır.
- Mobil cihazlarda Root ve jailbreak yapılmamalıdır.

HAVACILIK SEKTÖRÜNE YÖNELİK GÜNCEL SİBER TEHDİTLER VE SALDIRI ÖRNEKLERİ

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı tarafından kritik bir altyapı sektörü olarak belirlenen havacılık sektörümüz özellikle geçtiğimiz son 5 senede giderek artan oranda siber saldırı ve risklerin tehdidi altındadır. Bu saldırılara örnek olarak;

- Cathay Pasific Airways'in 9.4 milyon müşteri kişisel verisinin internete sızdırılması

- Petya Yazılımı Nedeniyle Hizmet Kesintisi Yaşanması

- 2016 Yılında Vienna Havalimanına Yönelik yapılan DDoS saldırısı sonucu yaklaşık 1 gün iş kesintisi yaşanması verilebilir.

September 7, 2016

Austrian officials investigate attempted cyberattack of Vienna's airport

Jeremy Seth Davis

Austria's Interior Ministry is reportedly investigating a hacking group known as 'Aslan Neferler Tim' that has claimed responsibility for an attempted cyberattack of Vienna's airport.

The hacking group, also known as 'Lion Soldiers Team,' announced this weekend that the group attacked the airport in response to the "racism" of airport officials, according to a Google translation of the Turkish-language tweet.

The tweet referred to an incident involving a grounded flight in which officials declined to issue

SİBER GÜVENLİK İHLAL DURUMLARI VE KURUMSAL SOME SİBER OLAY ACİL DURUM PROSEDÜRLERİ

Olası bir siber saldırıya maruz kalınması halinde paydaşların bu duruma karşı hazırlıklı olması ve alınacak aksiyonların önceden bilinerek hızlı bir şekilde reaksiyon verilmesi hayati derecede önemlidir.

Havacılık Sektörü çalışanları işletmelerinin Siber Güvenlik/ Bilgi Güvenliği prosedürleri gereği olası bir siber olayı fark etmeleri durumunda gerekli önlemlerin alınabilmesi için işletmelerine bildirimde bulunmakla yükümlüdür. Bu nedenle çalışanların işletme siber olay müdahale ve bilgi güvenliği prosedürlerini bilmeleri ve olası bir siber güvenlik olayında bu prosedürlere uygun şekilde nasıl İşletme Kurumsal SOME ekibi ile iletişime geçeceğini bilmeleri gerekmektedir.

Şüpheli Olay İle Karşılaşıldığında İletişime Geçilecek Kurumsal Mailler:

- ✓ Herhangi bir şüpheli veya fiili bilgi güvenliği politikası veya sistem ihlali derhal **some@dhmi.gov.tr** adresine bildirilmelidir.
- ✓ Kuruluşumuzda Kişisel Veriler Anlamında herhangi bir ihlal tespit edildiğinde **kvk@dhmi.gov.tr** mail adresine bildirimde bulunulur.
- ✓ Oltalama Mail ile karşılaşıldığında **BlackList@dhmi.gov.tr** mail adresine bildirimde bulunulur.

Kuruluşumuz Ağına Uzaktan (Vpn) Erişim:

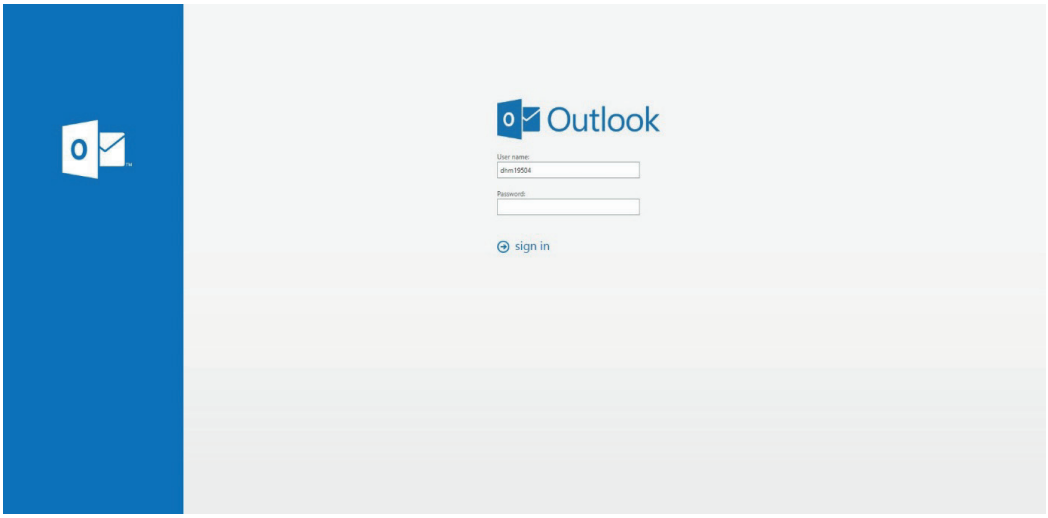
Kuruluşumuz ağına uzaktan bağlantı yaparak Kuruluşumuz sistemlerimize (Dhmi Online, Uçuş Bilgi v.b) herhangi bir yerden erişim sağlayabilirsiniz.

Uzaktan Erişim için Tarayıcınız ile https://durbin.dhmi.gov.tr adresine girdikten sonra;
-Username bölümüne dhm(Sicil No) giriniz (ÖRN: dhm21180)
-Password bölümüne Parolanızı girin (Kurum Bilgisayarınızın Oturum Açma Şifrenizi girin) ve LOG IN butonuna basınız ve Global Protect programını kurarak erişim sağlayabilirsiniz.
Uzaktan erişimle ilgili ayrıntılı dokümanlara Kurumsal web sitemiz üzerinde bulunan Eğitim Dokümanları sayfası altında bulabilirsiniz. https://dhmiportal.dhmi.gov.tr/Sayfalar/EgitimDokumanlari.aspx?RootFolder=%2FSiteCollectionDocuments%2FOrtak%2FEgitimDokumanlari

Kurumsal E-posta hesabınıza erişim:

Kurumsal e-posta hesabınıza (OWA) herhangi bir yerden erişim sağlayabilirsiniz.

Kurumsal e-posta hesabınıza erişmek için Tarayıcınız ile https://eposta.dhmi.gov.tr adresine girdikten sonra;
-Username bölümüne dhm(Sicil No) giriniz (ÖRN: dhm21180)
-Password bölümüne Parolanızı girin (Kurum Bilgisayarınızın Oturum Açma Şifrenizi girin) ve SIGN IN tuşuna basarak erişim sağlayabilirsiniz.



Kurumsal e-posta hesabınızı özel işleriniz için kullanılmaması, hesap güvenliğiniz için çok önemlidir!!!

SOME (SİBER OLAYLARA MÜDAHALE EKİBİ) NEDİR?

20 Ekim 2012'de Resmî Gazete'de Bakanlar Kurulu Kararı olarak "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi ve Koordinasyonuna İlişkin Karar" yayımlanmıştır.Karar neticesinde, kurulan USOM (Ulusal Siber Olaylara Müdahale Merkezi) koordinesinde Sektörel ve Kurumsal SOME'ler kurulması hakkında düzenlemeler yapılmıştır.

USOM ve SOME'ler siber olayları bertaraf etmede, oluşması muhtemel zararları önlemede veya azaltmada, siber olay yönetiminin ulusal düzeyde koordinasyon ve işbirliği içerisinde gerçekleştirilmesinde hayati önemi olan yapılardır.
Kurum iş süreçlerine, bilgi kaynaklarına, bilgi varlıklarına gelebilecek güvenlik olaylarına karşı etkin bir müdahale süreci işletmek için operasyonel bir yapı sağlamak ve bu olaylara karşı bir plan hazırlamaktır. SOME siber olay tiplerinin tanımlanmasında, yönetilmesinde, araştırılmasında ve iyileştirilmesinde rol alır. Ayrıca çeşitli siber güvenlik olayları ele alınırken operasyonel sürecin detaylarını dokümante ederek sürecin etkin yürütülmesini ve sürekli iyileştirilmesini sağlar. SOME ayrıca periyodik olarak zafiyet testleri ve denetimler yaparak Kurum ile ilgili tehditleri kontrol ve analiz etmelidir.

SOME Olay müdahale sürecinde siber olayları belirli bir yapı içerisinde ve kontrollü bir şekilde ele almaktadır. Bu süreç;

- Tüm siber olayların hızlı ve etkin bir şekilde yönetilmesini sağlar.
- Olay yönetiminde kararlı bir yaklaşım sağlar.
- Siber olayın neden olabileceği zararı minimize eder.
- Uygun kontroller ile tekrarlama olasılığı olan siber olayların iyileştirilmesini sağlar.

VERİ SIZINTISI ÖNLEME (DATA LOSS PREVENTION -DLP)

Hassas verilerin, işlendiği ve geçtiği her türlü kanaldan kasten ya da yanlışlıkla dışarıya sızmasını önlemeye yönelik olarak geliştirilen ve son yıllarda bir trend haline gören **DLP**'yi (Data Loss/Leakage Prevention) yani "veri sızıntısı önleme" teknolojisini, salt ve tek başına kullanılan bir ürün olarak ele almak yerine, kullanıldığı yerlerde farklı iş kollarıyla işbirliği ve diğer güvenlik cihazlarıyla birlikte bütünleşik kullanımıyla anlamlı hale gelen bir bütüncül veri güvenliği yaklaşımı ve sürecidir.

DLP **NEDİR?**

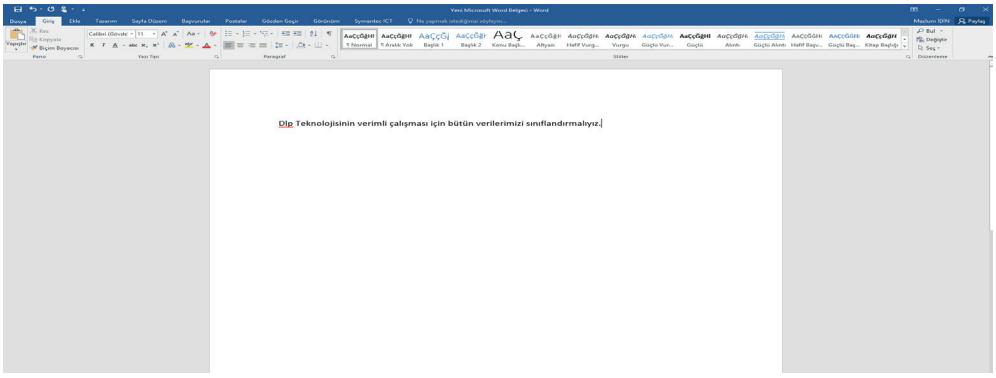
Güvenlik endüstrisindeki bakış farklılıklarına göre “veri sızıntısı önleme”, “veri kaybı önleme”, “veri kaçağı önleme”, “veri sızıntısı engelleme”, “veri kaybı engelleme” veya “veri kaçağı engelleme” olarak isimlendirilebilen **DLP (Data Loss Prevention)**, hassas verilerin bir ağ içinde yetkisiz olarak kullanımı ile iletiminin izlemesi ve korumasını sağlayan bir veri güvenliği teknolojisidir.

DLP KULLANIMI

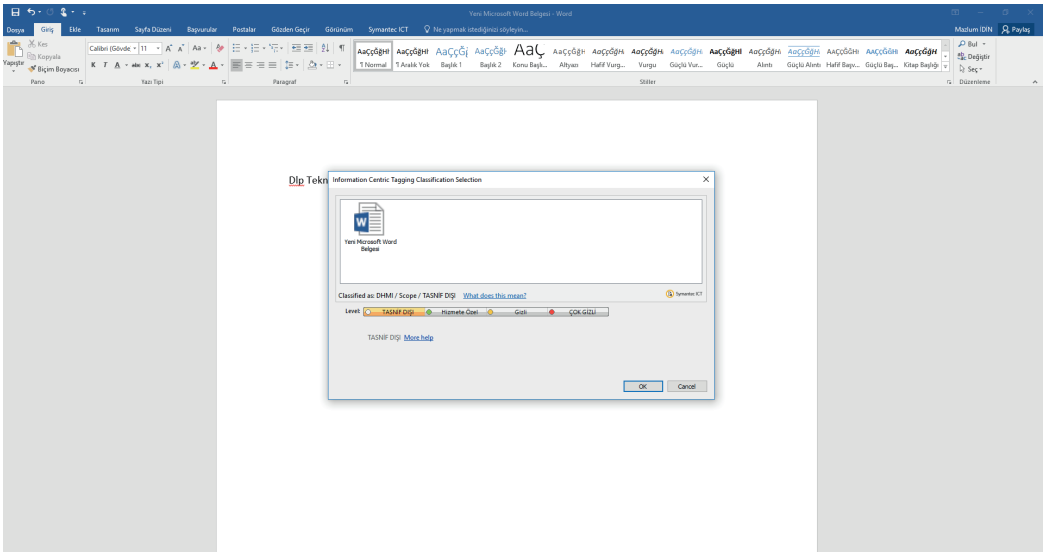
Kuruluşumuzda personelin DLP kullanımı ile yapması gerekenler:

Öncelikle kurumsal bütün bilgisayarlara ICT (Veri Sınıflandırma Aracı) programı yüklenilecektir. Bu program yüklenildikten sonra word, excel, pdf vb. uzantılı yeni bir veri dosyası oluşturulacağı zaman bu dosyaların gizlilik derecelerinin tanımlanması gerekmektedir.

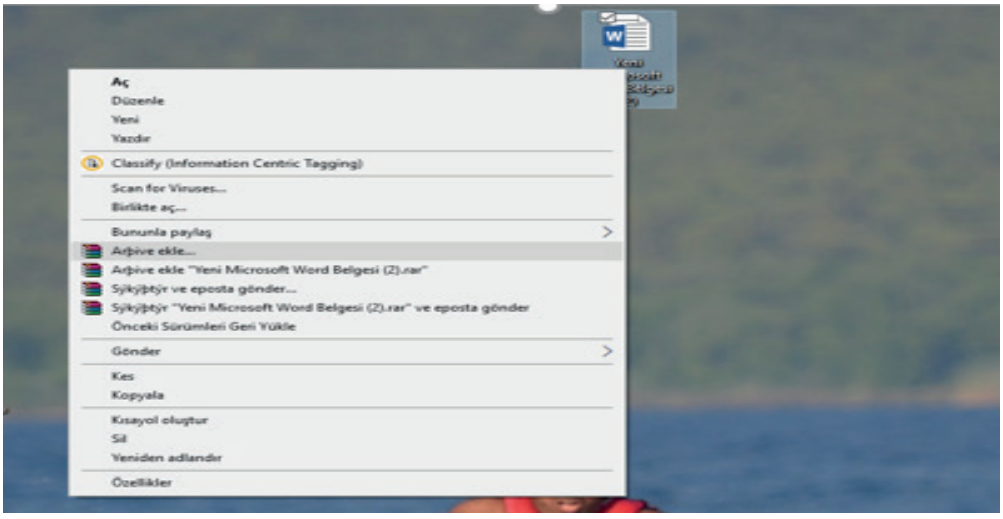
Örneğin yeni bir word dosyası oluşturalım.



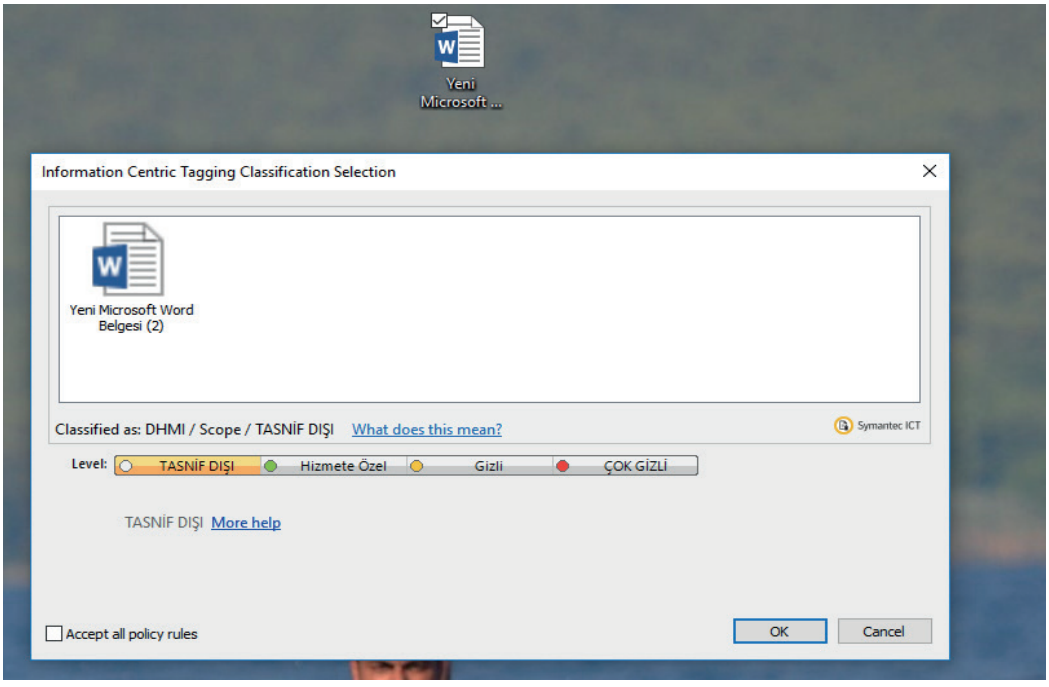
ICT programı yüklü olan bilgisayarlarda bu word belgesi kaydedilmeye çalışıldığında Aşağıdaki ekran görüntüsünde olduğu gibi bir mesaj ile sistem bu belgenin sınıflandırılmasını zorunlu tutacak ve Level kısmında bulunan Tasnif Dışı, Hizmete Özel, Gizli ve Çok Gizli olan kısımlardan biri seçilip belge kaydedilebilecek.



ICT programı ile bir belgenin içine girmeden ICT programı ile sınıflandırma yapmak için ise ekran görüntüsündeki gibi belgenin üstüne fare ile sağ tıklanılıp gelen ekranda Clasify (Information Centric Tagging) seçilir.



Gelen ekran aşağıdaki gibidir. Bu ekranda da belgenin içerisindeki verinin gizlilik derecesine göre ilgili alan seçilir ve kaydedilir.



DLP'DEKİ VERİ TÜRLERİ

Bilgi güvenliğinde "veri güvenliği" kategorisinde değerlendirilen veri sızıntısı önleme teknolojisinin işi/amacı veriyi ömrü boyunca **bulunduğu ağ içinde, depolama alanlarında ve son kullanıcı (uç) noktalarında** korumaktır. Bu doğrultuda DLP'de veri üç farklı şekilde ele alınır:

1. Hareket Halindeki Veri (Data in Motion): Ağ içinde hareket eden, yani eposta, anlık mesajlaşma, web ve P2P gibi iletim kanalları üzerinde sürekli hareket halinde olan veri türüdür.

2. Durağan Haldeki Veri (Data at Rest): Veri tabanları, dosya sistemleri ile diğer özel depolama birimlerindeki gerektiğinde sorgulanıp kullanılan hassas niteliğe sahip ve genelde ilk etapta korunması gerekli görülen veri türüdür.

3. Kullanım Halindeki Veri (Data in Use): Son kullanıcının sürekli olarak kullandığı ve işlediği türden olmakla birlikte hassas ve gizli verilerle bağlantısı olan aktif veri türüdür.

DLP teknolojilerinin (sistemlerinin) yukarıdaki veri türlerine göre ayrı tanımlama ve koruma yöntemleri bulunmaktadır. Koruma ve engelleme yöntemleri verinin yukarıda anlatılan

kullanım şekillerine göre çeşitlilik gösterirken veriler yukarıdaki bir ya da birkaç tane sınıfa birden girdiği zaman farklı noktalarda farklı koruma tedbirlerine tabi tutulurlar.

DLP SİSTEM TİPLERİ

DLP sistemleri, Network (Ağ) DLP ve Host (Son Nokta) Tabanlı DLP olmak üzere iki genel kategoride değerlendirilmektedir. Günümüzde piyasadaki mevcut DLP sistemleri genelde her iki sistemi birden içeren pekiştirilmiş çözümler halinde sunulur.

1. Network (Ağ) DLP: Gateway tabanlı sistemler olarak da bilinen Network (Ağ) DLP sistemi, ağ trafiği üzerine bir donanım ve/veya yazılım olarak yerleşerek e-posta, anlık mesajlaşma, FTP ve HTTP(S) gibi hareket halindeki veri trafiğinde yetkisiz bilgi iletimini engeller. Network (Ağ) DLP ayrıca organizasyon ağında güvensiz ve uygun olmayan bir biçimde tutulup risk oluşturan durağan haldeki verileri de tarayabilmektedir.

2. Host(SonNokta) Tabanlı DLP: Endpoint sistemi olarak da bilinen Host (Son Nokta) Tabanlı DLP, son kullanıcı bilgisayarı ya da server (sunucu) üzerine küçük ajan yazılımlar (agent) tarzı uygulamaların yüklenmesi ve DLP politikalarının da bir merkezi sunucudan güncellenmesi yoluyla işletilen DLP sistemdir. Bu sistemde kullanıcılar izinsiz bir işlemde uyarılıp, oluşan olay merkezi sunucuda bir kayıt olarak tutulmaktadır. Bu sistemin getirdiği en büyük fayda, taşınabilir bilgisayarlar ile mobil cihazların organizasyon ağı dışında oldukları zamanlarda bile kontrolünün sağlanabiliyor olmasıdır.
DLP sistem çözümlerinin hepsi yukarıdaki yapıda çalışmasına rağmen verileri ve içerikleri tararken farklı metotlar kullanırlar.

DLP'de İÇERİK ANALİZİ YÖNTEMLERİ

İlk çıkış amacı içeriden dışarıya doğru sızıntıları engellemek olan DLP sistemleri ağda ve uç noktalarda trafiği analiz edebilmek için derin paket analizi yöntemlerini kullanır. DLP, paketi ne kadar derin inceleyebilirse o kadar iyi tanımlama ve üzerindeki politikaya göre de engelleme yapar. DLP sistemleri bunun için belli başlı 8 yöntem kullanılır.

DLP'de içerik analizi yöntemleri genel olarak şu şekillerde sınıflandırılabilir:

DÜZENLİ İFADELER VE ANLAMLI KURALLAR

Düzenli ifadeler (regular expressions) ile anlamlı kurallar her DLP sisteminde mevcut olan ortak ve neredeyse standart bir yöntemdir. Düzenli ifadeler ile belirli bir kalıpta tanımlı kurallara denk gelen kaçak içerikler tespit edilebilmektedir. Buna verilebilecek en belirgin örnekler olarak T.C. kimlik numaraları, kredi kartı numaraları, vergi numaraları ya da banka hesap numaraları gösterilebilir. Bu tip özel numaralar ya da metinsel ifadeler belli bir algoritmaya göre üretildiği için, algoritmanın kendisi düzenli bir ifade ve anlamlı kurala dönüştürüldüğünde, DLP sisteminin içinden geçen ve kuralla eşleşen bilgiler anında tespit edilebilmektedir. Bu yöntem hem fazla yanlış alarm (false positive) üretir hem de yapılandırılmamış (unstructured) içeriklerin tepEsinde yetersizdir.

TAM DOSYA EŞLEŞTİRMESİ

Tam dosya eşleştirme (exact file matching) yönteminde özellikle fikri mülkiyet niteliğindeki video, resim, proje ve çizim gibi özel formattaki dosyaların özetleri (hash) çıkarılarak, DLP tarafından tanımlanması sağlanır. Buradaki asıl amaç dosyanın içeriğinin taranması değildir. Özellikle büyük boyutlu dosyaların tespit edilmesinde çok işe yarayan bu yöntemde içeriğe tam olarak bakılmamakta, sadece ilgili özetin eşleşmesi beklenmektedir. Özeti alınan dosyalar tekrar düzenlendiğinde, DLP'nin tespit edebilmesi için yeniden özet alma işlemi yapılmak zorunda kalınır.

VERİ TABANI PARMAK İZİ

Tam veri eşleştirmesi (database fingerprinting) olarak da bilinen bu yöntemde hassas veya gizli nitelikte verilerin tutulduğu (kimlik no, hesap no, müşteri bilgi gibi) veri tabanlarının parmak izi çıkartılarak, taramada ilgili eşleştirme yakalandığında başarılı bir şekilde engelleme yapılır. Parmak izi taramada her bir verinin birebir eşleşmesi esastır. Veri tabanlarında parmak izi alınması işlemi ister canlı olarak istenirse de belli aralıklarda yapılabilir. Veri tabanları üzerinde canlı parmak izi alımları sistem performans sorunları doğurabilirken, pasif olarak belirli periyotlarda alım gerçekleştirildiğinde de sürekli güncellenen veri tabanlarında parmak izi alınamayan veriler atlanılmış olur.

KISMİ BELGE EŞLEŞTİRMESİ

Bu yöntemde, korunan belgenin tam ya da kısmi eşleşmesi aranır. Bu yöntem, fikri mülkiyeti olan belgelerin tamamının ya da bir kısmının özellikle anlık mesajlaşma, internet teki forum ve yorum sayfaları ile sosyal ağların form alanlarına kopyalanıp yapıştırılmasının tespit edilmesine dayanır. Bu yöntemde önceden hassas ve gizli olarak belirlenen belgelerin ya tamamı ya da paragraf (cümle bazlı) olarak özetleri alınır. Ayrıca dilbilimsel analiz yoluyla kopyalanan cümlelerdeki ufak değişiklikler de tespit edilebilmektedir. Bu yöntemde çok miktarda içerik kullanılırsa performans sorunları yaşanabilir, ortak sözcük ve lazıf kalıpları yanlış alarmların sayısını artırabilir. Ama bu yöntem fikri mülkiyeti olan belgeler, program kaynak kodları ve belirli bir yapıda olmayan içeriklerin tespitinde başarılıdır.

İSTATİSTİKSEL ANALİZ

Bu yöntem Bayes analizi, makine öğrenme ve diğer istatistikî teknikleri kullanarak korunan içeriğe benzer olan içerik parçasındaki politikaları ihlal eden kısımları bulmaya dayanır. Spam engellemede kullanılan tekniklere benzeyen bu yöntem özellikle kısmi eşleştirmenin etkili olamadığı yapılandırılmamış içeriklerin tespitinde başarılıdır. Bu yöntem etkili olabilmek yani 'öğrenebilmek' için çok miktarda içeriğe ihtiyaç duyar.

ÖN TANIMLI KATEGORİLER

Ön tanımlı kategori, DLP ürünüyle birlikte gelen önceden oluşturulmuş ve PCI/DSS, COBIT, HIPAA ve ISO gibi belli başlı uluslararası standartlara dayalı kategorilerden oluşan bir yöntemdir. Bu yöntem ülkelere ve coğrafyalara göre farklılıklara gösterir. Birçok organizasyon türü için kategori yöntemi oldukça yeterli olabilirken, bütün kaçaklar için güvenilebilecek yegâne yöntem değildir.

KAVRAMSAL VE LÜGAT EŞLEŞMESİ

Bu yöntem belirli sözlükler, kurallar ve diğer analizleri bir arada kullanarak belli bir fikirle eşleşen içerikleri korumak için kullanılır. Örneğin cinsel taciz, iş arama ya da endüstriyel casusluk gibi hareketlerin tespitinde başvurulan bir yöntemdir. Bu yöntemde politika ihlallerini bulmak için anahtar sözcük, kelime sayıları ve kullanım konumlarına bakılır. Bu yöntemin en büyük zorluğu basitçe ve tek başına oluşturulamamasıdır. Bu, DLP sisteminin sağlayıcısı ve ihtiyaçlar doğrultusunda birden çok iş kolunun ortak ve uzun süreli çalışması

sonucu belli mantık çerçevesinde geliştirilebilecek bir yöntemdir. Kavramsal ve lügat eşleşmesi etkili bir yöntem olmakla beraber, karmaşıklığı ve kullanım şeklinden ötürü çok fazla yanlış sonuçları üretebilir.

OCR BAZLI EŞLEŞME

Yukarıdaki 7 genel yöntemin dışında bir de faydalandığı teknoloji açısından dikkate değer olan ve resim/fotoğraf türündeki medyaların direkt içini taramayı sağlayan OCR (optik karakter tanımlama) bazlı eşleşme yöntemidir. **Optik karakter tanıma** ya da OCR, "taranmış kâğıt evrakları, PDF dosyaları veya dijital bir kamerayla çekilen resimler gibi değişik belge türlerini düzenlenebilir ve aranabilir verilere dönüştürmenize olanak sağlayan bir teknolojidir" **OCR tabanlı eşleşme yöntemi** ise resim olarak kaydedilen dijital belgeler ya da tarayıcıdan resim olarak taranan belgelerin içindeki yazıların OCR ile tespit edilmesine dayanır. OCR yöntemi özellikle ağdaki tarayıcılardan sızan belgelerin tespitinde ve de bilgisayarda resim olarak kaydedilip dışarıya e-posta ya da web yoluyla çıkartılması olaylarında oldukça işe yarardır.

DLP'de içerik analizi olarak kullanılan bu 8 yöntem piyasadaki birçok DLP ürününde kullanılırken, bazıları bunların tamamını birden ya uygulamıyor ya da uygularken farklılıklar sergiliyorlar. Yine ürünlerin genelinde birden fazla analiz yöntemi zincirleme bir şekilde arka arkaya ya da iç içe kullanılarak daha etkin koruma gerçekleştirilebiliyor.

VERİ TÜRLERİNE GÖRE DLP'de KORUMA YERLERİ

DLP'nin veri sınıflandırmasında olduğu gibi veri koruma seviyeleri ve ağ içindeki engelleme noktaları da farklılık gösterir. DLP'nin, kurulum konumuna göre nasıl çalıştığı ve hangi tür verileri koruduğu değişirken, aynı veri için birden çok koruma şekli de geçerli olabilir. Koruma noktaları üç farklı yapıda ele alınır.

Verinin korunması için nerede bulunduğuna göre farklı yöntemler uygulanabilir. Öncelikle verinin konumunun tespit edilmesi DLP'den etkin bir biçimde yararlanmanın ilk şartıdır. DLP'de koruma yerleri ağda, depolama alanında ve uç noktada olmak üzere üç farklı yerdedir diyebiliriz.

NETWORK İÇİ KORUMA

Ağ içinde sürekli **hareket halinde olan verileri (data in motion)** kontrol etmek ve korumak için organizasyonlar tarafından DLP sistemlerinin network tipleri tercih edilerek gateway (ağ geçidi) yakınına veya ağ içindeki ana düğüm noktalarına yerleştirilir. Buradaki amaç ağdaki tüm hareketliliği gözlem altında tutmaktır. Network tipi DLP'de ağı gözetleyen bir "**network monitor**" ile e-posta trafiğine özel olarak bir **"e-posta entegrasyon bileşeni"** yapısı tercih edilir. Pratikte her iki yapı bir merkezi yönetim sunucusu altında birleştirilirken, geniş organizasyonlarda her iki yapı ayrı bir şekilde kontrol edilmekte ve yönetilebilmektedir. Ayrıca bu yapıda kullanımda olan verileri (data in use) kontrol etmek için tercih edilen agent yazılımlarından da yararlanılır.

DEPOLAMA ALANI KORUMASI

Bu yöntem, veri tabanları ile depolama sistemlerindeki durağan haldeki verileri (data at rest) korumak için verilerin önceden çeşitli yollarla keşfedilmesine dayanan bir mantıkta çalışır. Verilerin içerik keşfi yoluyla önceden tespit edilip işaretlenerek sızdırılması durumlarında çeşitli aksiyonların alındığı durağan haldeki verilerin DLP korumasında:

- SAN, NAS ve Exadata gibi depolama alanları,
- E-mail, dosya paylaşım ve belge yönetim sunucusu gibi uygulama sunucuları,
- Son kullanıcıların iş istasyonları ile dizüstü bilgisayarlarındaki yerleşik verilerin taranması bulunmaktadır. Depolama alanları ve sistemlerindeki verilerin içerik keşfi için kullanılan 3 temel yöntem vardır:

1. Uzaktan Tarama: Merkezi bir sunucu tarafından depolama alanlarının uzaktan taranması yoluyla gerçekleşir. Uzaktan taramanın etkisi network bant genişliği ile hızına bağlı olarak değişir. İhlal politikalarının sürekli güncel tutulabilmesi için uzaktan taramanın da sık yapılması gerekmektedir.

2. Uygulama Entegrasyonu: Belge yönetimi, içerik yönetimi ve diğer depolama depoları ile direkt entegrasyon sağlayan bir ajan kullanarak yapılır. Bu yöntemde doğrudan sistem içinde politika uygulaması sağlanabiliyor.

3. Agent Tabanlı Tarama: Sunuculara kurulan küçük ajan yazılımlar yoluyla lokal tarama

yapılmasına dayanır. Taramada network kaynakları yerine doğrudan ajanın kurulu olduğu sistemin lokal kaynakları kullanılmaktadır. Ajanlı taraması büyük boyutlu depolama sistemlerinin taranmasında oldukça etkilidir ve uzaktan taramadan daha hızlıdır. Ajan bazlı taramada bir de bellek yerleşimli agent taraması vardır. Bu yöntemde tam zamanlı çalışan bir ajan yerine taramayı yapıp, çalışmasını durdurarak işleyen bir yapı vardır. Bellek yerleşimli ajan taraması kaynakları daha az tüketir.

SON KULLANICI (UÇ NOKTA) KORUMASI

DLP ürünleri genelde en uygun maliyet açısından ve network çapında kapsama sağlamak adına ilk etapta network üzerinde kurulur. Fakat bütüncül veri güvenliğinde koruma alanının içine özellikle uç nokta kullanıcı sistemleri de girdiği için sadece ağ DLP ürünlerinin kullanımı güvenliğin önemli bir ayağını korumadan yoksun bırakmış olur. DLP'nin aslında en etkileşimli olduğu kullanımdaki veri (data in use) sınıfı kullanıcıların en çok kullandığı ve sızıntıların çok olabileceği verilerdir. Bu yüzden son kullanıcı veri güvenliğini sağlayan DLP ürünlerinin kurulması gerekmektedir. Endpoint DLP özellikli ürünler korumayı "agent" yani ajan tipi küçük yazılımlarla sağlar. Ajan yazılımlar sadece kurulu olduğu sistemi korumakla kalmaz, merkezi sunucudan kendisine yüklenen politikalar yoluyla verilerin network hareketliliğini de kontrol eder. Ajan yazılımların etkili olabilmesi için üzerine yüklenen politikaların sürekli güncel tutulması gerekir. Ajan yazılımların 4 farklı şekilde işleyen katmanı ve/veya özelliği bulunur:

- ✓ **İçerik Tarama:** Uç noktada depolanan içeriğin politika ihlallerine karşı taranmasıdır.
- ✓ **Dosya Sistemi Koruması:** Uç noktadaki içeriklerin yeniden keşfinden ziyade, herhangi bir ortama aktarılan verilerin taranmasında kullanılır. Özel içeriklerin USB ile harici depolama cihazlarına doğrudan ya da şifresiz olarak aktarılmasını engellemek için kullanılan bir koruma şeklidir.
- ✓ **Ağ Koruması:** Son kullanıcı cihazlarının ağ dışına çıkması durumunda ajan yazılımların üzerine son yüklü bulunan politikalara bağlı olarak network koruması görevini de sağlayan bir koruma şeklidir.

- ✓ **Grafiksel Kullanıcı Arayüzü (GUI) ve Kernel Koruması:** "Print Screen" tuşu ile ekran görüntüsü alma, kes/kopyala/yapıştır, uygulama kısıtlamaları veya CD'ye yazma gibi daha genel kullanım şekillerine odaklanmış bir korumadır.
- ✓ SB ile harici disk kontrolleri,
- ✓ "Print Screen" ile ekran görüntüsü alınmasının engellenmesi,
- ✓ CD yazıcı ile hassas bilgilerin CD ortamına aktarılması,
- ✓ "Kes/kopyala/yapıştır" işlemleri,
- ✓ Spesifik dosya erişim kısıtları,
- ✓ Ağdaki ya da sadece bir lokal bilgisayara bağlı yazıcılara çıktı gönderilmesi,
- ✓ Şifreli ve/veya şifresiz dosya gönderiminin kontrol altında tutulması, gibi koruma vektörünü oldukça genişleten özellikler geldi. DLP ajan yazılımların antivirüs ya da NAC (network access/admission control) ürünlerine nazaran daha hızlı ve efektif olması, son kullanıcı tarafındaki koruma işlevinin DLP'ye aktarılması sonucunu doğurdu. Ama DLP ile NAC ve antivirüs sistemlerinin entegrasyonunda statik koruma (USB, CD engeli gibi) işlevlerinin mevcut sistemlere aktarılıp, daha interaktif ve belli bir mantık gerektiren diğer eylemlerin kontrol altında tutulması işlevlerini ise DLP'ye yüklemek çok daha etkin bir güvenlik sağlayacaktır.

FINGERPRINT TEKNOLOJİSİ

Yazılımın veritabanı veya dosya sistemini tarayarak kendine özel bir algoritma çıkarması ve bul algoritma sonucunda verilerin tipik özelliklerinin anlaşılmasıdır. Bu tipik özellikler düzenli ifadeler ve yaklaşık düzenli ifadeler olarak gruplara ayrılmaktadır. Örneğin doküman içerisinde geçen bilimsel ifadelerin tespitidir. (şifre, formül, patent, banka hesap numaraları, T.C. kimlik numaraları, barkod numaraları vb). Çıkardığı sonuçlardan sonra uygulanacak politikalarda kendi veri tabanında bulunan şablonlar ile karşılaştırma yapması ve kuralları çalıştırmasıdır.

VERİ ŞİFRELEME

İşletim sistemi kurulu cihazların veri içeren disklerinin şifrelenmesi işlemidir. Böylece cihaz çalındığında bile içindeki veriler okunamayacaktır. Bu sistemde çözülmesi imkânsız ya da çok uzun yıllar süren AES(Advanced Encryption Standard (Gelişmiş Şifreleme Standartı)), 3DES(3.Data Encryption Standard (3.Veri Şifreleme Standartı)) gibi kriptografik algoritmalar kullanılır. DLP konusunda en önemli unsur ise "gizli veri" nedir sorununa cevap vermektir.

Öncelikle aşağıdaki sorulara cevap vermek gerekmektedir:

- ✓ Gizli veri nedir?
- ✓ Gizli verileri kimler izin dâhilinde kullanabilmelidir?
- ✓ Gizli veriler üzerinde nasıl çalışılmalıdır?
- ✓ Gerektiğinde veriler nasıl paylaşılmalıdır?
- ✓ Mobil cihaz kullanan personel hangi bilgilere erişebilmelidir?
- ✓ İstenmeyen bir durumda nasıl davranılmalıdır?
- ✓ Gizli veri paylaşımında onay mekanizması nasıl olmalıdır?

HUKUKİ DURUM

Fikri haklar kaybı, kurum bünyesinden gizli bilgilerin kaçırılması ya da sızdırılması, özel ticari anlaşmalarının, kuruma ait tasarımların ve patentli ürün bilgilerinin gizliliğini ihlal edilmesidir. Bu durum şirketler açısından itibar kaygısına da sebep olmaktadır. Kurumların yasal yönden kendilerini savunabilmeleri için ağ ve verileri üzerlerinde olan tüm hareketleri kanunlara belirtilen şekillerde kayıt altına almakla yükümlüdürler **(5651 sayılı Kanun)**

Ayrıca kişisel verilerin korunması kanunu 12. Maddesine göre Kurumlar kişisel verilere hukuka aykırı olarak erişilmesini önlemek, kişisel verilerin korunmasını sağlamak zorundadır.

Türk Ceza Kanunu 244.Madde 2. Fıkrasına göre;

Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, **var olan verileri başka bir yere gönderen kişi**, **altı aydan üç yıla kadar hapis cezası** ile cezalandırılır.

Aynı kanun maddesinin 3. Fıkrasına göre;

Bu fiillerin bir banka veya kredi kurumuna ya **da bir kamu kurum veya kuruluşuna** ait bilişim sistemi üzerinde işlenmesi halinde, verilecek **ceza yarı oranında** artırılır.

Türk Ceza Kanunu 136.maddesi 1. Fıkrasına göre;

Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, **bir yıldan dört yıla kadar hapis cezası** ile cezalandırılır.

Tck 137.maddede ise yukarıdaki fiilin

a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle,

b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle,

İşlenmesi halinde, verilecek ceza **yarı oranında** artırılır.

SON YILLARDAKİ BÜYÜK VERİ SIZINTILARI

Son 5-6 yılın en büyük veri sızıntılarından sadece bilinenleri incelendiğinde 1 milyardan fazla kullanıcı bilgisinin çalındığı görülebiliyor:

- ✓ **Adobe:** 2013 Mart'ta içinde kredi kartı bilgileri, isimler ve şifrelerin bulunduğu 152 milyon müşteri bilgisi çalındı.
- ✓ **Shanghai Roadway D&B:** 2012 Mart'ta firma içinde isimler, adresler ve mali bilgiler bulunan 150 milyon müşteri bilgisini yasadışı olarak alıp sattığı ortaya çıktı.
- ✓ **Bilinmeyen bir organizasyon:** 2013 Haziran'da Kuzey Kore'li hackerlar 140 milyon kişinin sosyal güvenlik numarası ile e-posta adreslerini çaldı.
- ✓ **Heartland Ödeme Sistemleri:** 2009 Haziran'da dünyanın 5. büyük kredi kartı işlemcisi 130 milyon kişinin kart bilgilerini kaybetmiş.
- ✓ **Target:** 2013 Kasım ve Aralık'ta hackerlar 70 milyon müşteri bilgisi ile 40 milyon kredi kartı bilgisini çalmış. Uzmanlar zayiatın aslında görünenden çok daha büyük olduğunu ifade ettiler.
- ✓ **Facebook:** 2008 Temmuz'da 80 milyon kullanıcının kullanıcı adını ve doğum tarihini yanlışlıkla açığa saçtı.
- ✓ **Sony:** 2011 Nisan'da 77 milyon müşteri bilgisini çaldırdı.
- ✓ **Pinterest:** 2013 Ağustos'ta 70 milyon kullanıcının e-posta bilgisi site üzeriden açığa saçıldı.
- ✓ **Yahoo!:** 2013 Mayıs'ta Japonya sitesinden 22 milyon kullanıcının e-posta kullanıcı bilgileri çalındı.
- ✓ **eBay:** 2014'ün ortasında hacker'ların çalışanların hesap bilgilerini kullanarak 145 milyon müşterinin şifreleri, kullanıcı adları, e-posta adresleri, adresleri, telefon numaraları ve doğum tarihlerini ele geçirdiği ortaya çıktı.

- ✓ **Shanghai Roadway D&B Marketing:** 2012'de içeriden bir köstebeğin 150 milyon kaydı çaldığı keşfedildi.
- ✓ **New York Taksi ve Limuzin Komisyonu:** 2014'ün ortasında şirket bilgi isteme özgürlüğü kapsamındaki talebe cevap verirken yanlışlıkla 173 milyon müşterinin bilgisini afişe etti.
- ✓ **Heartland Ödeme Sistemleri:** 2009'da ödeme sistemlerine bulaşan bir malware yüzünden 130 milyon müşterinin kart bilgileri çalındı.
- ✓ **Kore Kredi Bürosu:** 2014'ün başında şirketin bir IT çalışanının 104 milyon müşterinin bilgilerini bir USB diske atarak çaldığı söylendi.
- ✓ **JPMorgan Chase:** 2014'ün 3. çeyreğinde yapılan bir siber saldırıda 83 milyon müşteri verisi çalındı.
- ✓ **Ubisoft:** Hacker'ler 2013'te şirketin Web sitesini kırarak 58 milyon kullanıcının bilgisini çaldı.
- ✓ **LivingSocial:** 2013'te şirket sunucularına yapılan bie saldırı sonucu 50 milyon müşterinin bilgileri çalındı.
- ✓ **Evernote:** 2013'te şirket ağına sızılması sonucu 50 milyon müşterinin bilgisi çalındı.
- ✓ **NSA:** 2013 Haziran'da etkisi belki de gelmiş geçmiş en karmaşık olan veri sızıntısı olayı eski NSA çalışanı Edward Snowden'den vasıtasıyla gerçekleşti. Ortaya saçılan belgeler ülkeler arası ilişkileri etkileyecek boyutlara kadar dayandı. Hala ne kadarlık verinin sızdırıldığına dair net bir şey bilinmiyor. Bu sızıntılar sayesinde internet iletişimi ve e-posta haberleşmesinin aslında NSA ve GCHQ tarafından yıllardır gözlemlendiği ve internet altyapısının gizlilik ve güvenliğini sağlayan kriptoloji protokollerine arka kapılar bırakıldığı ortaya çıktı.

6. BİLGİ GÜVENLİĞİ VE RİSK YÖNETİMİ

BİLGİ GÜVENLİĞİNE İLİŞKİN TEMEL KAVRAMLAR

Bilgi; öğrenme, araştırma ve gözlem yoluyla elde edilen her türlü gerçek, haber ve kavrayışın tümüdür. Bir kurumun en değerli varlığı olan bilginin korunması ve etkili bir şekilde kullanılması sağlanmalıdır.

Bilgi Kaynakları: Basılı bilgi kaynakları; fiziksel ortamlar, arşiv belgeleri, kitaplar, dokümanlar. Dijital bilgi kaynakları; bilgisayarlar, internet siteleri, sunucular.

Bilgi Güvenliği: Bilginin yetkisiz erişimi, kullanımı, ifşa edilmesi, bozulması, değiştirilmesi, incelenmesi, kaydedilmesi ya da yok edilmesini engellemek için yapılabilecek tüm eylemlerdir.

Bilgi güvenliğinin 3 özelliği;

- Erişilebilirlik (Ne zaman, Nasıl?) "Bilgilerin, kişilerin yetkisi dâhilinde ihtiyaç duyulduğunda erişilebilir olması"
- Bütünlük (Ne, Hangi?) "Bilgilerin eksiksiz, tam, tutarlı ve doğru şekilde bulundurulması"
- Gizlilik (Kim?) "Bilgilerin yetkisiz erişime karşı korunması"

Bilgi Güvenliği Yönetim Sistemi (BGYS – ISO 27001)

Bilgi güvenliği yönetim sistemi, bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini; risk yönetimi sürecini uygulayarak muhafaza eder ve ilgili taraflara risklerin doğru bir şekilde yönetildiğine dair güvence verir.

Bilgi güvenliği yönetim sistemi, kurumsal hedeflere ulaşmak için bilgi güvenliğini;

- Kurmak,
- Uygulamak ve işletmek,
- İzlemek ve gözden geçirmek,
- Sürdürmek ve iyileştirmek için sistematik bir yaklaşımdır/yapıdır.

Bilgi Güvenliği Yönetim Sistemi'nin dayanak noktası; uluslararası bilgi güvenliği yönetim sistemi standardı olan ISO/IEC 27001 standardıdır. ISO/IEC 27001 standardizasyonu; bir bilgi güvenliği yönetim sistemi'nin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için şartları ortaya koymak amacıyla hazırlanmıştır. Standarda uyumluluk sürecinde göz önünde bulundurulması gereken maddeler vardır. Bunlar; Kuruluşun bağlamı, liderlik, planlama, destek, işletim, performans değerlendirmesi ve iyileştirmedir. Bunlara ilaveten Standart bağlamında Ek A maddeleri olarak sunulan Referans kontrol amaçları ve kontrolleri mevcuttur.

BGYS Sertifikasyon Döngüsü

BGYS SERTİFİKASYON DÖNGÜSÜ

1. BELİRLE: KAPSAMIN BELİRLENMESİ

5809 sayılı Elektronik ve Haberleşme Kanunu Siber Güvenlik Stratejisi ve Eylem Planı'na göre Kuruluşumuz "**Kritik Altyapıya**" sahiptir.
Bakanlığımız 2016-2019 Ulusal Siber Güvenlik Stratejisi Eylem Planı ve Kamunet (Kamu Sanal Ağ) gereksinimlerine uyumluluk kapsamında **2018** yılında Başkanlık bazında Bilgi Güvenliği Yönetim Sistemi (BGYS) ekibi kurulmuştur. Yine bu kapsamda **2021** yılında Başkanlık uhdesinde Bilgi Güvenliği Risk Yönetimi Şube Müdürlüğü kurularak iş süreçleri takip edilmektedir. 2021 yıl sonu itibariyle BGYS Kapsamımız, Genel Müdürlük 'tür.

2. PLANLA

- Politika ve Prosedürlerin oluşturulması
- Teknik tedbirlerin gözden geçirilmesi ve ilave tedbirlerin planlanması
- Varlık envanteri yönteminin belirlenmesi
- Risk planlama yönteminin belirlenmesi, kabul edilebilir risk kriterlerinin tespiti
- Tedarikçilerle ilişkilerin planlanması
- Hedef takip belirleme yöntemleri

2.1. Bilgi Güvenliği Politikaları

Bir kurumda izlenecek bilgi güvenliği politikalarının amaçları:

- Personelin kurumsal bilgi varlıklarının değerinin farkına varmasını ve iş süreçlerini bunu dikkate alarak yönetmesini sağlamak,
- Bilgi güvenliği hususunda daha bilinçli ve bilgili personel ile kurumun bilgi kaybından korunmasını sağlamak,
- Risklerin en aza indirgenmesi ve var olan riskleri de yönetilebilir kılmaktır.

Kuruluşumuz bilgi güvenliği politikasına ve diğer BGYS dokümanlarına KEYS - Kurumsal Entegre Yönetim Sistemi (keys.dhmi.gov.tr) olarak adlandırılan uygulama üzerinden ulaşılabilmektedir. Aynı zamanda Kuruluşumuz kurumsal web sitesinde (www.dhmi.gov.tr) bilgi güvenliği politikasına yer verilmektedir.

3. UYGULA

- Varlık envanterinin oluşturulması, kritikliklerinin belirlenmesi
- Tehdit ve zafiyetlerin tespit edilmesi
- Risk işleme faaliyetinin yürütülmesi
- Fırsatların belirlenmesi
- Tedarikçi değerlendirmeleri ile bilgi güvenliği temelinde tedarik süreçlerinin yürütülmesi
- Hedef belirleme ve performans ölçümleri
- Farkındalık eğitimleri
- İç tetkikler
- Yönetim Gözden Geçirme

3.1. Risk İşleme Faaliyeti

Risklerin belirlenmesinde Kuruluşta uygulanan Bilgi Güvenliği Yönetim Sisteminin kapsamı referans alınmıştır. Buna göre Kuruluşun ilgili taraflarla olan çalışmaları ve ilgili tarafların bilgi güvenliği beklentileri risk değerlendirme ve işleme çalışmaları için bir çerçeve oluşturmuştur. Kuruluşun Risk Değerlendirme Kapsamı: Bilgi Güvenliği Yönetim Sistemi kapsamında kuruluş tarafından işletilen süreçler ve bu süreçler ile ilişkili bilgi varlıklarıdır.

Risklerin belirlenmesinde; iç/dış hususlar ve paydaşların gereksinimleri, personel deneyimleri, ihlal olayı ve açıklık bilirimi formu, geçmiş yıllardaki risk değerlendirme çalışmaları, düzeltici faaliyetler, Türkiye'de ve dünyada ortaya çıkmış bilgi güvenliği olayları ve sızma, teknik açıklık ve servis durum test sonuçları göz önünde bulundurulur.

Risklerin, Kuruluş varlıklarına / süreçlerine / bilgilerine potansiyel etkilerini azaltmak, aktarmak, kabul etmek ya da ortadan kaldırmak için yapılan çalışmalar risk işleme olarak tanımlanır.
Risk hesaplaması Riskten etkilenen varlık veya sürecin gizlilik, bütünlük ve erişilebilirlik yönü değerlendirilerek, 1 ile 5 puan arasında yapılır. Aşağıda yer alan tabloda gizlilik, bütünlük ve erişilebilirlik durumlarının değerlendirilmesinde kullanılan puanlamalar açıklanmıştır.

Değerlendirme Derecesi	Tanımı
5 - Çok Yüksek	Kuruluşun en kritik bilgileridir. Bilgilerin ifşa edilmesi ya da yetkisiz kişilerin eline geçmesi durumunda; • Kuruluşun yapısını etkileyebilecek yasal yaptırımlara maruz kalır. • Kuruluşun ulusal veya uluslararası düzeyde imaj ve itibarı zedelenir.
4 - Yüksek	Kurum içi yüksek değerdeki hassas ve özel bilgilerdir. Bilgilerin ifşa edilmesi ya da yetkisiz kişilerin eline geçmesi durumunda; • Yasalara veya düzenlemelere tabii bir gereksinim karşılanamamış olur. • Kuruluşun ulusal düzeyde imaj ve itibarı zedelenir. • Kuruluşun iş süreçlerinin yeniden planlanması gerekir.
3 - Orta	Sadece birim çalışanlarının erişebileceği bilgilerdir. Bilgilerin ifşa edilmesi ya da yetkisiz kişilerin eline geçmesi durumunda; • Kuruluşun imaj ve itibarı olumsuz etkilenebilir. • Birimin iş süreçlerinde aksaklıklar oluşur.
2 - Düşük	Tüm Kuruluş çalışanlarının erişebildiği bilgilerdir. Bilgilerin ifşa edilmesi ya da yetkisiz kişilerin eline geçmesi durumunda; • Kuruluşun imaj ve itibarı olumsuz etkilenebilir.
1 - Çok Düşük	Kamuoyunun aydınlatılmasında kullanılan bilgilerdir. Yetkisiz kişilerin eline geçmesi durumunda Kuruluş zarar görmez.

3.2. Örnek Risk Tablosu

RİSK TANIMI	RİSKTEN ETKİLENEN VARLIK GRUBU	OLASILIK	Gizlilik	Bütünlük	Erişilebilirlik	ETKİ DEĞERİ	RİSK DEĞERİ	RİSK SAHİBİ	MEVCUT KONTROLLER	RİSK FIRSATLARI	RİSK İŞLEME SEÇENEKLERİ (Kabul-Kaçınma-Aktarma-Azaltmak)	RİSK İŞLEME FAALİYETLERİ	İLGİLİ KONTROL MADDELERİ
BGYS politikaları ve standartların düzenli gözden geçirilmemesi ve diğer politika/standartlar ile uyumunun sağlanmaması sebebiyle politikaların güncelliğini yitirmesi sonucu BGYS'nin doğru işletilememesi	Basılı Bilgi Varlıkları	5	5	4	5	3	15						A.18.2.2 - A.18.2.3
Pandemi döneminde uzaktan çalışmaya geçilmesi nedeniyle parola paylaşımının artması, sistemlere yetkisiz erişim sağlanması	Sayısal Bilgi Varlıkları	4	5	4	5	5	20						A.9.4.3 A. 7.2.2
Pandemi nedeniyle uzman personelin hastalanması neticesinde iş süreçlerinde aksaklıkların yaşanması	İş Süreçleri	4	5	4	5	5	20						A.7.2.1 A.12.3.1
Pandemi nedeniyle gerçekleştirilemeyen yüzyüze görüşmelerin kurumsal online toplantı platformları üzerinden sağlanmaması nedeniyle verilerin ifşası	İş Süreçleri	3	5	4	5	5	15						A.6.2.2

3.3. T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi

Kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmelerin bilgi ve iletişim güvenliği kapsamında genel olarak alması gereken tedbirleri belirlemek için 06.07.2019 tarih ve 30823 sayılı Resmi Gazete'de Bilgi ve İletişim Güvenliği Tedbirleri konulu 2019/12 sayılı Cumhurbaşkanlığı Genelgesi yayımlanmıştır. Yayımlanan Genelge doğrultusunda Cumhurbaşkanlığı Dijital Dönüşüm Ofisi koordinasyonunda paydaşların katılımıyla Bilgi ve İletişim Güvenliği Rehberi hazırlanmıştır.

Rehberin temel amacı; bilgi güvenliği risklerinin azaltılması, ortadan kaldırılması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik bilgi/verinin güvenliğinin sağlanması için asgari güvenlik tedbirlerinin belirlenmesi ve belirlenen tedbirlerin uygulanması için yürütülecek faaliyetlerin tanımlanmasıdır.

Bilgi ve İletişim Güvenliği Rehberinin Hedefleri

Rehber uygulama yol haritasının planlanması ve uygulanması aşamalarında gerçekleştirilecek tüm çalışmalarda aşağıda belirtilen temel prensipler dikkate alınmalıdır.

Bilgi ve İletişim Güvenliği Rehberi Temel Prensipler

Güvenlik Tedbirleri

Varlık gruplarına yönelik güvenlik tedbirleri ana başlıkları:

- Ağ ve Sistem Güvenliği
- Uygulama ve Veri Güvenliği
- Taşınabilir Cihaz ve Ortam Güvenliği
- Nesnelerin İnterneti (Iot) Cihazlarının Güvenliği
- Personel Güvenliği
- Fiziksel Mekânların Güvenliği

Uygulama ve teknoloji alanlarına yönelik güvenlik tedbirleri ana başlıkları:

- Kişisel Verilerin Güvenliği
- Anlık Mesajlaşma Güvenliği
- Bulut Bilişim Güvenliği
- Kripto Uygulamaları Güvenliği
- Kritik Altyapılar Güvenliği

- Yeni gelişmeler ve Tedarik

Sıkılaştırma faaliyetlerine yönelik güvenlik tedbirleri ana başlıkları:

- İşletim Sistemi Sıkılaştırma Tedbirleri
- Veri Tabanı Sıkılaştırma Tedbirleri
- Sunucu Sıkılaştırma Tedbirleri

3.4. DDO Rehber Uygulamaları

- Envanterini tut (donanım, yazılım, evrak vs.)
- Ağ güvenliğini sağla (ilgili fiziksel ve mantıksal portları açmak gibi)
- Veri sızıntısını önle
- Güvenli yazılım geliştir
- Log kayıtlarını al
- Güvenlik test ve denetimlerini gerçekleştir
- Erişim yönetimi tesis et, kimlik doğrulaması yap
- En az yetki prensibini uygula
- Personel eğitimine önem ver
- İş sürekliliğini sağla (FKM)
- Fiziksel güvenliği sağla

4. SERTİFİKA AL

- Yılda en az 1 kez politika ve prosedürler gözden geçirilir.
- Güvenlik test ve tatbikatları yapılır.
- İş sürekliliği tesis edilir.
- BGYS süreçlerinin tamamı işletilir. Genel Müdürlüğümüz dâhilinde ISO/IEC 27001:2017 sertifikası 25.12.2018 tarihinden itibaren bulunmakta ve sürdürülmektedir.

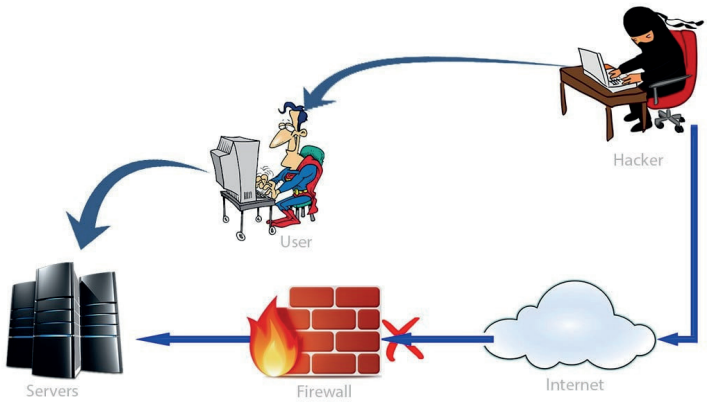
5. SÜRDÜR

- İç tetkik bulgularını değerlendirme
- Dış denetime hazırlık yapma (Sertifika süreçlerinin tamamı)
- Her yıl gerçekleşen dış denetim ile sertifikanın devamlılığı sağlanmaktadır.

BİLGİ GÜVENLİĞİNDE İNSAN FAKTÖRÜ

Bilgi güvenliği, fiziksel ve sistemsel önlemlerle sadece belirli bir ölçüde sağlanabilir. Bilgi güvenliğinin en yüksek seviyede sağlanabilmesi için çalışanların bilgi güvenliğiyle alakalı tehdit ve riskleri öngörebilmesi, riskleri azaltma, tehditlere karşı önlem alma konusunda bilgili olması ve kurum bilgi güvenliği politikalarının farkında olması gereklidir.

Güvenliğin en zayıf halkası insan olduğundan, kişilerin bu bilinçle hareket etmesi, bilgi güvenliğini önemli derecede artıracaktır. Güvenliği %20'lik kısmı teknik güvenlik önlemleri ile sağlanırken, %80'lik kısmı son kullanıcıya bağlı olmaktadır.



BİLGİ GÜVENLİĞİ KAPSAMINDA YAPILMASI GEREKENLER

- Kurumsal ve kişisel veri güvenliğine dikkat edilmeli
- Mesajlar, e-postalar, linkler güvenilir kaynaktan gelmiyorsa açılmamalı
- Cihaz ve ağlarda güvenlik hususlarına dikkat edilmeli
- Bilinçlendirilmiş ve doğru yetkilendirilmiş çalışanlar görevlendirilmeli
- Bilgi varlıklarının korunması için tüm personel iş birliği içinde çaba göstermelidir.
- Temiz Masa Temiz Ekran uygulamasına dikkat edilmeli
- Karmaşık parolalar tercih edilmeli
- Kişisel hesap parolaları ve kurumsal hesap parolaları birbirinden farklı olmalı
- Şifreler kesinlikle başkası ile paylaşılmamalı
- İnkâr edilemezlik ilkesi unutulmamalıdır.

Bilgi güvenliği olayı; Kuruluşun varlıklarına, saygınlığına, iş sürekliliğine zarar verecek potansiyele sahip aleyhte gelişen durumlardır. Bilgi güvenliği ihlallerine örnek olarak; işten çıkan bir kişinin yetkilerinin sonlandırılmaması, masadan önemli bir evrak bırakarak veya oturumu kilitlemeden kalkılması ve kurumsal iş süreçlerinde kişisel e-posta adreslerinin kullanılması gibi durumlar belirtilebilir. Bu tarz durumlar söz konusu olduğunda; Bilgi Teknolojileri Dairesi Başkanlığı ile telefon, resmi yazı vb. aracılığıyla irtibata geçilmeli veya KEYS aracılığıyla ihlal olay bildiriminde bulunulmalı ya da some@dhmi.gov.tr adresine e-posta gönderilmesi gerekmektedir.

İŞ SÜREKLİLİĞİ

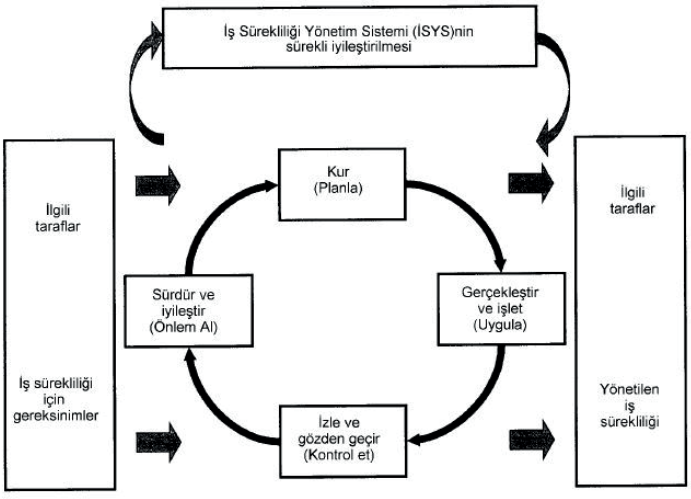
Kuruluş tarafından verilen hizmetlerin kesintisiz devam etmesi ve herhangi bir kesinti durumunda tanımlanan sürelerde tekrar hizmet vermeye devam edebilmesinin sağlanması becerisidir.

İş sürekliliğini kesintiye uğratan nedenler;

- Yangın
- Kuruluş itibarına yönelik saldırı
- Doğal Afet
- Tedarik Zinciri Kesintisi
- Enerji Kesintisi
- İletişim Kesintisi
- Sistem Kesintisi
- Siber Saldırı
- Terör Saldırısı
- Salgın Hastalık

Amaç

- Hizmet devamlılığı ile işletme devamlılığını sağlamak
- Yasalara uyum sağlamak
- Varlıkları korumak
- İtibarı korumak
- Erişilebilirlik taahhüdüne uyum (SLA)
- Kesinti maliyetlerini azaltarak riskleri minimize etmektir.



İş Sürekliliği Döngüsü

KİŞİSEL VERİLERİN KORUNMASI (ISO – 27701)

Kişisel veri, tek başına veya başka bilgilerle birleştiğinde bir bireyi tanımlayan veya çıkarım yapılmasını sağlayan her türlü bilgidir.

Kişisel veri türleri;

Kimlik: Ad Soyad, Anne/Baba adı, Anne kızlık soyadı, Doğum tarihi, Doğum yeri, Medeni hali, Nüfus cüzdanı seri sıra no, T.C kimlik no

İletişim: Adres bilgisi, E-posta adresi, İletişim adresi, Telefon no
Özlük: Bordro bilgileri, Disiplin soruşturması, İşe giriş belgesi kayıtları, Mal bildirimi bilgileri, Özgeçmiş bilgileri, Performans değerlendirme raporları, kişinin çalıştığı kurum, kurumdaki pozisyonu
Fiziksel Mekân Güvenliği: Çalışan ve ziyaretçilerin giriş çıkış kayıt bilgileri, Kamera kayıtları
Finans: Bilanço bilgileri, Malvarlığı bilgileri, banka hesap bilgisi, IBAN bilgisi, alacak-borç bilgisi, aylık fatura bilgisi
Mesleki Deneyim: Diploma bilgileri, Gidilen kurslar, Sertifikalar,
Görsel ve İşitsel Kayıtlar: Fotoğraf, Video, Ses kaydı
İşlem Güvenliği: IP adresi bilgileri, İnternet sitesi giriş çıkış bilgileri, Şifre ve parola bilgileri
Özel nitelikli kişisel veri ise öğrenildiği takdirde kişiyi mağdur edecek veya ayrımcılığa uğratacak nitelikteki verilerdir. Kişilerin; ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik verileri özel nitelikli kişisel veridir.
Anayasal güvence altına alınmış olan kişisel verilerin korunmasını isteme hakkını düzenlemek amacıyla hazırlanan 6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK) 7 Nisan 2016 tarihli 29677 Sayılı Resmî Gazetede yayımlanarak yürürlüğe girmiştir.

Kişisel Verilerin Korunması Kanununun (KVKK) Amacı

- Kişisel verilerin işlenmesinde, başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak
- Kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek
- Kişilerin mahremiyetini korumak
- Kişisel veri güvenliğini sağlamak

KVKK Hangi Verileri Kapsamaktadır?

- "Tamamen veya kısmen otomatik yollarla işlenen veriler ile herhangi bir kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen veriler" KVKK kapsamındadır.
- Otomatik olarak işlenen bütün veriler kanun kapsamında değerlendirilmektedir.
- Otomatik olmayan yollarla işlenen verilerin kanun kapsamında değerlendirilmesi için bir kayıt sisteminin parçası olması gerekmektedir.
- Yani, herhangi bir kritere bağlı olmadan kişilerin adının soyadının bir kâğıtta yazılmış olması kanun kapsamında değerlendirilmemektedir.
- Kanun, tüzel kişilerin verilerini kapsamaz.

KVKK'da Yer Alan Kavramlar

Veri İşleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel veri işleyen, veri sorumlusunun organizasyonu dışındaki gerçek veya tüzel kişiler

İlgili Kişi: Kişisel verisi işlenen gerçek kişidir. Tüzel kişiye ait bir verinin herhangi bir gerçek kişiyi belirlemesi ya da belirlenebilir kılması halinde bu veriler Kanun kapsamında koruma altındadır.

Açık Rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızadır.

Aydınlatma: Veri sorumlusunun, kişisel verilerini işlediği kişilere, bu verilerinin kim tarafından, hangi amaçlarla ve hangi hukuki gerekçelere dayanarak işlenebileceği, kimlere hangi amaçlarla aktarılabileceği hususunda bilgi vermesi yükümlülüğüdür.

VERBİS (Veri Sorumluları Sicil Bilgi Sistemi): Kişisel verileri işleyen gerçek ve tüzel kişilerin, kişisel veri işlemeye başlamadan önce kaydolmaları gereken ve işlemekte oldukları kişisel verilerle ilgili kategorik bazda bilgi girişi yapacakları bir kayıt sistemidir.

Kişisel Verilerin İşlenmesi

Kişisel verinin elde edilmesinden itibaren veri üzerinde gerçekleştirilen her türlü işlemdir. Bu işlemler; Elde etme, Depolama, Muhafaza Etme, Paylaşma, Yeniden Düzenleme, Devralma, Okuma, Değiştirme, Sınıflandırma vb.dir.

Kişisel Verilerin Kanuna Uygun İşlenmesi

Kişisel verilerin kanuna uygun olarak işlenmesi için aşağıdaki tüm şartların birlikte sağlanması gerekmektedir;

- İşlemenin veri işleme şartlarından en az birine dayanması
- Aydınlatmanın gerçekleşmiş olması
- Temel ilkelere uygun olması

Kişisel Veri İşleme Şartları

Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

- Kanunlarda açıkça öngörülmesi
- Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
- İlgili kişinin kendisi tarafından alenileştirilmiş olması.
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

Kişisel Verilerin İşlenmesinde Temel İlkeler

Veri işleme faaliyeti hangi şartına dayanırsa dayansın tüm veri işleme faaliyetleri aşağıdaki ilkelere uygun olarak gerçekleştirilmelidir;

- Hukuka ve dürüstlük kurallarına uygun olma,
- Doğru ve gerektiğinde güncel olma,
- Belirli, açık ve meşru amaçlar için işlenme,
- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,
- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme
- İşlemenin amaç ve süre ile sınırlı olması

Her kişisel verinin bir muhafaza süresi olmalıdır, hiçbir veri sonsuza kadar saklanamaz. Muhafaza süresi için varsa ilgili mevzuattaki süre, yoksa işlenen amaç için gerekli süre kadar muhafaza edilir.

Kuruluşumuz KVYS dokümanlarına KEYS - Kurumsal Entegre Yönetim Sistemi (keys.dhmi.gov.tr) olarak adlandırılan uygulama üzerinden ulaşılabilmektedir. Aynı zamanda Kuruluşumuz kurumsal web sitesinde (www.dhmi.gov.tr) kişisel verileri koruma politikasına yer verilmektedir.

İNTERNET ORTAMINDA YAPILAN YAYINLARIN DÜZENLENMESİ VE BU YAYINLAR YOLUYLA İŞLENEN SUÇLARLA MÜCA-DELE EDİLMESİ HAKKINDA KANUN

Kanun Numarası : 5651
Kabul Tarihi : 4/5/2007
Yayımlandığı Resmî Gazete : Tarih : 23/5/2007 Sayı : 26530
Yayımlandığı Düstur : Tertip : 5 Cilt : 46

Amaç ve kapsam

MADDE 1- (1) Bu Kanunun amaç ve kapsamı; içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usûlleri düzenle-mektir.

Tanımlar

MADDE 2- (1) Bu Kanunun uygulamasında;
a) Bakanlık: Ulaştırma Bakanlığını,
b) **(Mülga: 15/8/2016-KHK-671/20 md.; Aynen kabul: 9/11/2016-6757/17 md.)**
c) **(Değişik: 15/8/2016-KHK-671/20 md.; Aynen kabul: 9/11/2016-6757/17 md.)** Başkan: Bilgi Teknolojileri ve İletişim Kurumu Başkanını,
ç) Bilgi: Verilerin anlam kazanmış biçimini,
d) Erişim: Bir internet ortamına bağlanarak kullanım olanağı kazanılmasını,
e) Erişim sağlayıcı: Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü ger-çek veya tüzel kişileri,
f) İçerik sağlayıcı: İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişileri,
g) İnternet ortamı: Haberleşme ile kişisel veya kurumsal bilgisayar sistemleri dışında kalan ve kamuya açık olan internet üzerinde oluşturulan ortamı,
ğ) İnternet ortamında yapılan yayın: İnternet ortamında yer alan ve içeriğine belirsiz sayıda kişilerin ulaşabileceği verileri,

h) İzleme: İnternet ortamındaki verilere etki etmeksizin bilgi ve verilerin takip edilmesini,

ı) **(Değişik: 15/8/2016-KHK-671/20 md.; Aynen kabul: 9/11/2016-6757/17 md.)** Kurum: Bilgi Teknolojileri ve İletişim Kurumunu,

i) Toplu kullanım sağlayıcı: Kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayanı,

j) **(Değişik: 26/2/2014-6527/15 md.)** Trafik bilgisi: Taraflara ilişkin IP adresi, port bilgisi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgilerini,(1)

k) Veri: Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri,

_____

(1) 29/7/2020 tarihli ve 7253 sayılı Kanunun 1 inci maddesiyle, bu bende "IP adresi," ibaresinden sonra gelmek üzere "port bilgisi," ibaresi eklenmiştir.

l) Yayın: İnternet ortamında yapılan yayını,

m) Yer sağlayıcı: Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek ve-ya tüzel kişileri,

n) **(Ek: 6/2/2014-6518/85 md.)** Birlik: Erişim Sağlayıcıları Birliğini,

o) **(Ek: 6/2/2014-6518/85 md.)** Erişimin engellenmesi: Alan adından erişimin engellenmesi, IP adresinden erişimin engellenmesi, içeriğe (URL) erişimin engellenmesi ve benzeri yöntemler kullanılarak erişimin engellenmesini,

ö) **(Ek: 6/2/2014-6518/85 md.)** İçeriğin yayından çıkarılması: İçerik veya yer sağlayıcılar tarafından içeriğin sunuculardan veya barındırılan içerikten çıkarılmasını,

p) **(Ek: 6/2/2014-6518/85 md.)** URL adresi: İlgili içeriğin internette bulunduğu tam internet adresini,

r) **(Ek: 6/2/2014-6518/85 md.)** Uyarı yöntemi: İnternet ortamında yapılan yayın içeriği nedeniyle haklarının ihlal edildiğini iddia eden kişiler tarafından içeriğin yayından çıkarılması amacıyla öncelikle içerik sağlayıcısına, makul sürede sonuç alınamaması hâlinde yer sağlayıcısına iletişim adresleri üzerinden gerçekleştirilecek bildirim yöntemini,

s) **(Ek:29/7/2020-7253/1 md.)** Sosyal ağ sağlayıcı: Sosyal etkileşim amacıyla kullanıcıların internet ortamında metin, görüntü, ses, konum gibi içerikleri oluşturmalarına, görüntülemelerine veya paylaşmalarına imkân sağlayan gerçek veya tüzel kişileri,

ifade eder.

Bilgilendirme yükümlülüğü

MADDE 3- (1) İçerik, yer ve erişim sağlayıcıları, yönetmelikle belirlenen esas ve usûller çerçevesinde tanıtıcı bilgilerini kendilerine ait internet ortamında kullanıcıların ulaşabileceği şekilde ve güncel olarak bulundurmakla yükümlüdür.

(2) Yukarıdaki fıkrada belirtilen yükümlülüğü yerine getirmeyen içerik, yer veya erişim sağlayıcısına Başkan tarafından iki bin Türk lirasından elli bin Türk lirasına kadar idarî para cezası verilir.(1)(2)

(3) **(Ek: 6/2/2014-6518/86 md.)** Bu Kanun kapsamındaki faaliyetleri yurt içinden ya da yurt dışından yürütenlere, internet sayfalarındaki iletişim araçları, alan adı, IP adresi ve benzeri kaynaklarla elde edilen bilgiler üzerinden elektronik posta veya diğer iletişim araçları ile bildirim yapılabilir.

(4) **(Ek: 26/2/2014-6527/16 md.; Değişik: 10/9/2014-6552/126 md.; İptal: Anayasa Mahkemesinin 2/10/2014 tarihli ve E.: 2014/149, K.: 2014/151 sayılı Kararı ile.)**(3)

(5) **(Ek:29/7/2020-7253/2 md.)** Bu Kanun kapsamında verilen idari para cezaları, muhatabın yurt dışında bulunması hâlinde Kurum tarafından doğrudan muhataba üçüncü fıkradaki usulle de bildirilebilir. Bu bildirim 11/2/1959 tarihli ve 7201 sayılı Tebligat Kanununa göre yapılan tebligat hükmündedir. Bu bildirimin yapıldığı tarihi izleyen beşinci günün sonunda tebligat yapılmış sayılır.

İçerik sağlayıcının sorumluluğu

MADDE 4- (1) İçerik sağlayıcı, internet ortamında kullanıma sunduğu her türlü içerikten sorumludur.

_____

(1) 15/8/2016 tarihli ve 671 sayılı KHK'nin 21 inci maddesiyle, bu fıkrada yer alan "Başkanlık" ibaresi "Başkan" şeklinde değiştirilmiş olup, daha sonra bu hüküm 9/11/2016 tarihli ve 6757 sayılı Kanunun 18 inci maddesiyle aynen kabul edilerek kanunlaşmıştır.

(2) 10/9/2014 tarihli ve 6552 sayılı Kanunun 126 ncı maddesiyle, bu fıkrada yer alan "ikibin Yeni Türk Lirasından onbin Yeni Türk Lirasına" ibaresi "iki bin Türk lirasından elli bin Türk lirasına" şeklinde değiştirilmiştir.

(3) Bu İptal Kararı 1/1/2015 tarihli ve 29223 sayılı Resmî Gazete'de yayımlanmıştır.

(2) İçerik sağlayıcı, bağlantı sağladığı başkasına ait içerikten sorumlu değildir. Ancak, sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise genel hükümlere göre sorumludur.

(3) **(Ek: 6/2/2014-6518/87 md.) (İptal: Anayasa Mahkemesinin 8/12/2015 tarihli ve E.: 2014/87, K.: 2015/112 sayılı Kararı ile.)**[1]

Yer sağlayıcının yükümlülükleri [2]

MADDE 5- (1) Yer sağlayıcı, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir.

(2) **(Değişik: 6/2/2014-6518/88 md.)** Yer sağlayıcı, yer sağladığı hukuka aykırı içeriği bu Kanunun 8 inci ve 9 uncu maddelerine göre haberdar edilmesi hâlinde yayından çıkarmakla yükümlüdür.

(3) **(Ek: 6/2/2014-6518/88 md.)** Yer sağlayıcı, yer sağladığı hizmetlere ilişkin trafik bilgilerini bir yıldan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlüdür.

(4) **(Ek: 6/2/2014-6518/88 md.)** Yer sağlayıcılar, yönetmelikle belirlenecek usul ve esaslar çerçevesinde yaptıkları işin niteliğine göre sınıflandırılabilir ve hak ve yükümlülükleri itibarıyla farklılaştırılabilirler.

(5) **(Ek: 6/2/2014-6518/88 md.) (İptal: Anayasa Mahkemesinin 8/12/2015 tarihli ve E.: 2014/87, K.: 2015/112 sayılı Kararı ile.)**[1]

(6) **(Ek: 6/2/2014-6518/88 md.)** Yer sağlayıcılık bildiriminde bulunmayan veya bu Kanundaki yükümlülüklerini yerine getirmeyen yer sağlayıcı hakkında Başkan tarafından yüz bin Türk lirasından bir milyon Türk lirasına kadar idari para cezası verilir.[2][4]

Erişim sağlayıcının yükümlülükleri

MADDE 6- (1) Erişim sağlayıcı;

a) Herhangi bir kullanıcısının yayınladığı hukuka aykırı içerikten, bu Kanun hükümlerine uygun olarak haberdar edilmesi halinde (…)[3] erişimi engellemekle,[3]

_____

(1) Bu Kararın Resmi Gazete'de yayımlandığı 28/1/2016 tarihinden başlayarak bir yıl sonra yürürlüğe girmesi hüküm altına alınmıştır.

(2) 15/8/2016 tarihli ve 671 sayılı KHK'nin 21 inci maddesiyle, bu maddenin beşinci fıkrasında yer alan "Başkanlığın" ibaresi "Kurumun" şeklinde, "Başkanlığa" ibaresi "Kuruma" şeklinde, "Başkanlıkça" ibaresi "Kurum tarafından" şeklinde ve altıncı fıkrasında yer alan "Başkanlık" ibaresi "Başkan" şeklinde değiştirilmiş olup, daha sonra bu hüküm 9/11/2016 tarihli ve 6757 sayılı Kanunun 18 inci maddesiyle aynen kabul edilerek kanunlaşmıştır.

(3) 6518 sayılı Kanunun 89 uncu maddesiyle bu bentte yer alan "ve teknik olarak engelleme imkânı bulunduğu ölçüde" ibaresi yürürlükten kaldırılmıştır.

(4) 29/7/2020 tarihli ve 7253 sayılı Kanunun 3 üncü maddesiyle, bu fıkrada yer alan "on bin Türk Lirasından yüz bin Türk Lirasına" ibaresi "yüz bin Türk lirasından bir milyon Türk lirasına" şeklinde değiştirilmiştir.

b) Sağladığı hizmetlere ilişkin, yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğru-luğunu, bütünlüğünü ve gizliliğini sağlamakla,

c) Faaliyetine son vereceği tarihten en az üç ay önce durumu Kuruma, içerik sağlayıcılarına ve müşterilerine bildirmek ve trafik bilgilerine ilişkin kayıtları yönetmelikte belirtilen esas ve usûllere uygun olarak Kuruma teslim etmekle,

ç) **(Ek: 6/2/2014-6518/89 md.)** Erişimi engelleme kararı verilen yayınlarla ilgili olarak alternatif erişim yollarını engelleyici tedbirleri almakla,

d) **(Ek: 6/2/2014-6518/89 md.) (İptal: Anayasa Mahkemesinin 8/12/2015 tarihli ve E.: 2014/87, K.: 2015/112 sayılı Kararı ile.)**[1]

yükümlüdür.

(2) Erişim sağlayıcı, kendisi aracılığıyla erişilen bilgilerin içeriklerinin hukuka aykırı olup olmadıklarını ve sorumluluğu gerektirip gerektirmediğini kontrol etmekle yükümlü değildir.

(3) Birinci fıkranın (b), (c), (ç) (…)[3] bentlerinde yer alan yükümlülüklerden birini yerine getirmeyen erişim sağlayıcısına Başkan tarafından onbin Yeni Türk Lirasından ellibin Yeni Türk Li-rasına kadar idarî para cezası verilir.[2][3][4]

Erişim Sağlayıcıları Birliği

MADDE 6/A- (Ek: 6/2/2014-6518/90 md.)

(1) Bu Kanunun 8 inci maddesi kapsamı dışındaki erişimin engellenmesi kararlarının uygulanmasını sağlamak üzere Erişim Sağlayıcıları Birliği kurulmuştur.

(2) Birlik özel hukuk tüzel kişiliğini haizdir. Birliğin merkezi Ankara'dır.

(3) Birliğin çalışma usul ve esasları Kurum tarafından onaylanacak Tüzükle belirlenir. Tüzük değişiklikleri de Kurumun onayına tabidir.

(4) Birlik, Tüzüğünün Kurum tarafından incelenerek uygun bulunmasını müteakip faaliyete başlar.

(5) Birlik, 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu kapsamında yetkilendirilen tüm internet servis sağlayıcıları ile internet erişim hizmeti veren diğer işletmecilerin katılmasıyla oluşan ve koordinasyonu sağlayan bir kuruluştur.

---

(1) Bu Kararın Resmi Gazete'de yayımlandığı 28/1/2016 tarihinden başlayarak bir yıl sonra yürürlüğe girmesi hüküm altına alınmıştır.

(2) 6518 sayılı Kanunun 89 uncu maddesiyle bu bentte yer alan "(b) ve (c)" ibaresi "(b), (c), (ç) ve (d)" şeklinde değiştirilmiştir.

(3) Anayasa Mahkemesinin 8/12/2015 tarihli ve E:2014/87, K:2015/112 sayılı Kararı ile, bu fıkrada yer alan "..ve (d)…" ibaresi iptal edilmiş olup, Kararın Resmi Gazete'de yayımlandığı 28/1/2016 tarihinden başlayarak bir yıl sonra yürürlüğe girmesi hüküm altına alınmıştır.

(4) 15/8/2016 tarihli ve 671 sayılı KHK'nin 21 inci maddesiyle, bu fıkrada yer alan "Başkanlık" ibaresi "Başkan" şeklinde değiştirilmiş olup, daha sonra bu hüküm 9/11/2016 tarihli ve 6757 sayılı Kanunun 18 inci maddesiyle aynen kabul edilerek kanunlaşmıştır.

(6) Bu Kanunun 8 inci maddesi kapsamı dışındaki erişimin engellenmesi kararları erişim sağlayıcılar tarafından yerine getirilir. Kararların uygulanması amacıyla gerekli her türlü donanım ve yazılım erişim sağlayıcıların kendileri tarafından sağlanır.

(7) Bu Kanunun 8 inci maddesi kapsamı dışındaki erişimin engellenmesi kararları gereği için Birliğe gönderilir. Bu kapsamda Birliğe yapılan tebligat erişim sağlayıcılara yapılmış sayılır.

(8) Birlik, kendisine gönderilen mevzuata uygun olmadığını düşündüğü kararlara itiraz edebilir.

(9) Birliğin gelirleri, üyeleri tarafından ödenecek ücretlerden oluşur. Alınacak ücretler, Birliğin giderlerini karşılayacak miktarda belirlenir. Bir üyenin ödeyeceği ücret, üyelerin tamamının net satış tutarı toplamı içindeki o üyenin net satışı oranında belirlenir. Üyelerin ödeme dönemleri, yeni katılan üyelerin ne zamandan itibaren ödemeye başlayacağı ve ödemelere ilişkin diğer hususlar Birlik Tüzüğünde belirlenir. Süresinde ödenmeyen ücretler Birlikçe kanuni faizi ile birlikte tahsil edilir.

(10) Birliğe üye olmayan internet servis sağlayıcıları faaliyette bulunamaz.

Toplu kullanım sağlayıcıların yükümlülükleri

MADDE 7- (1) Ticarî amaçla toplu kullanım sağlayıcılar, mahallî mülkî amirden izin belge-si almakla yükümlüdür. İzne ilişkin bilgiler otuz gün içinde mahallî mülkî amir tarafından Kuruma bildirilir. Bunların denetimi mahallî mülkî amirler tarafından yapılır. İzin belgesinin verilmesine ve denetime ilişkin esas ve usûller, yönetmelikle düzenlenir.

(2) **(Değişik: 6/2/2014-6518/91 md.)** Ticari amaçla olup olmadığına bakılmaksızın bütün internet toplu kullanım sağlayıcılar, konusu suç oluşturan içeriklere erişimin engellenmesi ve kullanıma ilişkin erişim kayıtlarının tutulması hususlarında yönetmelikle belirlenen tedbirleri almakla yükümlüdür.

(3) **(Değişik: 6/2/2014-6518/91 md.)** Ticari amaçla toplu kullanım sağlayıcılar, ailenin ve çocukların korunması, suçun önlenmesi ve suçluların tespiti kapsamında usul ve esasları yönetmelikte belirlenen tedbirleri almakla yükümlüdür.

(4) **(Ek: 6/2/2014-6518/91 md.)** Bu maddede belirtilen yükümlülükleri ihlal eden ticari amaçla toplu kullanım sağlayıcılarına, ihlalin ağırlığına göre yönetmelikle belirlenecek usul ve esaslar çerçevesinde uyarma, bin Türk Lirasından on beş bin Türk Lirasına kadar idari para cezası verme veya üç güne kadar ticari faaliyetlerini durdurma müeyyidelerinden birine karar vermeye mahalli mülki amir yetkilidir.

İçeriğin çıkarılması ve erişimin engellenmesi kararları ile yerine getirilmesi[1]

MADDE 8- (1) İnternet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak içeriğin çıkarılmasına ve/veya erişimin engellenmesine karar verilir:[1]

a) 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununda yer alan;
1) İntihara yönlendirme (madde 84),
2) Çocukların cinsel istismarı (madde 103, birinci fıkra),
3) Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190),
4) Sağlık için tehlikeli madde temini (madde 194),
5) Müstehcenlik (madde 226),
6) Fuhuş (madde 227),
7) Kumar oynanması için yer ve imkân sağlama (madde 228),
suçları.

_____

(1) *29/7/2020 tarihli ve 7253 sayılı Kanunun 4 üncü maddesiyle, bu madde başlığı "Erişimin engellenmesi kararı ve yerine getirilmesi" iken metne işlendiği şekilde değiştirilmiş ve birinci fıkrada yer alan "erişimin engellenmesine" ibaresi "içeriğin çıkarılmasına ve/veya erişimin engellenmesine" şeklinde değiştirilmiştir.*

b) 25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar.

c) **(Ek:25/3/2020-7226/32 md.)** 29/4/1959 tarihli ve 7258 sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanunda yer alan suçlar.

(2) İçeriğin çıkarılması ve/veya erişimin engellenmesi kararı, soruşturma evresinde hâkim, kovuşturma evresinde ise mahkeme tarafından verilir. Soruşturma evresinde, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından da içeriğin çıkarılmasına ve/veya erişimin engellenmesine karar verilebilir. Bu durumda Cumhuriyet savcısı kararını yirmidört saat içinde hâkimin onayına sunar ve hâkim, kararını en geç yirmidört saat içinde verir. Bu süre içinde kararın onaylanmaması halinde tedbir, Cumhuriyet savcısı tarafından derhal kaldırılır. **(Ek cümle: 6/2/2014-6518/92 md.)** Erişimin engellenmesi kararı, amacı gerçekleştirecek nitelikte görülürse belirli bir süreyle sınırlı olarak da verilebilir. Koruma tedbiri olarak verilen içeriğin çıkarılmasına ve/veya erişimin engellenmesine ilişkin karara 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hü-kümlerine göre itiraz edilebilir.[5]

(3) Hâkim, mahkeme veya Cumhuriyet savcısı tarafından verilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararının birer örneği, gereği yapılmak üzere Kuruma gönderilir.[1][5]

(4) İçeriği birinci fıkrada belirtilen suçları oluşturan yayınların içerik veya yer sağlayıcısının yurt dışında bulunması halinde veya içerik veya yer sağlayıcısı yurt içinde bulunsa bile, içeriği birinci fıkranın (a) bendinin (2) ve (5) ve (6) ve (7) numaralı alt bentlerinde ve (c) bendinde yazılı suçları oluşturan yayınlara ilişkin olarak içeriğin çıkarılması ve/veya erişimin engellenmesi kararı re'sen Başkan tarafından verilir. **(Değişik cümle:29/7/2020-7253/4 md.)** Bu karar, ilgili içerik ve yer sağlayıcılar ile erişim sağlayıcısına bildirilerek gereğinin yerine getirilmesi istenir. [1][2][3][4][5]

---

(1) 15/8/2016 tarihli ve 671 sayılı KHK'nin 21 inci maddesiyle, 8 inci maddenin üçüncü fıkrasında yer alan "Başkanlığa" ibaresi "Kuruma" şeklinde, dördüncü fıkrasında yer alan "Başkanlık" ibaresi "Başkan" şeklinde değiştirilmiş olup, daha sonra bu hüküm 9/11/2016 tarihli ve 6757 sayılı Kanunun 18 inci maddesiyle aynen kabul edilerek kanunlaşmıştır.

(2) 6518 sayılı Kanunun 92 nci maddesiyle, bu fıkrada yer alan "(2) ve (5)" ibaresi "(2), (5) ve (6)" şeklinde değiştirilmiştir.

(3) 7/2/2018 tarihli ve 30325 sayılı Resmî Gazete'de yayımlanan Anayasa Mahkemesinin 15/11/2017 tarihli ve E.: 2015/76, K.: 2017/153 sayılı Kararı ile;

a) Bu fıkranın birinci cümlesinde yer alan "İçeriği birinci fıkrada belirtilen suçları oluşturan yayınların içerik veya yer sağlayıcısının yurt dışında bulunması halinde…" ibaresi, bu Kanunun 8 inci maddesinin birinci fıkrasının (a) bendinin (5) numaralı alt bendi yönünden;

b) Bu fıkranın birinci cümlesinde, 15/8/2016 tarihli ve 671 sayılı KHK'nin 21 inci maddesiyle değiştirilmesinden önce yer alan "…yayınlara ilişkin olarak erişimin engellenmesi kararı re'sen Başkanlık tarafından verilir." ibaresi, "İçeriği birinci fıkrada belirtilen suçları oluşturan yayın-ların içerik veya yer sağlayıcısının yurt dışında bulunması halinde…" ibaresi ve bu Kanunun 8 inci maddesinin birinci fıkrasının (a) bendinin (5) numaralı alt bendi yönünden; iptal edilmiş olup, söz konusu kararın Resmî Gazete'de yayımlanmasından başlayarak bir yıl sonra yürürlüğe gireceği hüküm altına alınmıştır.

(4) 25/3/2020 tarihli ve 7226 sayılı Kanunun 32 nci maddesiyle bu bentte yer alan "(6) numaralı alt bentlerinde" ibaresi "(6) ve (7) numaralı alt bentlerinde ve (c) bendinde" şeklinde değiştirilmiştir.

(5) 29/7/2020 tarihli ve 7253 sayılı Kanunun 4 üncü maddesiyle, ikinci fıkranın birinci cümlesinde yer alan "Erişimin engellenmesi" ibaresi "İçeriğin çıkarılması ve/veya erişimin engellenmesi" şeklinde, ikinci ve altıncı cümlelerde yer alan "erişimin engellenmesine" ibareleri "içeriğin çıkarılmasına ve/veya erişimin engellenmesine" şeklinde, üçüncü fıkrada yer alan "erişimin engellenmesi" ibaresi "içeriğin çıkarılması ve/veya erişimin engellenmesi" şeklinde, dördüncü fıkranın birinci cümlesinde yer alan "erişimin engellenmesi" ibaresi "içeriğin çıkarılması ve/veya erişimin engellenmesi" şeklinde değiştirilmiştir.

(5) İçeriğin çıkarılması ve/veya erişimin engellenmesi kararının gereği, derhal ve en geç kararın bildirilmesi anından itibaren dört saat içinde yerine getirilir.[1][5]

(6) Başkan tarafından verilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararının konusunu oluşturan yayını ya-panların kimliklerinin belirlenmesi halinde, Başkan tarafından, Cumhuriyet başsavcılığına suç duyu-rusunda bulunulur.[2][5]

(7) Soruşturma sonucunda kovuşturmaya yer olmadığı kararı verilmesi halinde, içeriğin çıkarılması ve/veya erişimin engellenmesi kararı kendiliğinden hükümsüz kalır. Bu durumda Cumhuriyet savcısı, hükümsüz kalan içeriğin çıkarılması ve/veya erişimin engellenmesi kararına konu internet adresini belirtmek suretiyle, kovuşturmaya yer olmadığı kararının bir örneğini Kuruma gönderir.[2][4][5]

(8) Kovuşturma evresinde beraat kararı verilmesi halinde, içeriğin çıkarılması ve/veya erişimin engellenmesi kararı kendiliğinden hükümsüz kalır. Bu durumda mahkemece hükümsüz kalan içeriğin çıkarılması ve/veya erişimin engellenmesi kararına konu internet adresini belirtmek suretiyle, beraat kararının bir örneği Kuruma gönderilir.[2][4][5]

(9) Konusu birinci fıkrada sayılan suçları oluşturan içeriğin yayından çıkarılması halinde; erişimin engellenmesi kararı, soruşturma evresinde Cumhuriyet savcısı, kovuşturma evresinde mah-keme tarafından kaldırılır.

(10) Koruma tedbiri olarak verilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararının gereğini yerine getirmeyen içerik, yer veya erişim sağlayıcılarının sorumluları, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, beş yüz günden üç bin güne kadar adli para cezası ile cezalandırılır.[3][5]

(11) İdarî tedbir olarak verilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararının yerine getirilmemesi halinde, Başkan tarafından ilgili içerik, yer ve erişim sağlayıcısına, onbin Yeni Türk Lirasından yüzbin Yeni Türk Lirasına kadar idarî para cezası verilir. İdarî para cezasının verildiği andan itibaren yirmidört saat içinde erişim sağlayıcı tarafından kararın yerine getirilmemesi halinde (…)[2] Kurum tarafından yetkilendirmenin iptaline karar verilebilir.[2][5]

(12) Bu Kanunda tanımlanan kabahatler dolayısıyla (…)[2] Kurum tarafından verilen idarî para cezalarına ilişkin kararlara karşı, 6/1/1982 tarihli ve 2577 sayılı İdarî Yargılama Usulü Kanunu hükümlerine göre kanun yoluna başvurulabilir.[2]

(13) **(Ek: 5/11/2008-5809/67 md.)** İşlemlerin yürütülmesi için Kuruma gönderilen hakim ve mahkeme kararlarına 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre Kurum tarafından itiraz edilebilir.[2]

---

(1) 10/9/2014 tarihli ve 6552 sayılı Kanunun 127 nci maddesiyle, bu fıkrada yer alan "yirmi dört saat" ibaresi "dört saat" şeklinde değiştirilmiştir.

(2) 15/8/2016 tarihli ve 671 sayılı KHK'nin 21 inci maddesiyle, 8 inci maddenin altıncı ve onbirinci fıkralarında yer alan "Başkanlık" ibareleri "Başkan" şeklinde; yedinci ve sekizinci fıkralarında yer alan "Başkanlığa" ibareleri "Kuruma" şeklinde; onüçüncü fıkrasında yer alan "Başkanlığa" ibaresi "Kuruma", "Başkanlıkça" ibaresi "Kurum tarafından" şeklinde değiştirilmiş; onbirinci fıkrasında yer alan "ise Başkanlığın talebi üzerine" ibaresi ile onikinci fıkrasında yer alan "Başkanlık veya" ibaresi yürürlükten kaldırılmış olup, daha sonra bu hüküm 9/11/2016 tarihli ve 6757 sayılı Kanunun 18 inci maddesiyle aynen kabul edilerek kanunlaşmıştır.

(3) 6518 sayılı Kanunun 92 nci maddesiyle bu fıkrada yer alan "altı aydan iki yıla kadar hapis cezası" ibaresi "beş yüz günden üç bin güne kadar adli para cezası" şeklinde değiştirilmiştir.

(4) 17/10/2019 tarihli ve 7188 sayılı Kanunun 36 ncı maddesiyle yedinci fıkraya "Cumhuriyet savcısı,", sekizinci fıkraya "mahkemece" ibarelerinden sonra gelmek üzere "hükümsüz kalan erişimin engellenmesi kararına konu internet adresini belirtmek suretiyle," ibaresi eklenmiştir.

(5) 29/7/2020 tarihli ve 7253 sayılı Kanunun 4 üncü maddesiyle, beşinci fıkrada yer alan "Erişimin engellenmesi" ibaresi "İçeriğin çıkarılması ve/veya erişimin engellenmesi" şeklinde, altıncı fıkrada yer alan "erişimin engellenmesi" ibaresi "içeriğin çıkarılması ve/veya erişimin engellenmesi" şeklinde, yedinci fıkranın birinci ve ikinci cümlelerinde yer alan "erişimin engellenmesi" ibareleri "içeriğin çıkarılması ve/veya erişimin engellenmesi" şeklinde, sekizinci fıkranın birinci ve ikinci cümlelerinde yer alan "erişimin engellenmesi" ibareleri "içeriğin çıkarılması ve/veya erişimin engellenmesi" şeklinde, onuncu fıkrada yer alan "erişimin engellenmesi kararının gereğini yerine getirmeyen" ibaresi "içeriğin çıkarılması ve/veya

erişimin engellenmesi kararının gereğini yerine getirmeyen içerik," şeklinde, onbirinci fıkrada yer alan "erişimin engellenmesi" ibaresi "içeriğin çıkarılması ve/veya erişimin engellenmesi" şeklinde, "erişim sağlayıcısına" ibaresi "ilgili içerik, yer ve erişim sağlayıcısına" şeklinde değiştirilmiş, aynı fıkraya "yirmidört saat içinde" ibaresinden sonra gelmek üzere "erişim sağlayıcı tarafından" ibaresi eklenmiştir.

(14) **(Ek: 12/7/2013-6495/47 md.)** 14/3/2007 tarihli ve 5602 sayılı Şans Oyunları Hasılatından Alınan Vergi, Fon ve Payların Düzenlenmesi Hakkında Kanunun 3 üncü maddesinin birinci fıkrasının (ç) bendinde tanımlanan kurum ve kuruluşlar, kendi görev alanına giren suçların internet ortamında işlendiğini tespit etmeleri hâlinde, bu yayınlarla ilgili olarak erişimin engellenmesi kararı alabilirler. Erişimin engellenmesi kararları uygulanmak üzere Kuruma gönderilir.(1)

(15) **(Ek: 26/2/2014-6527/17 md.)** Bu maddeye göre soruşturma aşamasında verilen hâkim kararı ile 9 uncu ve 9/A maddesine göre verilen hâkim kararı birden fazla sulh ceza mahkemesi bulunan yerlerde Hâkimler ve Savcılar Yüksek Kurulu tarafından belirlenen sulh ceza mahkemeleri tarafından verilir.

(16) **(Ek: 10/9/2014-6552/127 md.; İptal: Anayasa Mahkemesinin 2/10/2014 tarihli ve E.: 2014/149, K.: 2014/151 sayılı Kararı ile.)(2)**

(17) **(Ek:17/10/2019-7188/36 md.)** Bu maddenin ikinci, dördüncü ve ondördüncü fıkraları kapsamında verilen erişimin engellenmesi kararları, ihlalin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL vb. şeklinde) içeriğe erişimin engellenmesi yöntemiyle verilir. Ancak, teknik olarak ihlale ilişkin içeriğe erişimin engellenmesi yapılamadığı veya ilgili içeriğe erişimin engellenmesi yoluyla ihlalin önlenemediği durumlarda, internet sitesinin tümüne yönelik olarak erişimin engellenmesi kararı verilebilir.

Gecikmesinde sakınca bulunan hâllerde içeriğin çıkarılması ve/veya erişimin engellenmesi(3)(4)

MADDE 8/A- (Ek: 27/3/2015-6639/29 md.)

(1) Yaşam hakkı ile kişilerin can ve mal güvenliğinin korunması, millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması sebeplerinden bir veya bir kaçına bağlı olarak hâkim veya gecikmesinde sakınca bulunan hâllerde, Cumhurbaşkanlığı veya millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması ile ilgili bakanlıkların talebi üzerine Başkan tarafından internet ortamında yer alan yayınla ilgili olarak içeriğin çıkarılması ve/veya erişimin engellenmesi kararı verilebilir. Karar, Başkan tarafından derhâl erişim sağlayıcılara ve ilgili içerik ve yer sağlayıcılara bildirilir. İçerik çıkartılması ve/veya erişimin engellenmesi kararının gereği, derhâl ve en geç kararın bildirilmesi anından itibaren dört saat içinde yerine getirilir.(3)(4)

(2) Cumhurbaşkanlığı veya ilgili Bakanlıkların talebi üzerine Başkan tarafından verilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararı, Başkan tarafından, yirmi dört saat içinde sulh ceza hâkiminin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar; aksi hâlde, karar kendiliğinden kalkar.(3)(4)

(3) Bu madde kapsamında verilen erişimin engellenmesi kararları, ihlalin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL, vb. şeklinde) içeriğe erişimin engellenmesi yöntemiyle verilir. Ancak, teknik olarak ihlale ilişkin içeriğe erişimin engellenmesi yapılamadığı veya ilgili içeriğe erişimin engellenmesi yoluyla ihlalin önlenemediği durumlarda, internet sitesinin tümüne yönelik olarak erişimin engellenmesi kararı verilebilir.

---

(1) 15/8/2016 tarihli ve 671 sayılı KHK'nin 21 inci maddesiyle,bu fıkrada yer alan "Telekomünikasyon İletişim Başkanlığına" ibaresi "Kuruma" şeklinde değiştirilmiş olup, daha sonra bu hüküm 9/11/2016 tarihli ve 6757 sayılı Kanunun 18 inci maddesiyle aynen kabul edilerek kanunlaşmıştır.

(2) Bu İptal Kararı 1/1/2015 tarihli ve 29223 sayılı Resmî Gazete'de yayımlanmıştır.

(3) 15/8/2016 tarihli ve 671 sayılı KHK'nin 21 inci maddesiyle, bu maddenin birinci ve ikinci fıkralarında yer alan "Başkanlık" ibareleri "Başkan" şeklinde değiştirilmiş olup, daha sonra

bu hüküm 9/11/2016 tarihli ve 6757 sayılı Kanunun 18 inci maddesiyle aynen kabul edilerek kanunlaşmıştır.

(4) 2/7/2018 tarihli ve 700 sayılı Kanun Hükmünde Kararnamenin 181 inci maddesiyle bu maddenin birinci ve ikinci fıkralarında yer alan "Başbakanlık" ibareleri "Cumhurbaşkanlığı"şeklinde değiştirilmiştir.

(4) Bu madde kapsamındaki suça konu internet içeriklerini oluşturan ve yayanlar hakkında Başkan tarafından, Cumhuriyet Başsavcılığına suç duyurusunda bulunulur. Bu suçların faillerine ulaşmak için gerekli olan bilgiler içerik, yer ve erişim sağlayıcılar tarafından hâkim kararı üzerine adli mercilere verilir. Bu bilgileri vermeyen içerik, yer ve erişim sağlayıcıların sorumluları, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, üç bin günden on bin güne kadar adli para cezası ile cezalandırılır.(1)

(5) Bu madde uyarınca verilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararının gereğini yerine getirmeyen erişim sağlayıcılar ile ilgili içerik ve yer sağlayıcılara Başkan tarafından elli bin Türk lirasından beş yüz bin Türk lirasına kadar idari para cezası verilir.(1)

İçeriğin yayından çıkarılması ve erişimin engellenmesi(2)

MADDE 9- (Değişik: 6/2/2014-6518/93 md.)

(1) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden gerçek ve tüzel kişiler ile kurum ve kuruluşlar, içerik sağlayıcısına, buna ulaşamaması hâlinde yer sağlayıcısına başvurarak uyarı yöntemi ile içeriğin yayından çıkarılmasını isteyebileceği gibi doğrudan sulh ceza hâkimine başvurarak içeriğin çıkarılmasını ve/veya erişimin engellenmesini de isteyebilir.(3)

(2) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden kişilerin talepleri, içerik ve/veya yer sağlayıcısı tarafından en geç yirmi dört saat içinde cevaplandırılır.

(3) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik hakları ihlal edilenlerin talepleri doğrultusunda hâkim bu maddede belirtilen kapsamda içeriğin çıkarılmasına ve/veya erişimin engellenmesine karar verebilir.(3)

(4) Hâkim, bu madde kapsamında vereceği erişimin engellenmesi kararlarını esas olarak, yalnızca kişilik hakkının ihlalinin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL, vb. şeklinde) içeriğe erişimin engellenmesi yöntemiyle verir. Zorunlu olmadıkça internet sitesinde yapılan yayının tümüne yönelik erişimin engellenmesine karar verilemez. Ancak, hâkim URL adresi belirtilerek içeriğe erişimin engellenmesi yöntemiyle ihlalin engellenemeyeceğine kanaat getirmesi hâlinde, gerekçesini de belirtmek kaydıyla, internet sitesindeki tüm yayına yönelik olarak erişimin engellenmesine de karar verebilir.

(5) Hâkimin bu madde kapsamında verdiği içeriğin çıkarılması ve/veya erişimin engellenmesi kararları doğrudan Birliğe gönderilir.(3)

---

(1) 15/8/2016 tarihli ve 671 sayılı KHK'nin 21 inci maddesiyle, 8/A maddesinin dördüncü fıkrasında yer alan "Başkanlık" ibaresi "Başkan" şeklinde değiştirilmiş; beşinci fıkrasına "yer sağlayıcılara" ibaresinden sonra gelmek üzere "Başkan tarafından" ibaresi eklenmiş olup, daha sonra bu hüküm 9/11/2016 tarihli ve 6757 sayılı Kanunun 18 inci maddesiyle aynen kabul edilerek kanunlaşmıştır.

(2) Bu maddenin başlığı "İçeriğin yayından çıkarılması ve cevap hakkı" iken 6518 sayılı Kanunun 93 üncü maddesiyle metne işlendiği şekilde değiştirilmiştir.

(3) *29/7/2020 tarihli ve 7253 sayılı Kanunun 5 inci maddesiyle, birinci fıkrada yer alan "içeriğe erişimin engellenmesini" ibaresi "içeriğin çıkarılmasını ve/veya erişimin engellenmesini" şeklinde, üçüncü fıkrada yer alan "erişimin engellenmesine" ibaresi "içeriğin çıkarılmasına ve/veya erişimin engellenmesine" şeklinde, beşinci fıkrada yer alan "erişimin engellenmesi" ibaresi "içeriğin çıkarılması ve/veya erişimin engellenmesi" şeklinde değiştirilmiştir.*

(6) Hâkim bu madde kapsamında yapılan başvuruyu en geç yirmi dört saat içinde duruşma yapmaksızın karara bağlar. Bu karara karşı 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre itiraz yoluna gidilebilir.

(7) Erişimin engellenmesine konu içeriğin yayından çıkarılmış olması durumunda hâkim kararı kendiliğinden hükümsüz kalır.

(8) **(Değişik:29/7/2020-7253/5 md.)** Birlik tarafından ilgili içerik ve yer sağlayıcılar ile erişim sağlayıcıya gönderilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararının gereği derhâl, en geç dört saat içinde ilgili içerik ve yer sağlayıcılar ile erişim sağlayıcı tarafından yerine getirilir.

(9) Bu madde kapsamında hâkimin verdiği içeriğin çıkarılması ve/veya erişimin engellenmesi kararına konu kişilik hakkının ihlaline ilişkin yayının (…)[1] başka internet adreslerinde de yayınlanması durumunda ilgili kişi tarafından Birliğe müracaat edilmesi hâlinde mevcut karar bu adresler için de uygulanır.[1][3]

(10) **(Ek:29/7/2020-7253/5 md.)** İnternet ortamında yapılan yayın içeriği nedeniyle kişilik hakları ihlal edilenlerin talep etmesi durumunda hâkim tarafından, başvuranın adının bu madde kapsamındaki karara konu internet adresleri ile ilişkilendirilmemesine karar verilebilir. Kararda, Birlik tarafından hangi arama motorlarına bildirim yapılacağı gösterilir.[3]

(11) Sulh ceza hâkiminin kararını bu maddede belirtilen şartlara uygun olarak ve süresinde yerine getirmeyen içerik, yer ve erişim sağlayıcıların sorumluları, beş yüz günden üç bin güne kadar adli para cezası ile cezalandırılır.[3]

Özel hayatın gizliliği nedeniyle içeriğe erişimin engellenmesi[2]
MADDE 9/A- (Ek: 6/2/2014-6518/94 md.)

(1) İnternet ortamında yapılan yayın içeriği nedeniyle özel hayatının gizliliğinin ihlal edildiğini iddia eden kişiler, Kuruma doğrudan başvurarak içeriğe erişimin engellenmesi tedbirinin uygulanmasını isteyebilir.[2]

(2) Yapılan bu istekte; hakkın ihlaline neden olan yayının tam adresi (URL), hangi açılardan hakkın ihlal edildiğine ilişkin açıklama ve kimlik bilgilerini ispatlayacak bilgilere yer verilir. Bu bilgilerde eksiklik olması hâlinde talep işleme konulmaz.

(3) Başkan, kendisine gelen bu talebi uygulanmak üzere derhâl Birliğe bildirir, erişim sağlayıcılar bu tedbir talebini derhâl, en geç dört saat içinde yerine getirir.[2]

(4) Erişimin engellenmesi, özel hayatın gizliliğini ihlal eden yayın, kısım, bölüm, resim, video ile ilgili olarak (URL şeklinde) içeriğe erişimin engellenmesi yoluyla uygulanır.

(5) Erişimin engellenmesini talep eden kişiler, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edildiğinden bahisle erişimin engellenmesi talebini talepte bulunduğu saatten itibaren yirmi dört saat içinde sulh ceza hâkiminin kararına sunar. Hâkim, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edilip edilmediğini değerlendirerek vereceği kararını en geç kırk sekiz saat içinde açıklar ve doğrudan Kuruma gönderir; aksi hâlde, erişimin engellenmesi tedbiri kendiliğinden kalkar.[2]

---

(1) 28/1/2016 tarihli ve 29607 sayılı Resmî Gazete'de yayımlanan Anayasa Mahkemesinin 8/12/2015 tarihli ve E.: 2014/87, K.: 2015/112 sayılı Kararı ile bu fıkrada yer alan "…veya aynı mahiyetteki yayınların…" ibaresi iptal edilmiştir.

(2) 15/8/2016 tarihli ve 671 sayılı KHK'nin 21 inci maddesiyle, bu maddenin birinci ve beşinci fıkralarında yer alan "Başkanlığa" ibareleri "Kuruma" şeklinde, üçüncü fıkrasında yer alan "Başkanlık" ibaresi "Başkan" şeklinde değiştirilmiş olup, daha sonra bu hüküm 9/11/2016 tarihli ve 6757 sayılı Kanunun 18 inci maddesiyle aynen kabul edilerek kanunlaşmıştır.

(3) 29/7/2020 tarihli ve 7253 sayılı Kanunun 5 inci maddesiyle, dokuzuncu fıkrada yer alan "erişimin engellenmesi" ibaresi "içeriğin çıkarılması ve/veya erişimin engellenmesi" şeklinde değiştirilmiş, maddeye dokuzuncu fıkradan sonra gelmek üzere onuncu fıkra eklenmiş, mevcut onuncu fıkra buna göre teselsül ettirilmiş ve aynı fıkrada yer alan "sorumlu kişi" ibaresi "içerik, yer ve erişim sağlayıcıların sorumluları" şeklinde değiştirilmiştir.

(6) Hâkim tarafından verilen bu karara karşı Başkan tarafından 5271 sayılı Kanun hükümlerine göre itiraz yoluna gidilebilir.[1]

(7) Erişimin engellenmesine konu içeriğin yayından çıkarılmış olması durumunda hâkim kararı kendiliğinden hükümsüz kalır.

(8) Özel hayatın gizliliğinin ihlaline bağlı olarak gecikmesinde sakınca bulunan hâllerde doğrudan Başkanın emri üzerine erişimin engellenmesi Kurum tarafından yapılır. **(Mülga cümle: 26/2/2014-6527/18 md.)**[1]

(9) **(Ek: 26/2/2014-6527/18 md.)** Bu maddenin sekizinci fıkrası kapsamında Başkan tarafından verilen erişimin engellenmesi kararı, (…)[1] yirmi dört saat içinde sulh ceza hâkiminin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar.[1]

İdarî yapı ve görevler[2]

MADDE 10- (1) Kanunla verilen görevler, Kurum tarafından yerine getirilir.[2]

(2) Bu Kanunla ekli listedeki kadrolar ihdas edilerek Kurumun hizmetlerinde kullanılmak üzere 5/4/1983 tarihli ve 2813 sayılı Telsiz Kanununa ekli (II) sayılı listeye eklenmiştir. **(Mülga ikinci ve üçüncü cümle: 15/8/2016-KHK-671/21 md.; Aynen kabul: 9/11/2016-6757/18 md.)**[2]

(3) Kuruma Kanunla verilen görevlere ilişkin olarak yapılacak her türlü mal veya hizmet alımları, ceza ve ihalelerden yasaklama işleri hariç, 4/1/2002 tarihli ve 4734 sayılı Kamu İhale Kanunu ile 5/1/2002 tarihli ve 4735 sayılı Kamu İhale Sözleşmeleri Kanunu hükümlerine tâbi olmaksızın Kurum bütçesinden karşılanır.[2]

(4) Kanunlarla verilen diğer yetki ve görevleri saklı kalmak kaydıyla, Kurumun bu Kanun kapsamındaki görev ve yetkileri şunlardır:[2]

a) Bakanlık, kolluk kuvvetleri, ilgili kamu kurum ve kuruluşları ile içerik, yer ve erişim sağlayıcılar ve ilgili sivil toplum kuruluşları arasında koordinasyon oluşturarak internet ortamında yapılan ve bu Kanun kapsamına giren suçları oluşturan içeriğe sahip faaliyet ve yayınları önlemeye, internetin güvenli kullanımını sağlamaya, bilişim şuurunu geliştirmeye yönelik çalışmalar yapmak, bu amaçla, gerektiğinde, her türlü giderleri yönetmelikle belirlenecek esas ve usûller dahilinde Kurumca karşılanacak çalışma kurulları oluşturmak.[3]

---

(1) 15/8/2016 tarihli ve 671 sayılı KHK'nin 21 inci maddesiyle, 9/A maddesinin altıncı fıkrasında yer alan "Başkanlık" ibaresi "Başkan" şeklinde, sekizinci fıkrasında yer alan "Başkanlık" ibaresi "Kurum" şeklinde değiştirilmiş ve dokuzuncu fıkrasında yer alan "Başkanlık tarafından," ibaresi yürürlükten kaldırılmış olup, daha sonra bu hüküm 9/11/2016 tarihli ve 6757 sayılı Kanunun 18 inci maddesiyle aynen kabul edilerek kanunlaşmıştır.

(2) 15/8/2016 tarihli ve 671 sayılı KHK'nin 21 inci maddesiyle, bu maddenin birinci fıkrasında yer alan "bünyesinde bulunan Başkanlıkça" ibaresi "tarafından" şeklinde, ikinci ve dördüncü fıkralarında yer alan "Başkanlığın" ibareleri "Kurumun" şeklinde, üçüncü fıkrasında yer alan "Başkanlığa" ibaresi "Kuruma" şeklinde değiştirilmiş olup, daha sonra bu hüküm 9/11/2016 tarihli ve 6757 sayılı Kanunun 18 inci maddesiyle aynen kabul edilerek kanunlaşmıştır.

(3) 6518 sayılı Kanunun 95 inci maddesiyle bu bentte yer alan "yayınları önlemeye" ibaresinden sonra ", internetin güvenli kullanımını sağlamaya, bilişim şuurunu geliştirmeye" ibaresi eklenmiştir.

b) İnternet ortamında yapılan yayınların içeriklerini izleyerek, bu Kanun kapsamına giren suçların işlendiğinin tespiti halinde, bu yayınlara erişimin engellenmesine yönelik olarak bu Kanunda öngörülen gerekli tedbirleri almak.

c) İnternet ortamında yapılan yayınların içeriklerinin izlenmesinin hangi seviye, zaman ve şekilde yapılacağını belirlemek.

ç) Kurum tarafından işletmecilerin yetkilendirilmeleri ile mülkî idare amirlerince ticarî amaçlı toplu kullanım sağlayıcılara verilecek izin belgelerinde filtreleme ve bloke etmede kullanılacak sistemlere ve yapılacak düzenlemelere yönelik esas ve usûlleri belirlemek.

d) İnternet ortamındaki yayınların izlenmesi suretiyle bu Kanunun 8 inci maddesi ile 8/A maddesinde sayılan suçların işlenmesini önlemek için izleme ve bilgi ihbar merkezi dahil, gerekli her türlü teknik altyapıyı kurmak veya kurdurmak, bu altyapıyı işletmek veya işletilmesini sağlamak.(1)

e) İnternet ortamında herkese açık çeşitli servislerde yapılacak filtreleme, perdeleme ve izleme esaslarına göre donanım üretilmesi veya yazılım yapılmasına ilişkin asgari kriterleri belirlemek.

f) Bilişim ve internet alanındaki uluslararası kurum ve kuruluşlarla işbirliği ve koordinasyonu sağlamak.

g) Bu Kanunun 8 inci maddesinin birinci fıkrasında sayılan suçların, internet ortamında işlenmesini konu alan her türlü temsili görüntü, yazı veya sesleri içeren ürünlerin tanıtımı, ülkeye sokulması, bulundurulması, kiraya verilmesi veya satışının önlenmesini teminen yetkili ve görevli kolluk kuvvetleri ile soruşturma mercilerine, teknik imkânları dahilinde gereken her türlü yardımda bulunmak ve koordinasyonu sağlamak.

(5) **(Değişik: 6/2/2014-6518/95 md.)** Kurum; Bakanlık bünyesinde 26/9/2011 tarihli ve 655 sayılı Ulaştırma, Denizcilik ve Haberleşme Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname hükümleri uyarınca oluşturulan İnternet Geliştirme Kurulunca internetin yaygınlaştırılması, geliştirilmesi, yaygın ve güvenli kullanılması gibi konularda yapılacak öneriler ile ilgili gerekli her türlü tedbir veya kararları alır.(1)

(6) **(Ek: 6/2/2014-6518/95 md.)** Kurum, ulusal siber güvenlik faaliyetleri kapsamında, siber saldırıların tespiti ve önlenmesi konusunda, içerik, yer, erişim sağlayıcılar ve ilgili diğer kurum ve kuruluşlarla koordinasyon sağlar, gerekli tedbirlerin aldırılması konusunda faaliyet yürütür ve ihtiyaç duyulan çalışmaları yapar.(1)

(7) **(Ek: 6/2/2014-6518/95 md.)** Kurum kanunlarla kendisine verilen görevlerin ifası amacıyla araştırma ve geliştirme merkezleri kurabilir.(1)

---

(1) 15/8/2016 tarihli ve 671 sayılı KHK'nin 21 inci maddesiyle, 10 uncu maddenin dördüncü fıkrasının (d) bendinde yer alan "bu Kanunun 8 inci maddesinin birinci fıkrasında" ibaresi "bu Kanunun 8 inci maddesi ile 8/A maddesinde" şeklinde; beşinci, altıncı ve yedinci fıkralarında yer alan "Başkanlık" ibareleri "Kurum" şeklinde değiştirilmiş olup, daha sonra bu hüküm 9/11/2016 tarihli ve 6757 sayılı Kanunun 18 inci maddesiyle aynen kabul edilerek kanunlaşmıştır.

Yönetmelikler

MADDE 11- (1) Bu Kanunun uygulanmasına ilişkin esas ve usûller, Cumhurbaşkanı tarafından çıkarılacak yönetmeliklerle düzenlenir. Bu yönetmelikler, Kanunun yürürlüğe girdiği tarihten itibaren dört ay içinde çıkarılır.(1)

(2) Yer veya erişim sağlayıcı olarak faaliyet icra etmek isteyen kişilere, telekomünikasyon yoluyla iletişim konusunda yetkilendirme belgesi olup olmadığına bakılmaksızın, yer, erişim ve toplu kullanım sağlayıcıların yükümlülüklerine ilişkin esas ve usûller, Kurum tarafından çıkarılacak yönetmelikle düzenlenir. Bu yönetmelik, Kanunun yürürlüğe girdiği tarihten itibaren beş ay içinde çıkarılır.(2)

İlgili kanunlarda yapılan değişiklikler

MADDE 12- (1) (4/2/1924 tarihli ve 406 sayılı Telgraf ve Telefon Kanunu ile ilgili olup yerine işlenmiştir.)

(2) (4/7/1934 tarihli ve 2559 sayılı Polis Vazife ve Salahiyet Kanunu ile ilgili olup yerine işlenmiştir.)

(3) (5/4/1983 tarihli ve 2813 sayılı Telsiz Kanunu ile ilgili olup yerine işlenmiştir.)

(4) (1/11/1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu ile ilgili olup yerine işlenmiştir.)

EK MADDE 1- (Ek: 5/11/2008-5809/67 md.)[3]

(1) **(Mülga: 15/8/2016-KHK-671/21 md.; Aynen kabul: 9/11/2016-6757/18 md.)**

(2) **(Mülga: 15/8/2016-KHK-671/21 md.; Aynen kabul: 9/11/2016-6757/18 md.)**

(3) **(Mülga: 15/8/2016-KHK-671/21 md.; Aynen kabul: 9/11/2016-6757/18 md.)**

(4) **(Mülga: 15/8/2016-KHK-671/21 md.; Aynen kabul: 9/11/2016-6757/18 md.)**

(5) **(Ek: 6/2/2014-6518/97 md.)** 8/6/1984 tarihli ve 217 sayılı Devlet Personel Başkanlığı Kuruluş ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 2 nci maddesinde sayılan kamu kurum ve kuruluşlarında çalışanlar kurumlarının, hâkim ve savcılar ise kendilerinin muvafakati ile aylık, ödenek, her türlü zam ve tazminatlar ile diğer mali ve sosyal hak ve yardımları kurumlarınca ödenmek kaydıyla geçici olarak Kurum emrinde görevlendirilebilir. Bu kapsamda görevlendirilen personel sayısı Kurumun kadro sayısının yüzde yirmisini geçemez. Bu personel kurumlarından izinli sayılır. İzinli oldukları sürece memuriyetleri ile ilgili özlük hakları devam eder ve bu süreler terfi ve emekliliklerinde hesaba katılır. Terfileri başkaca bir işleme gerek kalmaksızın süresinde yapılır.[3][4]

(6) **(Ek: 6/2/2014-6518/97 md.; Mülga: 15/8/2016-KHK-671/21 md.; Aynen kabul: 9/11/2016-6757/18 md.)**[5]

(7) Bu Kanunla ekli (V) sayılı cetveldeki kadrolar ihdas edilerek Telekomünikasyon İletişim Başkanlığı hizmetlerinde kullanılmak üzere 5651 sayılı Kanuna ekli (I) sayılı listeye eklenmiştir.[5]

---

(1) 2/7/2018 tarihli ve 700 sayılı Kanun Hükmünde Kararnamenin 181 inci maddesiyle bu fıkrada yer alan "Adalet, İçişleri ve Ulaştırma bakanlıklarının görüşleri alınarak Başbakanlık" ibaresi "Cumhurbaşkanı"şeklinde değiştirilmiştir.

(2) 6/2/2014 tarihli ve 6815 sayılı Kanunun 96 ncı maddesiyle bu fıkrada yer alan "yer veya erişim sağlayıcı olarak faaliyet icra etmesi amacıyla yetkilendirme belgesi verilmesine" ibaresi "yer, erişim ve toplu kullanım sağlayıcıların yükümlülüklerine" şeklinde değiştirilmiştir.

(3) 6518 sayılı Kanunun 97 nci maddesiyle bu maddeye dördüncü fıkradan sonra gelmek üzere beşinci ve altıncı fıkralar eklenmiş ve mevcut beşinci fıkra yedinci fıkra olarak teselsül ettirilmiştir.

(4) 15/8/2016 tarihli ve 671 sayılı KHK'nin 21 inci maddesiyle, bu fıkrada yer alan "Telekomünikasyon İletişim Başkanlığı" ibaresi "Kurum" şeklinde değiştirilmiş olup, daha sonra bu hüküm 9/11/2016 tarihli ve 6757 sayılı Kanunun 18 inci maddesiyle aynen kabul edilerek kanunlaşmıştır.

(5) 6518 sayılı Kanunun 97 nci maddesiyle Ek Madde 1'e dördüncü fıkradan sonra gelmek üzere beşinci ve altıncı fıkralar eklenmiş ve mevcut beşinci fıkra yedinci fıkra olarak teselsül ettirilmiştir.

EK MADDE 2- (Ek: 6/2/2014-6518/99 md.)[1]

Kuruma verilen görevlerin yürütülmesi için, 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanunu ile diğer kanunların sözleşmeli personel çalıştırılmasına dair hükümlerine bağlı kalınmaksızın özel bilgi ve ihtisas gerektiren konularda Kurumda sözleşmeli personel çalıştırılabilir. Bu suretle çalıştırılacakların unvanı, sayısı, süresi, ücretleri ve diğer hususlar Cumhurbaşkanınca yürürlüğe konulacak hizmet sözleşmesi esaslarına göre tespit edilir. Bunlara ödenecek ücret, 657 sayılı Kanunun 4 üncü maddesinin (B) bendine göre çalıştırılanlar için uygulanmakta olan sözleşme ücreti tavanının beş katını, çalıştırılabilecek toplam sözleşmeli personel sayısı ise ikiyüzelliyi geçemez ve bu fıkrada belirtilen ücret dışında herhangi bir ödeme yapılamaz.[2]

EK MADDE 3- (Ek: 15/8/2016-KHK-671/22 md.; Aynen kabul: 9/11/2016-6757/19 md.)

(1) Telekomünikasyon İletişim Başkanlığı kapatılmıştır.

(2) Diğer mevzuatta Telekomünikasyon İletişim Başkanlığına yapılan atıflar Bilgi Teknolojileri ve İletişim Kurumuna, Telekomünikasyon İletişim Başkanına yapılan atıflar Bilgi Teknolojileri ve İletişim Kurumu Başkanına yapılmış sayılır.

EK MADDE 4 – (Ek:29/7/2020-7253/6 md.)

(1) Türkiye'den günlük erişimi bir milyondan fazla olan yurt dışı kaynaklı sosyal ağ sağlayıcı; Kurum, Birlik, adli veya idari makamlarca gönderilecek tebligat, bildirim veya taleplerin gereğinin yerine getirilmesi ve kişiler tarafından bu Kanun kapsamında yapılacak başvuruların cevaplandırılması ve bu Kanun kapsamındaki diğer yükümlülüklerin yerine getirilmesini temin için yetkili en az bir kişiyi Türkiye'de temsilci olarak belirler ve bu kişinin iletişim bilgilerine kolayca görülebilecek ve doğrudan erişilebilecek şekilde internet sitesinde yer verir. Sosyal ağ sağlayıcı bu kişinin kimlik ve iletişim bilgilerini Kuruma bildirmekle yükümlüdür. Temsilcinin gerçek kişi olması hâlinde Türk vatandaşı olması zorunludur.

(2) Birinci fıkrada düzenlenen temsilci belirleme ve bildirme yükümlülüğünü yerine getirmeyen sosyal ağ sağlayıcıya, Kurum tarafından bildirimde bulunulur. Bildirimden itibaren otuz gün içinde bu yükümlülüğün yerine getirilmemesi hâlinde sosyal ağ sağlayıcıya Başkan tarafından on milyon Türk lirası idari para cezası verilir. Verilen idari para cezasının tebliğinden itibaren otuz gün içinde bu yükümlülüğün yerine getirilmemesi hâlinde otuz milyon Türk lirası daha idari para cezası verilir. İkinci kez verilen idari para cezasının tebliğinden itibaren otuz gün içinde bu yükümlülüğün yerine getirilmemesi hâlinde Başkan tarafından Türkiye'de mukim vergi mükellefi olan gerçek ve tüzel kişilerin ilgili sosyal ağ sağlayıcısına yeni reklam vermesi yasaklanır, bu kapsamda yeni sözleşme kurulamaz ve buna ilişkin para transferi yapılamaz. Reklam yasağı kararının verildiği tarihten itibaren üç ay içinde bu yükümlülüğün yerine getirilmemesi hâlinde Başkan, sosyal ağ sağlayıcının internet trafiği bant genişliğinin yüzde elli oranında daraltılması için sulh ceza hâkimliğine başvurabilir. Başvurunun kabulüne ilişkin hâkim kararının uygulanmasından itibaren otuz gün içinde söz konusu yükümlülüğün yerine getirilmemesi hâlinde Başkan, sosyal ağ sağlayıcının internet trafiği bant genişliğinin yüzde doksan oranına kadar daraltılması için sulh ceza hâkimliğine başvurabilir. Hâkim ikinci başvuru üzerine vereceği kararında, yüzde elliden düşük olmamak kaydıyla, sunulan hizmetin niteliğini de dikkate alarak daha düşük bir oran belirleyebilir. Bu kararlara karşı Başkan tarafından 5271 sayılı Kanun hükümlerine göre itiraz yoluna gidilebilir. Hâkim tarafından verilen kararlar erişim sağlayıcılara bildirilmek üzere Kuruma gönderilir. Kararların gereği, bildirimden itibaren derhâl ve en geç dört saat içinde erişim sağlayıcıları tarafından yerine getirilir. Temsilci belirleme ve bildirme yükümlülüğünün yerine getirilmesi hâlinde; verilen idari para cezalarının dörtte biri tahsil edilir, reklam yasağı kaldırılır ve hâkim kararları kendiliğinden hükümsüz kalır. İnternet trafiği bant genişliğine yapılan müdahalenin sona erdirilmesi için erişim sağlayıcılara Kurum tarafından bildirim yapılır.

(1) 15/8/2016 tarihli ve 671 sayılı KHK'nin 21 inci maddesiyle, bu maddenin birinci fıkrasında yer alan "Başkanlığa" ibaresi "Kuruma" şeklinde, "Başkanlıkta" ibaresi "Kurumda" şeklinde ve "yetmiş beşi" ibaresi " ikiyüzelliyi " şeklinde değiştirilmiş olup, daha sonra bu hüküm 9/11/2016 tarihli ve 6757 sayılı Kanunun 18 inci maddesiyle aynen kabul edilerek kanunlaşmıştır.

(2) 2/7/2018 tarihli ve 700 sayılı Kanun Hükmünde Kararnamenin 181 inci maddesiyle bu fıkrada yer alan "Bakanlar Kurulunca" ibaresi "Cumhurbaşkanınca"şeklinde değiştirilmiştir.

(3) Türkiye'den günlük erişimi bir milyondan fazla olan yurt içi veya yurt dışı kaynaklı sosyal ağ sağlayıcı, 9 uncu ve 9/A maddeleri kapsamındaki içeriklere yönelik olarak kişiler tarafından yapılacak başvurulara, başvurudan itibaren en geç kırk sekiz saat içinde olumlu ya da olumsuz cevap vermekle yükümlüdür. Olumsuz cevaplar gerekçeli olarak verilir.

(4) Türkiye'den günlük erişimi bir milyondan fazla olan yurt içi veya yurt dışı kaynaklı sosyal ağ sağlayıcı, kendisine bildirilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararlarının uygulanmasına ve üçüncü fıkra kapsamındaki başvurulara ilişkin istatistiksel ve kategorik bilgileri içeren Türkçe hazırlanmış raporları altı aylık dönemlerle Kuruma bildirir. Üçüncü fıkra kapsamındaki başvurulara ilişkin rapor, kişisel verilerden arındırılmak suretiyle sosyal ağ sağlayıcının kendi internet sitesinde de yayınlanır.

(5) Türkiye'den günlük erişimi bir milyondan fazla olan yurt içi veya yurt dışı kaynaklı sosyal ağ sağlayıcı, Türkiye'deki kullanıcıların verilerini Türkiye'de barındırma yönünde gerekli tedbirleri alır.

(6) Üçüncü fıkradaki yükümlülüğü yerine getirmeyen sosyal ağ sağlayıcıya beş milyon Türk lirası, dördüncü fıkradaki yükümlülüğü yerine getirmeyen sosyal ağ sağlayıcıya ise on milyon Türk lirası idari para cezası Başkan tarafından verilir.

(7) Türkiye'den günlük erişimi bir milyondan fazla olan yurt dışı kaynaklı sosyal ağ sağlayıcılar hakkında 8 inci ve 8/A maddeleri kapsamında verilecek olan idari para cezaları bir milyon Türk lirası olarak, 8 inci ve 9 uncu maddeleri kapsamında verilecek olan adli para cezaları ise elli bin gün olarak verilir. Söz konusu idari para cezasını gerektiren ihlallerin bir yıl içinde her bir tekrarında cezalar bir kat artırılarak uygulanır.

(8) Hukuka aykırılığı hâkim veya mahkeme kararı ile tespit edilen içeriğin sosyal ağ sağlayıcıya bildirilmesi durumunda, bildirime rağmen yirmi dört saat içinde içeriği çıkarmayan veya erişimi engellemeyen sosyal ağ sağlayıcı, doğan zararların tazmin edilmesinden sorumludur. Bu hukuki sorumluluğun işletilmesi için içerik sağlayıcının sorumluluğuna gidilmesi veya içerik sağlayıcıya dava açılması şartı aranmaz.

(9) Bu maddenin uygulanmasında sosyal ağ sağlayıcının yükümlülükleri, içerik veya yer sağlayıcısı olmasından doğan sorumluluk ve yükümlülüklerini ortadan kaldırmaz.

(10) Bu maddenin uygulanmasına ilişkin usul ve esaslar Kurum tarafından belirlenir.

GEÇİCİ MADDE 1- (1) Başkanlığın kuruluştaki hizmet binasının yapımı, ceza ve ihalelerden yasaklama işleri hariç, Kamu İhale Kanunu ve Kamu İhale Sözleşmeleri Kanunu hükümlerine tâbi olmaksızın Kurum bütçesinden karşılanır.

(2) Halen faaliyet icra eden ticarî amaçla toplu kullanım sağlayıcılar, bu Kanunun yürürlüğe girdiği tarihten itibaren altı ay içinde 7 nci maddeye göre alınması gereken izin belgesini temin etmekle yükümlüdürler.

(3) Halen yer veya erişim sağlayıcı olarak faaliyet icra eden kişilere, Kurum tarafından, telekomünikasyon yoluyla iletişim konusunda yetkilendirme belgesi olup olmadığına bakılmaksızın, yer veya erişim sağlayıcı olarak faaliyet icra etmesi amacıyla bir yetkilendirme belgesi düzenlenir.

GEÇİCİ MADDE 2- (Ek: 5/11/2008-5809/67 md.)

(1) Telekomünikasyon İletişim Başkanlığı kadrolarında bulunan personelden ek 1 inci maddede belirtilen öğrenim şartlarını haiz olanlar; kamuda üç yıllık hizmet süresini tamamlamaları, KPDS'den en az 60 veya uluslararası geçerliliği olan sınavlardan muadili puan almaları ve hazırlayacakları tezin kabul edilmesi halinde bu Kanunun yayımı tarihinden itibaren beş yıl içerisinde iletişim uzmanı kadrosuna atanabilirler. Bu personelden; diğer kamu kurum ve kuruluşlarında özel mevzuatları uyarınca yarışma sınavına tabi tutularak mesleğe alınan ve yeterlik sınavını vererek veya tezi başarılı bulunarak kariyer meslek kadrolarına atanmış olanlar yabancı dil şartını karşıladıklarında; yüksek lisans veya doktora öğrenimini tamamlamış olanlardan, hazırladıkları yüksek lisans veya doktora tezlerinin konularının Kurumun veya Başkanlığın görev alanı ile ilgili olduğunun yapılacak inceleme sonucu belirlenenlerden doktora öğrenimini tamamlamış olanlar doğrudan, yüksek lisans öğrenimini tamamlamış olanlar yabancı dil şartını karşıladıklarında, iletişim uzmanı olarak atanabilirler.

(2) Telekomünikasyon İletişim Başkanlığı personelinden dört yıllık fakülte mezunu olanlar, kamuda üç yıllık hizmet süresini tamamlamaları, çıkarılacak yönetmelikte öngörülen şartları taşımaları ve buna ilave olarak hazırlayacakları tezin kabul edilmesi veya tezli yüksek lisans veya doktora yapmaları halinde, bu Kanunun yayımı tarihinden beş yıl içinde öğrenim alanına göre teknik uzman veya idarî uzman kadrosuna atanabilirler.

GEÇİCİ MADDE 3- (Ek: 6/2/2014-6518/100 md.)

(1) Birliğin kuruluşu bu Kanunun yayımı tarihinden itibaren üç ay içinde tamamlanır.

(2) Birlik, bu maddenin yürürlük tarihi itibarıyla abonesi bulunan mevcut internet servis sağlayıcıları ile erişim hizmeti veren işletmecilerin en az dörtte birinin katılımıyla imzalanan Birlik Tüzüğünün Kurum tarafından incelenerek uygun bulunmasını müteakip faaliyete başlar. Birliğin kurulmasını müteakip en geç bir ay içinde hâlen üye olmayan internet servis sağlayıcıları ve erişim hizmeti veren işletmeciler üyeliklerini tamamlamak zorundadır.(1)

(3) Belirtilen sürede Birliğin kuruluşunu tamamlayamaması hâlinde, Kurum tarafından internet servis sağlayıcılarına ve internet erişim hizmeti veren diğer işletmecilere bir önceki takvim yılındaki net satışlarının yüzde biri oranında idari para cezası uygulanır.

(4) Birliğin kurulmasını müteakip bir ay içinde üye olmayan internet servis sağlayıcılarına veya internet erişim hizmeti veren diğer işletmecilere, Kurum tarafından bir önceki takvim yılındaki net satışlarının yüzde biri oranında idari para cezası uygulanır.

GEÇİCİ MADDE 4- (Ek: 15/8/2016-KHK-671/23 md.; Aynen kabul: 9/11/2016-6757/20 md.)

(1) Telekomünikasyon İletişim Başkanının görevi bu maddenin yürürlüğe girdiği tarihte sona erer ve hakkında 375 sayılı Kanun Hükmünde Kararnamenin ek 18 inci maddesi hükümleri uygulanır. Telekomünikasyon İletişim Başkanlığında görevli daire başkanlarının görevleri bu maddenin yürürlüğe girdiği tarihte sona erer. Bunlardan daha önce İletişim Uzmanı unvanını ihraz etmiş olanlar Bilgi Teknolojileri ve İletişim Kurumunda Bilişim Uzmanı kadrolarına atanmış sayılırlar.

(2) Telekomünikasyon İletişim Başkanlığında görevli olup terör örgütlerine veya Milli Güvenlik Kurulunca Devletin milli güvenliğine karşı faaliyette bulunduğuna karar verilen yapı, oluşum veya gruplara üyeliği, mensubiyeti veya iltisakı yahut bunlarla irtibatı olmadığı değerlendirilen personelden İletişim Uzmanı ve İletişim Uzman Yardımcıları, Bilgi Teknolojileri ve İletişim Kurumunda bulunan Bilişim Uzmanı ve Bilişim Uzman Yardımcısı kadrolarına, diğer personel ise Bilgi Teknolojileri ve İletişim Kurumunda bulunan aynı unvanlı kadrolara başka bir işleme gerek kalmaksızın halen bulundukları kadro derecesiyle atanmış sayılırlar. Bunların atanmış sayıldıkları tarih itibarıyla diğer kanunlardaki hükümlere bakılmaksızın ve başka bir işleme gerek kalmaksızın kadroları ihdas edilmiş ve ilgili mevzuatı uyarınca Kurum kadro cetvellerine eklenmiş sayılır. Bu şekilde atananların Uzman ve Uzman Yardımcılığında geçirdiği süreler atanmış sayıldıkları Kurum kadrolarında geçmiş sayılır.

GEÇİCİ MADDE 5 – (Ek:29/7/2020-7253/7 md.)

(1) Sosyal ağ sağlayıcılar, ek 4 üncü maddenin;

a) Üçüncü fıkrası kapsamındaki yükümlülüklerini yerine getirmek üzere bu maddenin yürürlük tarihinden itibaren üç ay içinde gerekli çalışmaları tamamlar.

b) Dördüncü fıkrası kapsamındaki yükümlülükleri uyarınca hazırlayacakları ilk raporlarını, 2021 yılı Haziran ayında Kuruma bildirir ve internet sitesinde yayınlar.

Yürürlük

MADDE 13- (1) Bu Kanunun;

a) 3 üncü ve 8 inci maddeleri, yayımı tarihinden altı ay sonra,

b) Diğer maddeleri yayımı tarihinde,

yürürlüğe girer.

Yürütme

MADDE 14- (1) Bu Kanun hükümlerini Bakanlar Kurulu yürütür.

---

(1) 27/3/2015 tarihli ve 6639 sayılı Kanunun 30 uncu maddesiyle bu fıkrada yer alan "mevcut internet servis sağlayıcıları" ibaresi "bu maddenin yürürlük tarihi itibarıyla abonesi bulunan mevcut internet servis sağlayıcıları" şeklinde değiştirilmiştir.

ELEKTRONİK HABERLEŞME KANUNU

Kanun Numarası : **5809**
Kabul Tarihi : **5/11/2008**
Yayımlandığı Resmî Gazete : **Tarih: 10/11/2008 Sayı: 27050 (Mükerrer)**
Yayımlandığı Düstur : **Tertip: 5 Cilt : 48**

BİRİNCİ KISIM
Genel Hükümler

BİRİNCİ BÖLÜM
Amaç, Kapsam ve Tanımlar

Amaç

MADDE 1 – (1) Bu Kanunun amacı; elektronik haberleşme sektöründe düzenleme ve denetleme yoluyla etkin rekabetin tesisi, tüketici haklarının gözetilmesi, ülke genelinde hizmetlerin yaygınlaştırılması, kaynakların etkin ve verimli kullanılması, haberleşme alt yapı, şebeke ve hizmet alanında teknolojik gelişimin ve yeni yatırımların teşvik edilmesi ve bunlara ilişkin usul ve esasların belirlenmesidir.

Kapsam

MADDE 2 – (1) Elektronik haberleşme hizmetlerinin yürütülmesi ve elektronik haberleşme alt yapı ve şebekesinin tesisi ve işletilmesi ile her türlü elektronik haberleşme cihaz ve sistemlerinin imali, ithali, satışı, kurulması, işletilmesi, frekans dahil kıt kaynakların planlaması ve tahsisi ile bu konulara ilişkin düzenleme, yetkilendirme, denetleme ve uzlaştırma faaliyetlerinin yürütülmesi bu Kanuna tabidir.

(2) Millî güvenlik ve kamu düzeni ile olağanüstü hal, (...)[1] seferberlik, savaş hallerinde ve doğal afet durumlarında elektronik haberleşme hizmetlerinin sağlanmasına ilişkin özel kanunların ve 16/7/1965 tarihli ve 697 sayılı Ulaştırma ve Haberleşme Hizmetlerinin Olağanüstü Hallerde ve Savaşta Ne Suretle Yürütüleceğine Dair Kanun, 9/4/1987 tarihli ve 3348 sayılı Ulaştırma Bakanlığının Teşkilat ve Görevleri Hakkında Kanun, 16/6/2005 tarihli ve 5369 sayılı Evrensel Hizmetin Sağlanması ve Bazı Kanunlarda Değişiklik Yapılması Hakkında Kanun, 3/7/2005 tarihli ve 5397 sayılı Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun ile 4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun hükümleri saklıdır.[1]

---

(1) 2/7/2018 tarihli ve 703 sayılı Kanun Hükmünde Kararnamenin 205 inci maddesiyle bu fıkrada yer alan "sıkıyönetim," ibaresi madde metninden çıkarılmıştır.

(3) Türk Silahlı Kuvvetleri, Jandarma Genel Komutanlığı ile Sahil Güvenlik Komutanlığı ve kuruluş kanunları ile Cumhurbaşkanlığı kararnamelerinde belirtilen görev sahaları ile ilgili konularda olmak üzere Dışişleri Bakanlığı, Telekomünikasyon İletişim Başkanlığı, Millî İstihbarat Teşkilatı Müsteşarlığı ve Emniyet Genel Müdürlüğünün elektronik haberleşme cihaz, sistem ve şebekeleri ile bedeli bu kurumlar tarafından ödenerek işletmeciler tarafından kurulan veya kurulacak elektronik haberleşme cihaz, sistem ve şebekeleri hakkında 36 ncı ve 39 uncu maddeler hariç, bu Kanun hükümleri uygulanmaz.[1]

Tanımlar ve kısaltmalar

MADDE 3 – (1) Bu Kanunda geçen;

a) Abone: Bir işletmeci ile elektronik haberleşme hizmetinin sunumuna yönelik olarak yapılan bir sözleşmeye taraf olan gerçek ya da tüzel kişiyi,

b) Abonelik sözleşmesi: İşletmeci ile abone arasında akdedilen ve işletmecinin bir bedel karşılığında dönemsel ya da sürekli olarak bir hizmeti yerine getirmeyi veya mal teminini üstlendiği ya da her ikisini birden kapsayan sözleşmeyi,

c) Abone kimlik ve iletişim bilgileri: İşletmeci tarafından aboneye tahsis edilen özel bilgileri,

ç) Adres taşınabilirliği: Abonenin numarasını değiştirmeden bulunduğu adresi değiştirmesini,

d) Ana elektronik haberleşme şebekesi: Kamu kullanımına açık elektronik haberleşme hizmetlerinin üzerinden yürütüldüğü, belirli noktalar arasında elektronik haberleşme sağlayan transmisyon alt yapısı ve anahtarlama ekipmanları da dahil olmak üzere erişim ve iletim sistemleri şebekesini,

e) Arabağlantı: Bir işletmecinin kullanıcılarının aynı veya diğer bir işletmecinin kullanıcılarıyla irtibatının veya başka bir işletmeci tarafından sunulan hizmetlere erişiminin sağlanmasını teminen, aynı veya farklı bir işletmeci tarafından kullanılan elektronik haberleşme şebekelerinin birbirlerine fiziksel ve mantıksal olarak bağlantısını,

f) Arabağlantı yükümlüsü: Arabağlantı sağlama yükümlülüğü getirilen işletmeciyi,

g) Bakanlık: Ulaştırma Bakanlığını,

ğ) Dağıtıcı: Cihazın satış ve/veya tedarik zincirinde yer alan ve faaliyetleri cihazın özelliklerini etkilemeyen gerçek veya tüzel kişiyi,

h) Elektronik haberleşme: Elektriksel işaretlere dönüştürülebilen her türlü işaret, sembol, ses, görüntü ve verinin kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektrokimyasal, elektromekanik ve diğer iletim sistemleri vasıtasıyla iletilmesini, gönderilmesini ve alınmasını,

ı) Elektronik haberleşme alt yapısı: Elektronik haberleşmenin, üzerinden veya aracılığıyla gerçekleştirildiği anahtarlama ekipmanları, donanım ve yazılımlar, terminaller ve hatlar da dahil olmak üzere her türlü şebeke birimlerini, ilgili tesisleri ve bunların bütünleyici parçalarını,

i) Elektronik haberleşme alt yapısı işletimi: İlgili alt yapıya ilişkin gerekli elektronik haberleşme tesislerinin kurulması, kurdurulması, kiralanması veya herhangi bir surette temin edilmesiyle bu tesisin diğer işletmecilerin veya talep eden gerçek veya tüzel kişilerin kullanımına sunulmasını,

j) Elektronik haberleşme hizmeti: Elektronik haberleşme tanımına giren faaliyetlerin bir kısmının veya tamamının hizmet olarak sunulmasını,

---

(1) 2/7/2018 tarihli ve 703 sayılı Kanun Hükmünde Kararnamenin 205 inci maddesiyle bu fıkrada yer alan "kuruluş kanunlarında" ibaresi "kuruluş kanunları ile Cumhurbaşkanlığı kararnamelerinde" şeklinde değiştirilmiştir.

k) Elektronik haberleşme şebekesi: Bir veya daha fazla nokta arasında elektronik haberleşmeyi sağlamak için bu noktalar arası bağlantıyı teşkil eden anahtarlama ekipmanları ve hatlar da dahil olmak üzere her türlü iletim sistemleri ağını,

l) Elektronik haberleşme sektörü: Elektronik haberleşme hizmeti verilmesi, elektronik haberleşme şebekesi sağlanması, elektronik haberleşme cihaz ve sistemlerine yönelik üretim, ithal, satış ve bakım-onarım hizmetlerinin yürütülmesi ile ilgili sektörü,

m) Elektronik haberleşme şebekesi sağlanması: Elektronik haberleşme şebekesi kurulması, işletilmesi, kullanıma sunulması ve kontrolünü,

n) Elektronik kimlik bilgisi: Elektronik haberleşme cihazlarına tek ve benzersiz olarak tahsis edilmiş kimlik tanımını,

o) Elektromanyetik girişim (Enterferans): İlgili mevzuat hükümlerine uygun olarak yapılan her türlü elektronik haberleşmeyi engelleyen, kesinti doğuran veya kalitesini bozan her türlü yayın veya elektromanyetik etkiyi,

ö) Erişim: Bu Kanunda belirtilen koşullarla, elektronik haberleşme şebekesi, alt yapısı ve/veya hizmetlerinin, diğer işletmecilere sunulmasını,

p) Erişim yükümlüsü: Erişim sağlama yükümlülüğü getirilen işletmeciyi,

r) Etkin piyasa gücü: İşletmecinin, ilgili elektronik haberleşme pazarında, tek başına ya da diğer işletmecilerle birlikte, rakiplerinden, kullanıcılarından ve tüketicilerinden fark edilir bir şekilde bağımsız olarak hareket edebilmesine imkan sağlayan ekonomik gücü,

s) Geçiş hakkı: İşletmecilere, elektronik haberleşme hizmeti sunmak için gerekli şebeke ve alt yapıyı kurmak, kaldırmak, bakım ve onarım yapmak gibi amaçlar ile kamu ve özel mülkiyet alanlarının altından, üstünden, üzerinden geçmeleri için tanınan hakları,

ş) Geçiş hakkı sağlayıcısı: Geçiş hakkına konu olan kamuya ait ya da kamunun ortak kullanımında olan taşınmazlar da dahil olmak üzere, taşınmaz sahipleri ve/veya taşınmaz üzerindeki hak sahiplerini,

t) Hizmet taşınabilirliği: Abonenin numarasını değiştirmeden aldığı hizmet türünü değiştirmesini,

u) İlgili pazar: Ülkenin tümünde veya bir bölümünde sunulmakta olan belirli bir elektronik haberleşme hizmeti ve onunla yüksek derecede ikame edilebilen diğer elektronik haberleşme hizmetlerinden oluşan pazarı,

ü) İlgili tesisler: İlgili şebeke ve/veya hizmet aracılığıyla hizmetlerin sunulmasını sağlayan ve/veya destekleyen bir elektronik haberleşme şebekesine ve/veya bir elektronik haberleşme hizmetine ilişkin tesisleri,

v) İnternet alan adı: İnternet üzerinde bulunan bilgisayar veya internet sitelerinin adresini belirlemek için kullanılan internet protokol numarasını tanımlayan adları,

y) İnternet alan adı sistemi: Okunması ve akılda tutulması kolay olan ve genelde aranan adres sahipleri ile ilişkilendirilebilen simgesel isimlerle yapılan adreslemede, karşılığı olan internet protokolü numarasını bulan ve kullanıcıya veren sistemi,

z) İşletmeci: Yetkilendirme çerçevesinde elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme şebekesi sağlayan ve alt yapısını işleten şirketi,

aa) İşletmeci numara taşınabilirliği: Abonenin numarasını değiştirmeden hizmet aldığı işletmeciyi değiştirmesini,

bb) Koşullu erişim sistemi: Radyo ve televizyon yayın sistemlerine abonelik veya başka bir yöntemle önceden izin verilmesi yoluyla koşullu olarak erişimi sağlayan her türlü teknik tedbir ve düzenlemeyi,

cc) Kullanıcı: Aboneliği olup olmamasına bakılmaksızın elektronik haberleşme hizmetlerinden yararlanan gerçek veya tüzel kişiyi,

çç) Kullanım hakkı: Frekans, numara, uydu pozisyonu gibi kıt kaynakların kullanılması için verilen hakkı,

dd) Kurul: Bilgi Teknolojileri ve İletişim Kurulunu,

ee) Kurum: Bilgi Teknolojileri ve İletişim Kurumunu,

ff) MCKS (CEIR): Merkezî mobil cihaz kimlik tanımı veri tabanı sistemini,

gg) MCKT (EIR): Mobil cihaz kimlik tanımı veri tabanını,

ğğ) Numara: Şebeke ve/veya şebeke sonlanma noktasını tanımlayan, söz konusu noktaya ses, veri ve görüntünün yönlendirilmesini sağlayan, kullanıldığı yere göre abone, işletmeci, elektronik haberleşme şebekesi ve/veya hizmeti ile ilişkilendirilebilen bilgiyi içeren harf, rakamlar dizini veya sembolleri,

hh) Numara taşınabilirliği: Abonelerin numarasını değiştirmeden, hizmet aldığı işletmeciyi veya adresini veya aldığı hizmetin türünü değiştirebilmesini,

ıı) Onaylanmış kuruluş: Uygunluk değerlendirme faaliyetinde bulunmak üzere, Kurum tarafından belirlenerek, 29/6/2001 tarihli ve 4703 sayılı Ürünlere İlişkin Teknik Mevzuatın Hazırlanması ve Uygulanmasına Dair Kanun ve ilgili teknik düzenlemelerde belirtilen esaslar çerçevesinde yetkilendirilen kamu kurum ve kuruluşları ile gerçek veya tüzel kişileri,

ii) Radyo ve televizyon yayını: Karasal, kablo, uydu ve diğer ortamlar üzerinden, şifreli veya şifresiz olarak kitle haberleşmesi amacıyla yapılan ve bireysel iletişim hizmetlerini kapsamayan görüntü ve/veya ses iletimini,

jj) Son kullanıcı: Elektronik haberleşme hizmeti ve/veya elektronik haberleşme şebekesi sağlamayan gerçek veya tüzel kişileri,

kk) Spektrum: Elektronik haberleşme amacıyla kullanılan, frekansı 9 kHz-3000 GHz arasında olan ve uluslararası düzenleme yapılması halinde 3000 GHz'in üzerindeki frekanslar da dahil olmak üzere elektromanyetik dalgaların frekans aralığını,

ll) Standart: Üzerinde mutabakat sağlanmış olan, kabul edilmiş bir kuruluş tarafından onaylanan, mevcut şartlar altında en uygun seviyede bir düzen kurulmasını amaçlayan, ortak ve tekrar eden kullanımlar için ürünün özellikleri, işleme ve üretim yöntemleri, bunlarla ilgili terminoloji, sembol, ambalajlama, işaretleme, etiketleme ve uygunluk değerlendirmesi işlemleri hususlarından biri veya birkaçını belirten ve bu kapsamda uyulması ihtiyari olan düzenlemeyi,

mm) Şebeke sonlanma noktası: Elektronik haberleşme şebekesinde aboneye erişimin sağlandığı fiziksel noktayı, anahtarlama veya yönlendirme ihtiva eden şebekelerde ise abone numarası veya ismi ile ilişkilendirilebilen özel bir şebeke adresiyle tanımlanan noktayı,

nn) Tarife: İşletmecilerin, elektronik haberleşme hizmetinin sunulması karşılığında kullanıcılardan farklı adlar altında alabilecekleri ücretleri içeren cetveli,

oo) Taşıyıcı: Bir çağrının başlatılması, sonlandırılması veya taşınması hizmetlerinin tümünü veya bir kısmını sunan işletmeciyi,

öö) Taşıyıcı ön seçimi: Taşıyıcının, taşıyıcı seçim kodu çevrilmeksizin seçilmesine imkan sağlayacak şekilde önceden seçilmesi yöntemini,

pp) Taşıyıcı seçimi: Taşıyıcının, taşıyıcı seçim kodu çevrilmesi suretiyle seçilmesi yöntemini,

rr) Taşıyıcı seçim kodu: Taşıyıcılara, taşıyıcı seçimi amacıyla Kurumca tahsis edilen kodu,

ss) Telsiz: Aralarında herhangi bir fiziki bağlantı olmaksızın elektromanyetik dalgalar yoluyla açık, kodlu veya kriptolu ses ve veri vermeye, almaya veya yalnızca vermeye veya almaya yarayan sistemleri,

şş) Telsiz kurma ve kullanma izni: Bu Kanun kapsamında kurulacak ve kullanılacak telsiz cihaz ve sistemleri için Kurum tarafından verilen izni,

tt) Telsiz ruhsatnamesi: Bu Kanun kapsamında kurulacak ve kullanılacak telsiz cihaz ve sistemleri için Kurum tarafından verilen ruhsatnameyi,

uu) Tüketici: Elektronik haberleşme hizmetini ticari veya mesleki olmayan amaçlarla kullanan veya talep eden gerçek veya tüzel kişiyi,

üü) Ulusal dolaşım: Bir işletmeciye ait hizmetlerin, teknik uyumluluk şartları saklı kalmak üzere, diğer bir işletmecinin abonelerine ait ekipmanlar üzerinden sunulmasına veya bir diğer sistemin arabağlantısına imkân sağlayan sistemlerarası dolaşımı,

vv) Ulusal numaralandırma planı: Numaraların yapısını tanımlayan, yönlendirme, adresleme, ücretlendirme veya hizmet türüne ilişkin bilgi vermek üzere bölümlere ayrılarak tanımlanabilen numaralandırma planını,

yy) Uyumlaştırılmış Avrupa standardı: Avrupa Topluluğu Resmi Gazetesinde ismi yayımlanan standardı,

zz) Uyumlaştırılmış ulusal standart: Uyumlaştırılmış Avrupa standartlarına uygun olarak Türk Standartları Enstitüsü tarafından uyumlaştırılarak kabul edilen ve Kurum tarafından listeleri tebliğler ile yayımlanan Türk standartlarını,

aaa) Üretici: Elektronik haberleşme cihazı imal eden, ıslah eden veya cihaza adını, ticarî markasını veya ayırt edici işaretini koymak suretiyle kendini üretici olarak tanıtan gerçek veya tüzel kişiyi, üreticinin Ülke dışında olması halinde, üretici tarafından yetkilendirilen temsilciyi ve/veya ithalatçıyı, ayrıca, cihazın satış ve/veya tedarik zincirinde yer alan ve faaliyetleri cihazın güvenliğine ilişkin özelliklerini etkileyen gerçek veya tüzel kişiyi,

bbb) Yerel ağ: Sabit elektronik haberleşme şebekesinde abone tarafındaki şebeke sonlanma noktasını, abonenin bağlı bulunduğu ana dağıtım çatısına veya eşdeğer tesise bağlayan fiziksel devreyi,

ccc) Yetkilendirme: Elektronik haberleşme hizmetlerinin sunulması ve/veya elektronik haberleşme şebekesi sağlanmasını teminen şirketlerin, Kurum nezdinde kayıtlanmasını veya kayıtlanmasıyla birlikte bu şirketlere elektronik haberleşme hizmetlerine özel, belirli hak ve yükümlülükler verilmesini,

ifade eder.

ilkeler

MADDE 4 – (1) Her türlü elektronik haberleşme cihaz, sistem ve şebekelerinin kurulması ve işletilmesine müsaade edilmesi, gerekli frekans, numara, uydu pozisyonu ve benzeri kaynak tahsislerinin yapılması ile bunların düzenlenmesi Devletin yetki ve sorumluluğu altındadır. İlgili merciler tarafından elektronik haberleşme hizmetinin sunulmasında ve bu hususta yapılacak düzenlemelerde aşağıdaki ilkeler göz önüne alınır:

a) Serbest ve etkin rekabet ortamının sağlanması ve korunması.

b) Tüketici hak ve menfaatlerinin gözetilmesi.

c) Kalkınma planları ve üst politika metinleri ile Bakanlık tarafından belirlenen stratejilerin gözetilmesi.[2]

ç) Herkesin, makul bir ücret karşılığında elektronik haberleşme şebeke ve hizmetlerinden yararlanmasını sağlayacak uygulamaların teşvik edilmesi.

d) Aksini gerektiren objektif nedenler bulunmadıkça veya toplumdaki ihtiyaç sahibi kesimlere özel, kapsamı açık ve sınırları belirlenmiş kolaylıklar sağlanması halleri dışında, eşit şartlardaki aboneler, kullanıcılar ve işletmeciler arasında ayrım gözetilmemesi ve hizmetlerin benzer konumdaki kişiler tarafından eşit şartlarla ulaşılabilir olması.

e) Bu Kanunda aksi belirtilmedikçe ya da objektif nedenler aksini gerektirmedikçe, niteliksel ve niceliksel devamlılık, düzenlilik, güvenilirlik, verimlilik, açıklık, şeffaflık ve kaynakların verimli kullanılmasının gözetilmesi.

f) Elektronik haberleşme sistemlerinin uluslararası normlara uygun olması.

g) Teknolojik yeniliklerin uygulanması ile araştırma-geliştirme faaliyet ve yatırımlarının teşvik edilmesi.

ğ) Hizmet kalitesi artırımının teşvik edilmesi.

h) Millî güvenlik ile kamu düzeni gereklerine ve acil durum ihtiyaçlarına öncelik verilmesi.

ı) Bu Kanunda, ilgili mevzuatta ve yetkilendirmelerde açıkça belirlenen durumlar haricinde, işletmecilerin, arabağlantı da dahil olmak üzere erişim ücretleri ile hat ve devre kiralarını da kapsayacak biçimde, elektronik haberleşme hizmeti sunulması karşılığı alacakları ücretleri serbestçe belirlemesi.

i) Elektronik haberleşme cihaz ve sistemlerinin kurulması, kullanılması ve işletilmesinde insan sağlığı, can ve mal güvenliği, çevre ve tüketicinin korunması açısından asgarî uluslararası normların dikkate alınması.

j) Elektronik haberleşme hizmetlerinin sunulmasında ve bu hususlarda yapılacak düzenlemelerde tarafsızlığın sağlanması.

k) Teknolojik yeniliklerin kullanılması da dahil olmak üzere engelli, yaşlı ve sosyal açıdan korunmaya muhtaç diğer kesimlerin özel ihtiyaçlarının dikkate alınması. [1]

l) Bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi.

---

(1) 25/4/2013 tarihli ve 6462 sayılı Kanunun 1 inci maddesiyle, bu bentte yer alan "özürlü" ibaresi "engelli" şeklinde değiştirilmiştir.

(2) 2/7/2018 tarihli ve 703 sayılı Kanun Hükmünde Kararnamenin 205 inci maddesiyle bu bentte yer alan "Hükümet programlarındaki hedefler ile Bakanlık tarafından belirlenen strateji ve politikaların gözetilmesi" ibaresi "üst politika metinleri ile Bakanlık tarafından belirlenen stratejilerin gözetilmesi" şeklinde değiştirilmiştir.

İKİNCİ BÖLÜM
Elektronik Haberleşme Sektöründe Yetkili Merciler ve Görevleri

Bakanlığın görev ve yetkileri

MADDE 5 – (1) Bakanlığın elektronik haberleşme sektörüne ilişkin yetki ve görevleri şunlardır:

a) Numaralandırma, internet alan adları, uydu pozisyonu, frekans tahsisi gibi kıt kaynaklara dayalı elektronik haberleşme hizmetlerine ilişkin strateji ve politikaları belirlemek.

b) Elektronik haberleşme sektörünün; serbest rekabet ortamında gelişimini teşvik etmeye ve bilgi toplumuna dönüşümün desteklenmesini sağlamaya yönelik hedef, ilke ve politikaları belirlemek ve bu amaçla teşvik edici tedbirleri almak.

c) Elektronik haberleşme alt yapı, şebeke ve hizmetlerinin; teknik, ekonomik ve sosyal ihtiyaçlara, kamu yararına ve millî güvenlik amaçlarına uygun olarak kurulması, geliştirilmesi ve birbirlerini tamamlayıcı şekilde yürütülmesini sağlamaya yönelik politikaları belirlemek.

ç) Elektronik haberleşme cihazları sanayisinin gelişmesine ilişkin politikaların oluşumuna ve elektronik haberleşme cihazları bakımından yerli üretimi özendirici tedbirleri almaya yönelik politikaları belirlemeye katkıda bulunmak.

d) Ülkemizin üyesi bulunduğu elektronik haberleşme sektörü ile ilgili uluslararası birlik ve kuruluşlar nezdinde 5/5/1969 tarihli ve 1173 sayılı Milletlerarası Münasebetlerin Yürütülmesi ve Koordinasyonu Hakkında Kanun hükümleri saklı kalmak üzere Devleti temsil etmek veya temsile yetkilendirmek, çalışmalara katılım ve kararların uygulanması konusunda koordinasyonu sağlamak.

e) Elektronik haberleşme politikalarının tespiti ve uygulanması amacıyla gerekli araştırmaları yapmak ve yaptırmak.

f) Elektronik haberleşmenin doğal afetler ve olağanüstü haller nedeniyle aksamamasını teminen gerekli tedbirleri almak ve koordinasyonu sağlamak. Haberleşmenin aksaması riskine karşı önceden haberleşmenin kesintisiz bir biçimde sağlanmasına yönelik alternatif haberleşme alt yapısını kurmak, kurdurmak ve ihtiyaç durumunda söz konusu sistemi devreye sokmak.

g) Olağanüstü hal ve savaşta elektronik haberleşme hizmetlerini, 16/7/1965 tarihli ve 697 sayılı Kanun hükümleri dahilinde planlamak, gerekli işleri yapmak ve yaptırmak.

ğ) Elektronik haberleşme sistemlerinin yerli tasarım ve üretimini, bu amaçla sektöre ilişkin araştırma, geliştirme ve eğitim faaliyetlerini teknik ve maddi destek de dahil olmak üzere teşvik etmek ve Kurumun gelirlerinin % 20'sini aşmamak kaydıyla söz konusu faaliyetlere ilişkin olarak ayıracağı kaynağı belirlemek ve bu kaynağın kullanımına ilişkin gereken düzenlemeleri yaparak bu kaynağı kullandırmak.

h) **(Ek: 6/2/2014-6518/102 md.)** Ulusal siber güvenliğin sağlanması amacıyla politika, strateji ve hedefleri belirlemek, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilere yönelik siber güvenliğin sağlanmasına ilişkin usul ve esasları belirlemek, eylem planlarını hazırlamak, (…)[1] ilgili faaliyetlerin koordinasyonunu sağlamak, kritik altyapılar ile ait oldukları kurumları ve konumları belirlemek, gerekli müdahale merkezlerini kurmak, kurdurmak ve denetlemek, her türlü siber müdahale aracının ve millî çözümlerin üretilmesi ve geliştirilmesi amacı ile çalışmalar yapmak, yaptırmak ve bunları teşvik etmek ve siber güvenlik konusunda bilinçlendirme, eğitim ve farkındalığıartırma çalışmaları yürütmek, siber güvenlik alanında faaliyet gösteren gerçek ve tüzel kişilerin uyması gereken usul ve esasları hazırlamak.[1]

ı) **(Ek: 27/3/2015-6639/31 md.)** Ulusal kamu entegre veri merkezlerine yönelik politika, strateji ve hedefleri belirlemek, eylem planlarını hazırlamak, eylem planlarını izlemek, e-Devlet hizmetlerinde kullanılan verilerin ve sistemlerin barındırıldığı veri merkezlerini kamu entegre veri merkezlerinde toplamak amacıyla verilerin transferi de dahil gerekli altyapıları kurmak, kurdurmak, işletmek, işlettirmek ve tüm bu faaliyetlere yönelik uygulama usul ve esaslarını belirlemek, kurulum, uygulama ve işletim süreçlerini planlamak, yürütmek ve koordine etmek.

_____

(1) 2/7/2018 tarihli ve 703 sayılı Kanun Hükmünde Kararnamenin 205 inci maddesiyle bu bentte yer alan "Siber Güvenlik Kurulunun sekretaryasını yapmak," ibaresi madde metninden çıkarılmıştır.

Kurumun görev ve yetkileri [1]

MADDE 6 – (1) Kurumun görev ve yetkileri şunlardır:

a) Elektronik haberleşme sektöründe; rekabeti tesis etmeye ve korumaya, rekabeti engelleyici, bozucu veya kısıtlayıcı uygulamaların giderilmesine yönelik düzenlemeleri yapmak, bu amaçla ilgili pazarlarda etkin piyasa gücüne sahip işletmecilere ve gerekli hallerde diğer işletmecilere yükümlülükler getirmek ve mevzuatın öngördüğü tedbirleri almak.

b) Bu Kanun ve bu Kanuna dayanılarak yapılan düzenlemelere aykırı olarak, elektronik haberleşme sektöründe ortaya çıkan rekabet ihlallerini denetlemek, yaptırım uygulamak, mevzuatın öngördüğü hallerde elektronik haberleşme sektöründe rekabet ihlallerine ilişkin konularda Rekabet Kurumundan görüş almak.

c) Abone, kullanıcı, tüketici ve son kullanıcıların hakları ile kişisel bilgilerin işlenmesi ve gizliliğinin korunmasına ilişkin gerekli düzenlemeleri ve denetlemeleri yapmak.

ç) İşletmeciler ile tüketicileri ilgilendiren Kurul kararlarını gerekçe ve süreçleri ile kamuoyuna açık tutmak.

d) Bu Kanun çerçevesinde gerektiğinde işletmeciler arasında uzlaştırma prosedürünü işletmek, uzlaşma sağlanamadığı takdirde ilgili taraflar arasında aksi kararlaştırılıncaya kadar geçerli olmak üzere gerekli tedbirleri almak.

e) Elektronik haberleşme sektöründeki gelişmeleri takip etmek, sektörün gelişimini teşvik etmek amacıyla gerekli araştırmaları yapmak veya yaptırmak ve bu konularda ilgili kurum ve kuruluşlarla işbirliği halinde çalışmak.

f) Bu Kanunun 5 inci maddesinin (a) bendini de göz önünde bulundurarak, elektronik haberleşme hizmetlerinin sunulması ve elektronik haberleşme şebeke ve altyapılarının tesis ve işletilmesi için gerekli olan frekans, uydu pozisyonu ve numaralandırma planlamasını ve tahsisini yapmak.

g) Elektronik haberleşme ile ilgili olarak Bakanlığın strateji ve politikalarını dikkate alarak, yetkilendirme, tarifeler, erişim, geçiş hakkı, numaralandırma, spektrum yönetimi, telsiz cihaz ve sistemlerine kurma ve kullanma izni verilmesi, spektrumun izlenmesi ve denetimi, piyasa gözetimi ve denetimi de dahil gerekli düzenlemeler ile denetlemeleri yapmak.

ğ) Telsiz sistemlerinin belirlenen tekniklere ve usullere uygun olarak kurulmasının ve çalıştırılmasının kontrolünü yapmak, elektromanyetik girişimleri tespit etmek ve giderilmesini sağlamak.

h) İşletmecilerin ticari sırları ile kamuoyuna açıklanabilecek bilgilerinin kapsamını belirlemek, işletmecilerin ticari sırları ile yatırım ve iş planlarının gizliliğini korumak ve bunları adli makamların talepleri dışında muhafaza etmek.

ı) Elektronik haberleşmeyle ilgili olarak, işletmeciler, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerden ihtiyaç duyacağı her türlü bilgi ve belgeyi almak ve gerekli kayıtları tutmak, Bakanlık tarafından elektronik haberleşme sektörüne yönelik strateji ve politikaların belirlenmesinde ihtiyaç duyulanları, talebi üzerine Bakanlığa iletmek.

i) Bu Kanunun 5 inci maddesinin birinci fıkrasının (ğ) bendi uyarınca Bakanlıkça yapılacak düzenlemeler çerçevesinde, elektronik haberleşme sektörüne ilişkin araştırma, geliştirme ve eğitim faaliyetlerine ilişkin olarak, mevcut Kurum gelirlerini göz önünde bulundurarak gelirlerinin % 20'sini aşmamak kaydıyla ayıracağı kaynağı Bakanlığa aktarmak. Bu aktarım, katma değer vergisi ve damga vergisi dahil her türlü vergi, resim, harç ve benzeri mali yükümlülüklerden istisnadır.

j) Kullanıcılara ve erişim kapsamında diğer işletmecilere uygulanacak tarifelere, sözleşme hükümlerine, teknik hususlara ve görev alanına giren diğer konulara ilişkin genel kriterler ile

uygulama usul ve esaslarını belirlemek, tarifeleri onaylamak, tarifelerin denetlenmesine ilişkin düzenlemeleri yapmak.

(1) 6/2/2014 tarihli ve 6518 sayılı Kanunun 103 üncü maddesiyle bu maddenin birinci fıkrasına (ü) bendinden sonra gelmek üzere (v) bendi eklenmiş ve diğer bent buna göre teselsül ettirilmiştir.

k) İşletmeciler tarafından hazırlanan referans erişim tekliflerini onaylamak.

l) Yürütülecek elektronik haberleşme hizmetleri, şebeke ve/veya alt yapısı ile ilgili olarak yapılacak yetkilendirmelere ilişkin hüküm ve şartları belirlemek, uygulanmasını ve yetkilendirmeye uygunluğu denetlemek, bu hususta gereken iş ve işlemleri yürütmek ve mevzuatın öngördüğü tedbirleri almak.

m) Radyo ve televizyon yayıncılığına ilişkin ilgili kanununda belirtilen hükümler saklı kalmak kaydıyla, frekans planlama, tahsis ve tescil işlemlerini, güç ve yayın sürelerini de göz önünde tutarak uluslararası kuruluşlarla işbirliği de yapmak suretiyle yürütmek.

n) Elektronik haberleşme sektöründe kullanılacak her çeşit sistem ve cihazların, uyumlaştırılmış ulusal standartlarını yayımlatmak ve uygulanmasını sağlamak, teknik düzenlemelerini yapmak, piyasa denetimini yapmak ve/veya yaptırmak, bu amaçla laboratuvarlar kurup işletebilmek ve bu laboratuvarlarda verebileceği eğitim ve danışmanlık hizmetleri karşılığında alınacak ücretleri belirlemek.

o) Elektronik haberleşme sektöründe tesis, ölçüm ve bakım-onarım yapacak kuruluşların yetkilendirmesini bu konuda görevli kuruluşlarla koordine etmek.

ö) Elektronik haberleşme sektörüne yönelik pazar analizleri yapmak, ilgili pazarı ve ilgili pazarda etkin piyasa gücüne sahip işletmeci veya işletmecileri belirlemek.

p) Elektronik haberleşme sektörü ile ilgili uluslararası birlik ve kuruluşların çalışmalarına katılmak, kararların uygulanmasını takip etmek ve gerekli koordinasyonu sağlamak.

r) Bu Kanunun 46 ncı maddesinde belirtilen ücretlerle ilgili olarak terkin de dahil olmak üzere her türlü usul ve esasları belirlemek, Kurumun yıllık bütçesini, gelir-gider kesin hesabını, yıllık çalışma programını onamak, gerekirse bütçede hesaplar arasında aktarma yapmak veya gelir fazlasını mevzuat çerçevesinde genel bütçeye devretmek.

s) Elektronik haberleşme sektöründe faaliyet gösterenlerin mevzuata uymasını denetlemek ve/veya denetlettirmek, konu ile ilgili usul ve esasları belirlemek, aykırılık halinde mevzuatın öngördüğü işlemleri yapmak ve yaptırımları uygulamak.

ş) Elektronik haberleşme sektörüne yönelik olarak, millî güvenlik, kamu düzeni veya kamu hizmetinin gereği gibi yürütülmesi amacıyla mevzuatın öngördüğü tedbirleri almak.

t) Ara bağlantı ve ulusal dolaşım da dahil erişim ile ilgili uygulanacak usul ve esasları belirlemek ve mevzuatın öngördüğü düzenlemeleri yapmak, elektronik haberleşme sağlanması amacıyla imzalanan anlaşmaların rekabeti kısıtlayan, mevzuata ve/veya tüketici menfaatlerine aykırı hükümler içermemesi amacıyla mevzuatın öngördüğü tedbirleri almak.

u) İlgili kanun hükümleri dahilinde, evrensel hizmetlere ilişkin hizmet kalitesi ve standartları da dahil olmak üzere, gerektiğinde her türlü elektronik haberleşme hizmetine yönelik hizmet kalitesi ve standartlarını belirlemek, denetlemek, denetlettirmek ve buna ilişkin usul ve esasları belirlemek.

ü) Elektronik haberleşme sektöründe, bağımsız denetim faaliyetine ilişkin esasları, bağımsız denetleme faaliyetlerinde bulunacak kuruluşların kuruluş şartlarını, çalışma esaslarını ve çalıştıracağı personelin niteliklerini belirlemek.

v) **(Ek: 6/2/2014-6518/103 md.)** Siber güvenlik ve internet alan adları konularında Cumhurbaşkanı, Bakanlık ve/veya Siber Güvenlik Kurulu tarafından verilen görevleri Telekomünikasyon İletişim Başkanlığı veya diğer birimleri marifetiyle yerine getirmek.[1][2]

y) Bu Kanunla verilen görevlere ilişkin yönetmelik, tebliğ ve diğer ikincil düzenlemeleri çıkarmak.[1]

(1) 6/2/2014 tarihli ve 6518 sayılı Kanunun 103 üncü maddesiyle bu Kanunun 6 ncı maddesinin birinci fıkrasına (ü) bendinden sonra gelmek üzere (v) bendi eklenmiş ve diğer bent buna göre teselsül ettirilmiştir.

(2) 2/7/2018 tarihli ve 703 sayılı Kanun Hükmünde Kararnamenin 205 inci maddesiyle bu bentte yer alan "Bakanlar Kurulu" ibaresi "Cumhurbaşkanı" şeklinde değiştirilmiştir.

Rekabetin sağlanması

MADDE 7 – (1) Kurum, 7/12/1994 tarihli ve 4054 sayılı Rekabetin Korunması Hakkında Kanun hükümleri saklı kalmak kaydıyla, elektronik haberleşme sektöründe rekabete aykırı davranış ve uygulamaları re'sen veya şikâyet üzerine incelemeye, soruşturmaya ve rekabetin tesisine yönelik gerekli gördüğü tedbirleri almaya, görev alanına giren konularda bilgi ve belgelerin sağlanmasını talep etmeye yetkilidir.

(2) Rekabet Kurulu, elektronik haberleşme sektörüne ilişkin olarak yapacağı inceleme ve tetkiklerde, birleşme ve devralmalara ilişkin olarak vereceği kararlar da dahil olmak üzere elektronik haberleşme sektörüne ilişkin olarak vereceği tüm kararlarda, öncelikle Kurumun görüşünü ve Kurumun yapmış olduğu düzenleyici işlemleri dikkate alır.

(3) Kurum, yapacağı pazar analizleri sonucu ilgili pazarlarda etkin piyasa gücüne sahip işletmecileri belirleyebilir. Kurum, etkin rekabet ortamının sağlanması ve korunması amacıyla etkin piyasa gücüne sahip işletmecilere yükümlülükler getirebilir. Aynı ve/veya farklı pazarlarda etkin piyasa gücüne sahip olan işletmeciler arasında söz konusu yükümlülükler açısından farklılaştırma yapılabilir.

İKİNCİ KISIM
Genel Düzenlemeler

BİRİNCİ BÖLÜM
Yetkilendirme

Elektronik haberleşme hizmetlerinin yetkilendirilmesi

MADDE 8 – (1) Bakanlığın strateji ve politikaları da dikkate alınarak Kurumca yapılacak yetkilendirmeyi müteakip, elektronik haberleşme hizmeti verilebilir ve/veya elektronik haberleşme şebekesi veya alt yapısı kurulup işletilebilir.

(2) İhtiyaç duyulan elektronik haberleşme hizmeti ve/veya şebekesi veya altyapısının öncelikle Kurumca yetkilendirilmiş işletmecilerden karşılanması esastır. Ancak;

a) Bir gerçek veya tüzel kişinin, kendi kullanımındaki taşınmazların dâhilinde ve her bir taşınmazın sınırları dışına taşmayan, münhasıran şahsi veya kurumsal ihtiyaçları için kullanılan ve üçüncü şahıslara herhangi bir elektronik haberleşme hizmeti verilmesinde kullanılmayan, sağlanmasında herhangi bir ticari amaç güdülmeyen ve kamu kullanımına açık olarak sunulmayan,

b) Kamu kurum ve kuruluşlarının münhasıran verdikleri hizmetler ile ilgili olarak özel kanunları uyarınca kurdukları,

elektronik haberleşme hizmeti ve/veya şebekesi veya altyapısı yetkilendirmeye tabi değildir.

(3) Kurum bu şebeke veya altyapıların bu maddedeki esaslara uygunluğunu ve kullanılan teçhizatın standartlara uygunluğunu denetlemeye ve uygun olmayanların kaldırılmasını sağlamaya ve bu maddenin uygulanmasına ilişkin usul ve esasları düzenlemeye yetkilidir.

(4) Radyo ve televizyon yayıncılığı ile ilgili Kanun hükümleri saklıdır.

Yetkilendirme usulü

MADDE 9 – (1) Yetkilendirme, bildirim veya kullanım hakkının verilmesi yoluyla yapılır.

(2) Elektronik haberleşme hizmeti sunmak ve/veya şebekesi veya alt yapısı kurup işletmek isteyen şirketler faaliyete başlamadan önce Kurum düzenlemeleri çerçevesinde Kuruma bildirimde bulunurlar.

(3) Kuruma bildirimde bulunan şirketler, sunmak istedikleri elektronik haberleşme hizmeti ve/veya işletmek istedikleri elektronik haberleşme şebekesi veya altyapısı için numara, frekans, uydu pozisyonu gibi kaynak tahsisine ihtiyaç duymuyorlar ise Kurumun belirlediği usul ve esaslara uygun bildirimle birlikte; kaynak tahsisine ihtiyaç duyuyorlar ise Kurumdan kullanım hakkı alınması kaydıyla yetkilendirilirler.

(4) Kurum, kullanım hakkı verilmesinin gerektiği elektronik haberleşme hizmetlerini ve bu hizmetlere ilişkin kullanım hakkı sayısının sınırlandırılmasının gerekip gerekmediğini tespit eder.

(5) Kullanım hakkı sayısının sınırlandırılmasının gerekmediği tespit edilen elektronik haberleşme hizmetleri için usulüne uygun başvuruyu müteakip 30 gün içerisinde Kurumca kullanım hakkı verilir.

(6) Kullanım hakkı sayısı, ancak kaynakların sınırlı sayıda işletmeci tarafından yürütülmesinin gerektiği durumlarda ve kaynakların etkin ve verimli kullanılmasını teminen sınırlandırılabilir. Kullanım hakkı sayısının sınırlandırılması halinde;

a) Uydu pozisyonu ile ulusal çapta verilecek frekans bandı kullanımını ihtiva eden ve sınırlı sayıda işletmeci tarafından yürütülmesi gereken elektronik haberleşme hizmetlerine ilişkin yetkilendirme politikası, hizmetin başlama zamanı, yetkilendirme süresi ve hizmeti sunacak işletmeci sayısı gibi kıstaslar Bakanlık tarafından belirlenir ve yetkilendirme Kurum tarafından yapılır. Ancak, ulusal çapta verilecek frekans bandı kullanımını ihtiva eden ve sınırlı sayıda işletmeci tarafından yürütülmesi gereken elektronik haberleşme hizmetlerine ilişkin ihaleleri Bakanlık gerekli gördüğü hallerde doğrudan kendisi de yapabilir.

b) (a) bendinde belirtilen hususların dışında kalan ve sınırlı sayıda işletmeci tarafından verilecek olan elektronik haberleşme hizmetlerinin yürütülmesine ve/veya elektronik haberleşme şebeke ve alt yapısının tesisi ve işletilmesine ilişkin olarak, gerekli işlemler Kurum tarafından yürütülür.

(7) Kurum, kaynakların etkin kullanımını sağlamak amacıyla Bakanlığın görüşüne başvurarak gerekli tedbirleri alır ve yapılacak ihaleye ilişkin usul ve esasları belirler. Kurum ve yukarıdaki fıkranın (a) bendinde öngörülen hallerde Bakanlık, kullanım hakkı ile ilgili olan ihalelerde 8/9/1983 tarihli ve 2886 sayılı Devlet İhale Kanunu ve 4734 sayılı Kamu İhale Kanununa tabi değildir.

(8) Kullanım haklarının süresi, yirmibeş yıldan fazla olmamak üzere belirlenir. Bu madde uyarınca belirlenen yetkilendirme süreleri, şebeke ve hizmetin niteliği ile başvuru sahibinin talebi de dikkate alınmak suretiyle tespit edilir.

(9) Kurum, kullanım hakkı verilmesi taleplerini, millî güvenlik, kamu düzeni, kamu sağlığı ve benzeri kamu yararı gerekleri, tahsis edilmesi gereken kaynakların yetersizliği ve ihale aşamasında belirlenen yeterlik şartlarının sağlanmaması sebepleriyle reddedebilir.

(10) Kullanım hakkı, işletmecinin faaliyetlerinin mevzuata aykırı olması durumunda Kurum tarafından belirlenen usul ve esaslara göre iptal edilebilir. Kullanım hakkının iptal edildiği hallerde abonelerin menfaatlerini korumak için gerekli tedbirler alınır.

(11) Kurum, kamu güvenliği, kamu sağlığı ve benzeri kamu yararı gereklerinden kaynaklanan sebeplerin tespiti halinde, şirketlerin elektronik haberleşme alanında faaliyete geçmelerini veya elektronik haberleşme sağlamalarını gerektiğinde Bakanlığın görüşünü de alarak engelleyebilir.

(12) Bu madde hükümlerine aykırı olarak elektronik haberleşme tesisi kuran, işleten veya elektronik haberleşme hizmeti verenlerin tesisleri Kurumun talebi üzerine ilgili mülki amirlerce kapatılarak faaliyetlerine son verilir.

(13) Bildirim ve kullanım hakkı ile ilgili usul ve esaslar Kurum tarafından çıkarılacak yönetmeliklerle belirlenir.

Deneme izni

MADDE 10 – (1) Kurum, elektronik haberleşme hizmetinin verilebilmesi, elektronik haberleşme şebekesi ve altyapısının işletilebilmesi için başvuruda bulunan gerçek ve tüzel kişilere deneme veya gösterim amaçlı geçici izin verebilir. Bununla ilgili usul ve esaslar Kurum tarafından belirlenir.

Yetkilendirme ücreti

MADDE 11 – (1) Yetkilendirme ücreti, idarî ücretler ve kullanım hakkı ücretlerinden oluşur.

(2) Kurum; pazar analizi, düzenlemelerin hazırlanması ve uygulanması, işletmecilerin denetlenmesi, teknik izleme ve denetleme hizmetleri, piyasanın kontrolü, uluslararası işbirliği, uyumlaştırma ve standardizasyon çalışmaları ve diğer faaliyetleri ile her türlü idarî giderlerinden kaynaklanan masraflara katkı amacıyla işletmecinin bir önceki yıl net satışlarının

binde beşini geçmemek üzere, uluslararası yükümlülükler de dikkate alınarak işletmecilerden idarî ücret alır. **(Ek cümleler: 28/11/2017-7061/97 md.)** Ancak yıllık alınan idarî ücret, 10.000 Türk lirası alt sınırından daha az olamaz. Söz konusu alt sınır her yıl bir önceki yıla ilişkin olarak 4/1/1961 tarihli ve 213 sayılı Vergi Usul Kanunu hükümlerine göre belirlenen yeniden değerleme oranında artırılmak suretiyle uygulanır. Buna ilişkin usul ve esaslar Kurum tarafından belirlenir. (1)

(3) Tespit edilen usul ve esaslar çerçevesinde belirlenen sürede idarî ücretlerin işletmeciler tarafından ödenmemesi halinde 21/7/1953 tarihli ve 6183 sayılı Amme Alacaklarının Tahsil Usulü Hakkında Kanunun 51 inci maddesinde belirlenen usule göre hesaplanacak gecikme zammı oranı kadar faiz uygulanır. İşletmecilerden alınacak idarî ücretlerden süresinde ödenmeyenler Kurumun bildirimi üzerine 6183 sayılı Kanun hükümleri uyarınca ilgili vergi dairesi tarafından tahsil edilir ve Kuruma gelir kaydedilir. Kurum, idarî maliyet ve toplanan idarî ücreti gösteren yıllık rapor yayımlar.

(4) Kaynakların kullanım hakkının verilmesine ve söz konusu kaynakların etkin bir şekilde kullanılmasının teminine yönelik olarak kullanım hakkı ücreti alınır.

(5) Kullanım hakkı ücretlerinin asgari değerleri, Kurumun önerisi ve Bakanlığın teklifi üzerine Cumhurbaşkanı tarafından belirlenir.(2)

_____

(1) 28/11/2017 tarihli ve 7061 sayılı Kanunun 97 nci maddesiyle bu fıkraya birinci cümlesinden sonra gelmek üzere eklenen cümlelerin; yine 7061 sayılı Kanunun 123 üncü maddesiyle 1/1/2018 tarihinden itibaren elde edilecek net satışlara uygulanmak üzere aynı tarihte yürürlüğe girmesi hüküm altına alınmıştır.

(2) 2/7/2018 tarihli ve 703 sayılı Kanun Hükmünde Kararnamenin 205 inci maddesiyle bu fıkrada yer alan "Bakanlar Kurulu" ibaresi "Cumhurbaşkanı" şeklinde değiştirilmiştir.

(6) Kullanım hakkı ücretleri, 5369 sayılı Kanun hükümleri saklı kalmak kaydıyla Hazineye gelir kaydedilmek üzere ilgili muhasebe birimine yatırılır. Zamanında ödenmeyen kullanım hakkı ücretleri, Kurumun bildirimi üzerine, 6183 sayılı Kanun hükümleri uyarınca, ilgili vergi dairesince tahsil olunur.

İşletmecilerin hak ve yükümlülükleri

MADDE 12 – (1) İşletmeci, Kurum düzenlemeleri ve yetkilendirmesinde öngörülen şartlara uygun olarak yetkilendirildiği kapsamdaki elektronik haberleşme hizmetini sunma hakkına sahiptir.

(2) Kurum, işletmecilere sektörün ihtiyaçları, uluslararası düzenlemeler, teknolojide meydana gelen gelişmeler gibi hususları gözeterek aşağıdaki hususlar başta olmak üzere, mevzuat doğrultusunda yükümlülükler getirebilir:

a) İdari ücretler.

b) Hizmetlerin birbiriyle uyumlu çalışabilmesi ve şebekelerarası arabağlantının sağlanması.

c) Ulusal numaralandırma planındaki numaralardan son kullanıcılara erişimin sağlanması.

ç) Ortak yerleşim ve tesis paylaşımı.

d) Kişisel veri ve gizliliğin korunması.

e) Tüketicinin korunması.

f) Kuruma bilgi ve belge verilmesi.

g) Kanunlarla yetkili kılınan ulusal kurumlarca yasal dinleme ve müdahalenin yapılmasına teknik olanak sağlanması.

ğ) Afet durumlarındaki haberleşmenin kesintisiz devam edebilmesi için gerekli tedbirlerin alınması.

h) Elektronik haberleşme şebekelerinden kaynaklanan elektromanyetik alanlara kamu sağlığını tehdit edecek şekilde maruz kalınmasının engellenmesi ile ilgili önlemlerin bu Kanun çerçevesinde alınması.

ı) Erişim yükümlülükleri.

i) Elektronik haberleşme şebekelerinin bütünlüğünün idame ettirilmesi.

j) İzinsiz erişime karşı şebeke güvenliğinin sağlanması.

k) Hizmet kalitesi de dahil olmak üzere standartlar ve spesifikasyonlara uyumluluk.

l) İlgili mevzuat uyarınca Kurum tarafından istenen hizmetleri yerine getirmek.

(3) Kullanım hakkı verildiği durumlarda, yukarıdakilere ilaveten sektörün ihtiyaçları, uluslararası düzenlemeler, teknolojide meydana gelen gelişmeler gibi hususları gözeterek aşağıdaki hususlar başta olmak üzere, mevzuat doğrultusunda yükümlülükler getirilebilir:

a) Frekans kullanım hakkının verildiği hizmet, şebeke ya da teknoloji türü ile numara kullanım hakkının verildiği hizmetin kapsamı.

b) Frekans ve numaraların etkin ve verimli kullanımı.

c) Elektromanyetik girişimin önlenmesi.

ç) Numara taşınabilirliği.

d) Rehber hizmeti.

e) Yetkilendirme süresi.

f) Hak ve yükümlülüklerin devri.

g) Kullanım hakkı ücretleri.

ğ) İhale sürecinde üstlenilen taahhütler.

h) Frekans ve numara kullanımları ile ilgili uluslararası anlaşmalar çerçevesindeki yükümlülüklere uyulması.

(4) İşletmecilerin hak ve yükümlülükleri ile ilgili usul ve esaslar Kurumca belirlenir.

(5) İşletmeciler, elektronik haberleşme sistemleri üzerinden millî güvenlikle ve 5397 ve 5651 sayılı kanunlar ve ilgili diğer kanunlarda getirilen düzenlemelerle ilgili taleplerin karşılanmasına yönelik teknik alt yapıyı, elektronik haberleşme sistemini hizmete sunmadan önce kurmakla yükümlüdür. Halen elektronik haberleşme hizmeti sunan işletmeciler de; söz konusu teknik alt yapıyı, Kurum tarafından belirlenecek süre içerisinde aynı şartlarla ve tüm harcamaları kendilerine ait olmak üzere kurmakla yükümlüdürler.

İKİNCİ BÖLÜM
Tarifeler

Tarifelerin düzenlenmesi

MADDE 13 – (1) Tarife; abonman ücreti, sabit ücret, konuşma ücreti, hat kirası ve benzeri değişik ücret kalemlerinden birisi veya birkaçı olarak tespit edilebilir.

(2) Her türlü elektronik haberleşme hizmetinin sunulması karşılığında uygulanacak tarifeler aşağıdaki hükümlere tabidir:

a) İşletmeciler, uygulayacakları tarifeleri, ilgili mevzuat ve Kurum düzenlemelerine aykırı olmayacak şekilde serbestçe belirlerler.

b) İşletmecinin ilgili pazarda etkin piyasa gücüne sahip olduğunun belirlenmesi halinde Kurum, tarifelerin onaylanması, izlenmesi ve denetlenmesine ilişkin yöntemleri ve tarifelerin alt ve üst sınırları ile bunların uygulama usul ve esaslarını belirleyebilir.

c) İşletmecinin ilgili pazarda etkin piyasa gücüne sahip olduğunun belirlenmesi halinde; Kurum, fiyat sıkıştırması, yıkıcı fiyatlandırma gibi rekabeti engelleyici tarifelerin önlenmesi için gerekli düzenlemeleri yapar ve uygulamaları denetler.

(3) Bu maddenin uygulanması ile tarifelerin Kuruma sunulması, kamuoyuna duyurulması ve yayımlanması hususlarına ilişkin usul ve esaslar Kurum tarafından belirlenir.

Tarifelerin düzenlenmesine ilişkin ilkeler

MADDE 14 – (1) Kurum, her türlü elektronik haberleşme hizmetinin sunulması karşılığında uygulanacak tarifelere ilişkin düzenlemeleri yaparken, aşağıdaki ilkeleri göz önünde bulundurur:

a) Kullanıcıların makul bir ücret karşılığında elektronik haberleşme hizmetlerinden yararlanmasını sağlayacak uygulamaların teşvik edilmesi.

b) Tarifelerin, 5369 sayılı Kanunun 3 üncü maddesinin birinci fıkrasının (c) bendinde belirtilen ihtiyaç sahibi kesimlere mahsus, kapsamı açık ve sınırları belirlenmiş kolaylıklar sağlanması halleri saklı olmak üzere, benzer konumdaki kullanıcılar arasında haklı olmayan nedenlerle ayrım gözetilmeksizin adil ve şeffaf olması.

c) Tarifelerin, sunulan elektronik haberleşme hizmetlerine ilişkin maliyetleri mümkün olduğunca yansıtması.

ç) Bir hizmetin maliyetinin diğer bir hizmetin ücreti yoluyla desteklenmemesi veya karşılanmaması.

d) Tarifelerin, rekabetin engellenmesi, bozulması veya kısıtlanmasına neden olacak şekilde belirlenmemesi.

e) Uluslararası uygulamaların uygun olduğu ölçüde dikkate alınması.

f) Tarifelerin, teknolojik gelişmeyi ve yeni teknolojilerin makul fiyatlarla kullanılmasına olanak veren yatırımları teşvik edecek nitelikte olması.

g) Tüketici menfaatinin gözetilmesi.

ğ) Tüketicilerin tarifelere ilişkin hususları bilmesinin sağlanması.

h) Rakip işletmecilerin kendi kullanıcılarına sunacağı elektronik haberleşme hizmetleri için etkin piyasa gücüne sahip işletmeciden talep edeceği temel girdi niteliğinde olan elektronik haberleşme hizmetlerinde oluşan fiyatları da dikkate alması.

ÜÇÜNCÜ BÖLÜM
Erişim ve Arabağlantı

Erişimin kapsamı

MADDE 15 – (1) Elektronik haberleşme hizmetlerinde erişim kapsamında aşağıdaki hususlar yer alır:

a) Yerel ağa ayrıştırılmış erişim ve veri akış erişimini de içerecek şekilde elektronik haberleşme şebekesi bileşenlerine ve ilgili tesislerine her türlü yöntemle erişim.

b) Binalar, borular ve direkleri de içerecek şekilde mevcut erişim seçeneklerini de dikkate alarak fiziksel alt yapıya erişim.

c) İşletim destek sistemlerini de içerecek şekilde ilgili yazılım sistemlerine erişim.

ç) Numara dönüşümüne veya eşdeğer işlevselliğe sahip sistemlere erişim.

d) Sanal şebeke hizmetlerine rekabet durumunu da dikkate alarak erişim.

e) İki elektronik haberleşme şebekesi arasındaki arabağlantı.

f) Ulusal dolaşım da dahil olmak üzere sabit ve mobil şebekelere erişim.

g) Koşullu erişim sistemlerine erişim.

ğ) Yeniden satış amacıyla hizmetlerin toptan seviyede sunulması.

h) Kurum düzenlemeleri ile belirlenen diğer hallerdeki erişim.

Erişim yükümlülüğü

MADDE 16 – (1) Erişim yükümlüleri ve yükümlülüğün kapsamı Kurum tarafından belirlenir. Kurum; bir işletmecinin diğer bir işletmecinin bu Kanunun 15 inci maddesinde belirtilen hususlarda erişimine izin vermemesinin veya aynı sonucu doğuracak şekilde erişim için makul olmayan süre ve şartlar ileri sürmesinin, rekabet ortamının oluşumunu engelleyeceğine veya ortaya çıkacak durumun, son kullanıcıların aleyhine olacağına karar vermesi halinde, söz konusu işletmeciye diğer işletmecilerin erişim taleplerini kabul etme yükümlülüğü getirebilir.

(2) Bu Kanun uyarınca, tüm işletmeciler, talep gelmesi halinde birbirleriyle arabağlantı müzakerelerinde bulunmakla yükümlüdürler. Tarafların anlaşamamaları halinde Kurum, işletmecilere arabağlantı sağlama yükümlülüğü getirebilir.

(3) Kurum, erişim ve arabağlantı yükümlülüklerini, bu Kanunun 4 üncü maddesinde belirtilen ilkeleri göz önünde bulundurarak kamu menfaati açısından gerekli gördüğü hallerde, yapacağı düzenlemelerle sınırlandırabilir.

(4) Kurum, tüm erişim anlaşmalarının bu Kanunun amaç ve kapsamına, rekabetin ve tüketici haklarının korunmasına ve şebekelerin bütünlüğü ve birlikte çalışılabilirliği ile hizmetlerin karşılıklı işletilebilirliğine uygun olarak tesis edilmesine ve uygulanmasına yönelik düzenlemeleri yapar.

(5) Kurum, erişim yükümlüsü işletmecilere, diğer işletmecilerin makul erişim taleplerini, bu Kanun hükümleri çerçevesinde karşılamalarına yönelik olarak eşitlik, ayrım gözetmeme, şeffaflık, açıklık, maliyet ve makul kâra dayalı olma yükümlülükleri ile erişim hizmetlerini kendi ortaklarına, iştiraklerine veya ortaklıklarına sağladıkları ile aynı koşul ve kalitede sunma yükümlülüğü getirebilir.

(6) Bu maddenin uygulanmasına ilişkin usul ve esaslar Kurum tarafından belirlenir.

Tesis paylaşımı ve ortak yerleşim

MADDE 17 – (1) Bir işletmecinin tesislerini kamuya veya üçüncü şahıslara ait bir arazinin üzerine veya altına yerleştirebildiği veya bu tür arazileri kullanabildiği veya kamulaştırma müessesesinden yararlanabildiği hallerde Kurum, çevrenin korunması, kamu sağlığı ve güvenliği, şehir ve bölge planlaması ve kaynakların etkin kullanılması gereklerini gözeterek ilgili işletmeciye söz konusu tesisleri ve/veya araziyi makul bir bedel karşılığında diğer işletmecilerle paylaşmasına ilişkin rekabet üzerindeki etkileri dikkate alarak yükümlülükler getirebilir.

(2) Kurum, işletmecilere kendi tesislerinde, diğer işletmecilerin ekipmanları için maliyet esaslı bir bedel karşılığında, başta fiziksel ortak yerleşim olmak üzere her türlü ortak yerleşim sağlama yükümlülüğü getirebilir. Kurumca öngörülmesine rağmen işletmecilerin ortak yerleşim tarifelerini maliyet esaslı belirlememesi ve bu durumun tespit edilmesi halinde, Kurum ortak yerleşim tarifelerini; maliyetleri, uluslararası uygulamaları ve/veya rayiç bedelleri uygun olduğu ölçüde dikkate alarak belirler.

(3) Radyo ve televizyon yayınlarını da içeren her türlü yayının belirlenmiş emisyon noktalarından yapılabilmesini teminen, ortak anten sistem ve tesisleri kurulması da dahil tesis paylaşımı ve ortak yerleşim ile ilgili usul ve esaslar Kurumca belirlenir. Gerekli hallerde uygulamayı teşvik amacıyla ortak anten sistem ve tesisleriyle ilgili olarak bu Kanuna ekli ücret tarifesinde yer alan ücretlerden muafiyet uygulaması da dahil olmak üzere gerekli iş ve işlemler Kurumca yürütülür. Ortak anten sistem ve tesisleri hakkında da elektronik haberleşmeyle ilgili alt yapı oluşumuna ilişkin hükümler uygulanır. Kurum düzenlemeleri çerçevesinde, belediyeler, mülki amirler ve diğer kamu kurumları ortak anten sistem ve tesisleriyle ilgili yer temini de dahil her türlü kolaylığı göstermek ve yardımda bulunmakla yükümlüdürler.

Erişim anlaşmaları ve uzlaşmazlıkların çözümü

MADDE 18 – (1) Erişim anlaşmaları taraflar arasında ilgili mevzuata ve Kurum düzenlemelerine aykırı olmamak kaydıyla serbestçe müzakere edilerek imzalanır. Taraflar arasında erişim talebinden itibaren azami iki ay içerisinde anlaşma tesis edilememesi veya mevcut erişim sözleşmesinde bu Kanun kapsamında herhangi bir anlaşmazlık vuku bulması halinde Kurum, taraflardan herhangi birinin başvurusu üzerine, belirleyeceği esaslar çerçevesinde taraflar arasında uzlaştırma prosedürü işletmeye ve/veya geçici ücretin belirlenmesi de dahil olmak üzere, kamu menfaati açısından gerekli gördüğü diğer tedbirleri almaya veya uzlaştırma talebini reddetmeye yetkilidir.

(2) Kurum, uzlaştırma sürecinde tarafların anlaşamaması halinde, erişim anlaşmasının anlaşmazlık konusu olan hüküm, koşul ve ücretlerini, belirlenen istisnai haller hariç olmak üzere iki ay içerisinde belirlemeye yetkilidir. Belirlenen hüküm, koşul ve ücretlerin işletmeciler tarafından, mevzuat ve Kurum düzenlemeleri çerçevesinde aksi kararlaştırılıncaya kadar uygulanmasına devam olunur.

(3) Erişim anlaşmaları imzalanmasını müteakip Kuruma sunulur. Kurum ilgili mevzuata ve Kurum düzenlemelerine aykırılık hallerinde işletmecilerden anlaşmalarda değişiklik yapılmasını ister. İşletmeciler Kurumun değişiklik isteğini yerine getirmekle yükümlüdür.

(4) Erişim anlaşmaları, ticarî sırlar dışında alenîdir.

(5) Bu maddenin uygulanma usul ve esasları Kurum tarafından belirlenir.

Referans erişim teklifi

MADDE 19 – (1) Kurum, erişim yükümlüsü işletmecilere referans erişim teklifi hazırlama yükümlülüğü getirebilir. Kurum tarafından referans erişim teklifi hazırlama yükümlülüğü getirilen işletmeciler, bu yükümlülüğün getirildiği tarihten itibaren üç ay içerisinde söz konusu teklifleri Kurumun onayına sunmakla yükümlüdürler.

(2) Kurum, bu Kanunun 4 üncü maddesindeki ilkeleri göz önünde bulundurarak, referans erişim tekliflerinde gerekli değişikliklerin yapılmasını işletmecilerden isteyebilir. İşletmeciler, Kurumun istediği değişiklikleri belirtilen biçimde ve verilen sürede yerine getirmekle yükümlüdürler. Verilen süre içerisinde Kurumun istediği değişikliklerin yapılmaması halinde, Kurum bu değişiklikleri re'sen yapabilir.

(3) Kurum uygun gördüğü teklifleri onaylar. İşletmeciler, Kurum tarafından onaylanan referans erişim tekliflerini yayımlamakla ve Kurum tarafından onaylanan referans erişim tekliflerindeki şartlarla erişim sağlamakla yükümlüdürler.

(4) Bu maddenin uygulama usul ve esasları Kurum tarafından belirlenir.

Erişim tarifeleri

MADDE 20 – (1) Kurum, erişim yükümlüsü işletmecilere, erişim tarifelerini maliyet esaslı olarak belirleme yükümlülüğü getirebilir. Kurum tarafından talep edilmesi halinde yükümlü işletmeciler erişim tarifelerinin maliyet esaslı belirlendiğini ispat etmek zorundadır.

(2) Yükümlü işletmecilerin tarifelerini maliyet esaslı belirlemediğini tespit etmesi halinde, Kurum erişim tarifelerini maliyet esasına göre belirler. Kurum, tarifeleri maliyet esasına göre belirleyinceye kadar diğer ülke uygulamalarını uygun olduğu ölçüde dikkate alarak, tarifeleri belirler ve/veya tarifelere üst sınır koyabilir. Kurumun belirlediği tarifelere uyulması zorunludur.

Hesap ayrımı ve maliyet muhasebesi

MADDE 21 – (1) Kurum ilgili pazarda etkin piyasa gücüne sahip işletmecilere hesap ayrımı yükümlülüğü getirebilir. Hesap ayrımı yükümlülüğü getirilen işletmeciler, Kurum tarafından belirlenecek hesap ayrımı ve maliyet muhasebesine ilişkin usul ve esaslar kapsamında faaliyet alanları ve iş birimleri için ayrı ayrı hesap tutma ile yükümlüdür.

(2) Kurum işletmecilerin hesaplarını denetleyebilir veya denetim yetkisi vermek suretiyle denetletebilir veya işletmecilere hesaplarını bağımsız denetim kuruluşlarına denetletme yükümlülüğü getirebilir. Denetim yetkisi verilenler ve bağımsız denetim kuruluşları, bu Kanun ve hesap ayrımı ve maliyet muhasebesine ilişkin mevzuat hükümleri çerçevesinde inceleme ve denetimden sorumludurlar. Denetim yetkisi verilenler ve bağımsız denetim kuruluşları, denetimlere ilişkin olarak hazırladıkları raporlardaki yanlış ve yanıltıcı bilgi ve kanaatler nedeniyle doğabilecek zararlardan ve üçüncü kişilere verecekleri zararlardan sorumludurlar. Hesap ayrımı ve maliyet muhasebesi kapsamında yapılan denetime ilişkin giderler ilgili işletmeciler tarafından karşılanır.

(3) Kurum, işletmecilere; hesap ayrımı ve maliyet muhasebesi yükümlülükleri kapsamında hazırladıkları bilgi ve belgeleri yayımlama yükümlülüğü getirebilir. Kurum, gerekli gördüğü takdirde bu bilgi ve belgeleri kendisi de yayımlayabilir. Yayımlanacak bilgi ve belgelerin kapsamı Kurum tarafından belirlenir.

(4) Bu maddenin uygulanmasına ilişkin hususlar Kurum tarafından düzenlenir.

DÖRDÜNCÜ BÖLÜM
Geçiş Hakkı

Geçiş hakkının kapsamı

MADDE 22 – (1) Geçiş hakkı; elektronik haberleşme hizmeti vermek amacıyla, her türlü elektronik haberleşme alt yapısını ve bunların destekleyici ekipmanlarını, kamu ve/veya özel mülkiyete konu taşınmazların altından, üstünden, üzerinden geçirme ve bu alt yapıyı kurmak, değiştirmek, sökmek, kontrol, bakım ve onarımlarını sağlamak ve benzeri amaçlarla söz konusu mülkiyet alanlarını bu Kanun hükümleri çerçevesinde kullanma hakkını kapsar.

Geçiş hakkı talebinin kabulü

MADDE 23 – (1) Taşınmaza kalıcı zarar verilmemesi, bu taşınmaz üzerindeki hakların kullanımının sürekli biçimde aksatılmaması koşuluyla, teknik olarak imkan dahilinde, seçeneksiz ve ekonomik açıdan orantısız maliyetler ihtiva etmeyen geçiş hakkı talepleri, makul ve haklı sebepler saklı kalmak üzere, kabul edilir.

(2) Kamu kurum ve kuruluşları, kendilerine yapılan geçiş hakkı talebini içeren başvuruları öncelikli olarak ve gecikmeye mahal vermeden, değerlendirir ve altmış gün içinde sonuçlandırırlar. Benzer konumdaki işletmeciler arasında ayrım gözetmeksizin şeffaf davranılır.

Tesis paylaşımı ve ortak yerleşimin önceliği

MADDE 24 – (1) Geçiş hakkı kapsamında kullanılacak bir taşınmaz üzerinde halihazırda bu Kanun ve Kurum düzenlemeleri çerçevesinde, Kurum tarafından ortak yerleşim ve tesis paylaşımı yükümlülüğüne karar verilmiş bir elektronik haberleşme şebekesi bulunması halinde ortak yerleşim ve tesis paylaşımına öncelik verilir.

Anlaşma serbestisi

MADDE 25 – (1) İşletmeci ile geçiş hakkı sağlayıcısı, ilgili mevzuata ve Kurum düzenlemelerine aykırı olmamak koşulu ile geçiş hakkına ilişkin anlaşmaları 4721 sayılı Türk Medeni Kanunu hükümleri saklı kalmak üzere serbestçe yapabilirler. İşletmeciler, Kurum tarafından istenmesi halinde yapılan anlaşma ile ekleri ve değişikliklerini, her türlü bilgi, belge ile yazışmaları Kuruma bildirmekle yükümlüdürler.

Çevrenin korunması

MADDE 26 – (1) Geçiş hakkı kapsamında tanınan hakların kullanımı sırasında geçiş yollarında ve etrafında bulunan ağaçların ve çevresel değerlerin korunması esastır. Geçiş hakkı uygulamasında tarihi eserler ile kültür ve tabiat varlıklarının korunmasına ilişkin mevzuat hükümleri saklıdır. Bu konuda alınması gereken izinlere ilişkin başvurular ilgili kuruluşlarca altmış gün içinde sonuçlandırılır.

Diğer alt yapılarla ilişkili durumlar

MADDE 27 – (1) İşletmeciye ait elektronik haberleşme şebekesi ve bunların destekleyici ekipmanları, geçiş hakkının kullanılacağı taşınmaz üzerinde halihazırda bulunan, kanalizasyon, su, gaz kanalları, demiryolları, elektrik tesisleri, diğer elektronik haberleşme şebekesi ve benzeri kamu hizmeti alt yapısına zarar vermeyecek şekilde ve mesafede tesis edilir. Yeni alt yapı ve şebeke tesis edecek işletmeci, ilgili kamu kurumu ve kuruluşu ile gerekli koordinasyonu sağlayarak hareket eder. Zaruri hallerde söz konusu kamu hizmetlerinin kesintiye uğramaması için alınacak önlemlerden doğan masrafları geçiş hakkını kullanan taraf tazmin eder. Geçiş hakkına ilişkin çalışmalardan kaynaklanan tüm masraflar işletmeci tarafından karşılanır.

Geçiş hakkına ilişkin yükümlülükler

MADDE 28 – (1) Geçiş hakkı sağlayıcısı, işletmecinin geçiş hakkı kapsamında yürüteceği faaliyetlerin, kesintisiz ve güvenli bir şekilde gerçekleştirilmesini sağlamak amacıyla, masrafları işletmeci tarafından karşılanmak üzere, gerekli tüm önlemlerin alınmasına ve çalışmaların yapılmasına izin verir.

(2) Geçiş hakkı sağlayıcısı bu haklarını kullanırken, işletmecinin geçiş hakkı kapsamında yürüteceği faaliyetler ile işletmeciye ait elektronik haberleşme şebekesini tehlikeye düşürücü veya zarar verici işlemlerden kaçınmakla yükümlüdür.

(3) Geçiş hakkı kullanan işletmeciler, geçiş hakkı sağlayıcısının geçiş hakkının kullanımı dışında ayrıca uğradıkları zararları en geç bir ay içerisinde karşılamak zorundadırlar.

Yetkilendirmenin devri halinde geçiş hakkı anlaşması

MADDE 29 – (1) Yetkilendirmenin devri halinde kamu hizmetinin kesintiye uğramaması için, geçiş hakkı sağlayıcısı tarafından aksi ileri sürülmediği müddetçe; geçiş hakkı anlaşmasının, geçiş hakkı sağlayıcısı ile yeni işletmeci arasında aynı şartlarda geçerli olacağı kabul olunur.

Kamulaştırma

MADDE 30 – (1) Bu Kanunda öngörülen faaliyetlerin gerektirmesi halinde, kişilerin özel mülkiyetinde bulunan taşınmazlar hakkında 4/11/1983 tarihli ve 2942 sayılı Kamulaştırma Kanununda belirtilen esaslar dahilinde kamulaştırma yapılır. Bu konuda Bakanlıkça verilecek lüzum kararı, kamu yararı kararı yerine geçer ve başka bir onaya gerek kalmaksızın müteakip işlemler Kamulaştırma Kanunu hükümlerine göre Bakanlıkça yürütülür. Kamulaştırılan taşınmazların mülkiyeti Hazineye ait olur ve bu taşınmazlar üzerinde Maliye Bakanlığı tarafından işletmeci lehine yetkilendirme süresi ile sınırlı olmak üzere bedelsiz olarak irtifak hakkı tesis edilir. Yetkilendirmenin sona ermesi veya iptali halinde, bu taşınmazların üzerinde işletmeci lehine tescil edilmiş olan irtifak hakkı ilgili defterdarlık veya malmüdürlüğünün talebi üzerine tapu idaresince re'sen terkin edilir ve bu taşınmazlar başkaca bir işleme gerek kalmaksızın Hazineye devredilir. İşletmeci tarafından daha önce ödenen kamulaştırma bedelleri iade edilmez.

(2) Bu Kanunda öngörülen faaliyetler ile ilgili olarak işletmeci tarafından Hazinenin özel mülkiyetindeki veya Devletin hüküm ve tasarrufu altındaki taşınmazlar üzerinde irtifak hakkı tesisi, kullanma izni verilmesi veya kiralama yapılmasına ihtiyaç duyulması halinde Kurumdan talepte bulunulur. Bu talebin Kurulca uygun görülmesi halinde, ilgili mevzuatı uyarınca Maliye

Bakanlığı ile ilgili işletmeci arasında yetkilendirme süresi ile sınırlı olmak üzere bedeli karşılığında irtifak hakkı tesisi, kullanma izni veya kiralama sözleşmesi düzenlenir. Bu sözleşmelerde, sözleşmenin geçerliliğinin yetkilendirme süresi ile sınırlı olacağı yönünde hüküm yer alır. Bu şekilde tesis edilen irtifak hakkı, kullanma izni veya kiralama bedelini ödeme yükümlülüğü işletmeciye aittir.

BEŞİNCİ BÖLÜM
Numaralandırma ve İnternet Alan Adları

Ulusal numaralandırma planı

MADDE 31 – (1) Kurum, Bakanlık politikası doğrultusunda ulusal numaralandırma planını hazırlar ve plana uygun olarak numara tahsis işlemlerini yapar. Numara kaynaklarının tahsisi, etkin ve verimli kullanımının sağlanması, geri alımı ve benzeri konular Kurumca çıkarılacak yönetmelikle belirlenir. Kurum, elektronik haberleşme hizmeti ve/veya şebekesi veya altyapısı için yeterli numara kaynağının bulunmasını sağlayacak şekilde gerekli planlamaları yapar ve numara kaynaklarının adil, şeffaf ve ayrımcı olmayan ilkeler çerçevesinde yönetimini sağlar.

(2) Kurum, numara kaynağının etkin ve verimli kullanılmasına yönelik olarak yapacağı düzenlemeler veya ilgili uluslararası kuruluşların düzenlemeleri doğrultusunda yapılabilecek yeni planlamalar çerçevesinde, işletmecilerin de görüşünü alarak ulusal numaralandırma planında değişiklik yapabilir. Değişikliklerin uygulanması amacıyla işletmecilere uluslararası normlara uygun olacak şekilde süre verilir. İşletmeciler bu değişiklikleri uygular ve gerekli önlemleri alır.

(3) Kurum, numara tahsis ve kullanımını koşullara bağlayabilir, kamu düzeni ve millî güvenliğin gerektirdiği durumlar, numara kapasitesi ihtiyacı, üye olunan uluslararası kuruluşların düzenlemeleri veya taraf olunan uluslararası anlaşmalar doğrultusunda veya Kurum düzenlemelerine uygun olarak kullanılmadığı durumlarda tahsisli numaralarda değişiklik yapılabilir ve tahsisli numaralar geri alınabilir. Bu konuda yapılacak düzenlemeler sonucunda Kurum herhangi bir yükümlülük altına girmez.

(4) Ankesörlü telefon hizmeti kullanıcıları da dahil olmak üzere, kamu kullanımına açık telefon hizmetinden faydalanan kullanıcılar, herhangi bir ücret ödemeden 112 ve Kurumca belirlenen diğer acil çağrı numaralarını çevirerek acil çağrıya cevap vermekle yetkili kuruluşa erişme hakkına sahiptir. Kurumca belirlenen esaslar çerçevesinde işletmeciler ücretsiz olarak, kullanıcıların 112 acil çağrı numarasına ve Kurumca belirlenebilecek diğer acil çağrı numaralarına sunmakta oldukları hizmetin kapsam ve kalitesine uygun olarak erişimlerini sağlamak ve acil yardım talebinde bulunan kullanıcıların yerlerini tespit ederek ilgili kuruluşa bildirmekle yükümlüdür.

Numara taşınabilirliği

MADDE 32 – (1) İşletmeciler, Kurum düzenlemeleri çerçevesinde işletmeci numara taşınabilirliğini sağlamakla yükümlüdür. Kurum bu yükümlülüğün uygulanmasına ilişkin usul ve esasları işletmecilerin de görüşünü alarak belirler. İşletmeciler, Kurum düzenlemelerine uygun olarak şebekelerinde gerekli düzenlemeleri yapar ve uygular. İşletmeciler, işletmeci numara taşınabilirliği kapsamında şebekelerinde yapacakları düzenlemelerden kaynaklanabilecek gider kalemleri için Kurumdan hak talebinde bulunamaz.

(2) İşletmeciler, işletmeci numara taşınabilirliği hizmeti vermek veya taşınmış numaralara çağrı göndermek üzere kuracakları sistemler ile mevcut sistemlerinde yapacakları değişiklikler dolayısıyla oluşan maliyeti kendileri karşılar. Ortak kurulacak referans veri tabanı ve benzeri sistemler, Kurumca veya talep eden işletmeciler tarafından Kurum düzenlemeleri çerçevesinde kurulur ve/veya işletilir. Söz konusu sistemler Kurumun belirleyeceği usul ve esaslar çerçevesinde işletmeci numara taşınabilirliği hizmeti vermekle yükümlü işletmecilerce veya üçüncü bir tarafça da kurulabilir ve/veya işletilebilir. Bu sistemlere ilişkin maliyet paylaşım esasları Kurum tarafından düzenlenebilir.

(3) Kurum, işletmeci numara taşınabilirliği kapsamında tüketicilerin korunması ve anılan hizmetten en iyi koşullarda faydalanabilmelerini sağlamak amacıyla gerekli her türlü tedbiri alır.

(4) İşletmecilerin, işletmeci numara taşınabilirliği kapsamında birbirlerine uygulayacağı ücretler konusunda bu Kanunun 20 nci maddesi hükümleri uygulanır.

(5) Numara taşınabilirliği dolayısıyla aboneye doğrudan yansıyabilecek ücretler, abonelerin bu hizmeti almalarını engelleyici nitelikte olmamalıdır.

(6) Kurum işletmecilere, adres taşınabilirliği veya hizmet taşınabilirliği sunma yükümlülüğü getirebilir. Bu yükümlülüğe ilişkin usul ve esaslar işletmecilerin de görüşü alınarak Kurum tarafından belirlenir.

Taşıyıcı seçimi ve taşıyıcı ön seçimi

MADDE 33 – (1) Kurum, işletmecilere taşıyıcı seçimi ve taşıyıcı ön seçimi uygulama yükümlülüğü getirebilir. İlgili pazarda etkin piyasa gücüne sahip işletmeciler, şebekelerinde Kurum düzenlemeleri doğrultusunda taşıyıcı seçimi ve taşıyıcı ön seçimi uygulamakla yükümlü kılınabilir. Kurum bu yükümlülüğün uygulama usul ve esaslarını belirler. İşletmeciler, taşıyıcı seçimi ve taşıyıcı ön seçimi kapsamında Kurum düzenlemelerine uygun olarak şebekelerinde gerekli düzenlemeleri yapar ve uygular. İşletmeciler, taşıyıcı seçimi ve taşıyıcı ön seçimi kapsamında şebekelerinde yapacakları düzenlemelerden kaynaklanabilecek gider kalemleri için Kurumdan hak talebinde bulunamaz.

(2) İşletmecilerin taşıyıcı seçimi ve taşıyıcı ön seçimi kapsamında birbirlerine uygulayacağı ücretler konusunda bu Kanunun 20 nci maddesi hükümleri uygulanır.

(3) Taşıyıcı seçimi ve taşıyıcı ön seçimi dolayısıyla aboneye doğrudan yansıyabilecek ücretler, abonelerin bu hizmeti almalarını engelleyici nitelikte olamaz.

(4) Abonelere ait faturalama bilgisi bulunan sabit ya da mobil telefon hizmeti sunan işletmeciler ile bu şebekeler üzerindeki abonelere hizmet veren diğer işletmeciler arasında, abonenin birden fazla fatura almasını önlemek amacıyla, tüketiciye ek yük getirmeyecek şekilde, faturalama anlaşması yapılabilir. Bu konuya ilişkin usul ve esasları belirlemeye Kurum yetkilidir.

Haczedilmezlik ve haberleşme hizmetlerinin sürekliliği

MADDE 34 – (1) Elektronik haberleşme hizmetleri ile ilgili olarak abone veya kullanıcılara tahsis edilen frekans, numara ve hat kullanımı ile internet alan adları gibi intifa ve kullanım hakları ile işletmecilerin yetkilendirmeleri hiçbir şekilde haczedilemez.

(2) Genel güvenlik ve asayişe yönelik haberleşmelerden kapsamı Kurum tarafından belirlenmiş olanlar her ne sebeple olursa olsun kesintiye uğratılamaz.

(3) Elektronik haberleşme alt yapısına mahkeme kararı veya ilgili mevzuatı uyarınca Kurum, Bakanlık veya diğer yetkili merciler tarafından alınmış bir karar olmadıkça, elektronik haberleşmenin aksamasına neden olacak biçimde müdahalelerde bulunulamaz.

İnternet alan adları

MADDE 35 – (1) İnternet alan adlarının tahsisini yapacak kurum veya kuruluşun tespiti ile alan adı yönetimine ilişkin usul ve esaslar Bakanlık tarafından belirlenir.

ÜÇÜNCÜ KISIM
Spektrum Yönetimi

Frekans planlama, tahsis ve tescili

MADDE 36 – (1) Radyo ve televizyon yayınlarına ilişkin ilgili kanununda belirtilen hükümler saklı kalmak kaydıyla:

a) Telsiz yayınlarının birbirleri üzerinde elektromanyetik girişim oluşturmaması ve frekans bantlarının etkin ve verimli şekilde kullanılmasını sağlamak amacıyla uluslararası frekans planlaması ve uluslararası kuruluşların aldığı kararlar da dikkate alınarak milli frekans planlaması, tahsisi, uluslararası koordinasyon ile tescil işlemleri Kurum tarafından yapılır ve uygulanır.

b) Telsiz cihaz veya sistemi kurmak ve işletmek isteyenler Kuruma frekans tahsis ve tescil işlemlerini yaptırmak zorundadır. Ancak, bu Kanunun 37 nci maddesinde belirtilen, herhangi bir telsiz kurma ve kullanma iznine ve telsiz ruhsatnamesine ihtiyaç göstermeksizin kullanılan telsiz cihaz ve sistemlerinde kullanılacak frekanslar için tahsis ve tescil işlemi yapılmaz.

(2) Frekans tahsislerinde Dışişleri Bakanlığı, Jandarma Genel Komutanlığı ile Sahil Güvenlik Komutanlığı ihtiyaçları da dahil Türk Silahlı Kuvvetlerine, Millî İstihbarat Teşkilatı Müsteşarlığına ve Emniyet Genel Müdürlüğüne öncelik tanınır.

(3) Türk Silahlı Kuvvetleri ile Radyo ve Televizyon Üst Kurulu, milli frekans planı çerçevesinde kendilerine tahsis edilen frekans bantlarında frekans planlamasını yapar ve uygular.

(4) Teknolojik gelişmeler ve Ülkemizin taraf olduğu uluslararası kuruluşların kararları doğrultusunda yapılabilecek yeni planlamalar çerçevesinde, Kurum, tahsis edilen frekans ve bantlar için Bakanlık ve ilgili kurumlar ile gerekli koordinasyonu sağlar. Kurum, Devlet güvenlik ve istihbaratında zafiyet yaratmayacak şekilde iptal dahil her türlü değişiklik yapabilir. Bu konuda yapılacak düzenlemeler sonucunda Kurum, herhangi bir yükümlülük altına girmez.

Telsiz kurma ve kullanma izni, telsiz ruhsatnamesi ve kullanıma ilişkin esaslar

MADDE 37 – (1) Radyo ve televizyon yayınlarına ilişkin ilgili kanununda belirtilen hükümler saklı kalmak kaydıyla, Kurum düzenlemelerinde belirtilen ve işletilmesi için frekans tahsisine ihtiyaç gösteren telsiz cihaz veya sistemi kullanıcıları, telsiz kurma ile kullanma izni ve telsiz ruhsatnamesi almak zorundadır. Bu kapsamdaki kullanıcılar telsiz cihaz veya sistemlerini Kurum düzenlemeleri ve telsiz ruhsatnamesinde belirtilen esaslara uygun olarak kurmak ve kullanmak mecburiyetindedirler.

(2) Telsiz kurma ve kullanma izni ve telsiz ruhsatnamesi verilmesi, izin ve telsiz ruhsatnamesinin süresi, yenilenmesi, değişikliği ve iptali ile ilgili usul ve esaslar ile bu çerçevede öngörülen telsiz cihaz veya sistemlerinin kurulması, kullanılması, nakli, işletme tipinin değiştirilmesi, devri ve hizmet dışı bırakılmasında kullanıcıların tabi olacağı hususlar Kurum tarafından çıkarılacak yönetmelikle belirlenir. Yetkilendirmeye tabi bulunmayan telsiz kurma ve kullanma izinleri en fazla beş yıl için verilir. Süresi içerisinde yenilenmeyen telsiz kurma ve kullanma izni ve telsiz ruhsatnamelerinde belirtilen cihaz ve sistemler için tahsis edilen frekanslar iptal edilir. Kurum tarafından yetkilendirilmiş olmak suretiyle telsiz hizmeti sunan işletmecilerin sistemlerine dahil telsiz cihazı kullanıcıları, telsiz kullanma izni ve telsiz ruhsatnamesinden bu Kanunun 46 ncı maddesinin ikinci fıkrası çerçevesinde muaftırlar.

(3) Kurum düzenlemelerinde belirlenen ve işletilmesi için frekans tahsisine ihtiyaç duyulmayan özel amaçlar için tahsis edilmiş frekans bantlarında ve çıkış gücünde çalışan Kurumca onaylı telsiz cihaz ve sistemleri, herhangi bir telsiz kurma ve kullanma iznine ve telsiz ruhsatnamesine ihtiyaç göstermeksizin kullanılabilir.

(4) Ulusal ve uluslararası kuruluşların belirlediği standart değerleri dikkate almak suretiyle telsiz cihaz ve sistemlerinin kullanımında uyulacak elektromanyetik alan şiddeti limit değerlerinin belirlenmesi, kontrol ve denetimleri münhasıran Kurum tarafından yapılır veya yaptırılır. Bu işlemler ile ilgili usul ve esaslar, Sağlık Bakanlığı ile Çevre ve Orman Bakanlığının görüşleri de dikkate alınmak suretiyle Kurum tarafından çıkarılacak yönetmelik ile belirlenir. Yönetmelik ile belirlenen limit değerlere ve güvenlik mesafesine uygun bulunan ilgili tesisler başkaca bir işleme gerek kalmaksızın Kurum tarafından güvenlik sertifikası düzenlenmesini müteakip kurulur ve faaliyete geçirilir.

Uydu pozisyonu tahsisi

MADDE 38 – (1) Uluslararası planlama ve kriterler çerçevesinde uydu pozisyonlarına ilişkin planlama, tahsis, uluslararası koordinasyon ile tescil işlemlerini Kurum, Bakanlıkla koordineli olarak yürütür.

Kodlu ve kriptolu haberleşme

MADDE 39 – (1) Telsiz haberleşme sistemleri üzerinden kriptolu haberleşme yapmaya Türk Silahlı Kuvvetleri, Jandarma Genel Komutanlığı ve Sahil Güvenlik Komutanlığı, Milli İstihbarat Teşkilatı, Emniyet Genel Müdürlüğü ve Dışişleri Bakanlığı yetkilidir. Ayrıca yukarıda belirtilen kurumlara ait olanlar dışında kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin elektronik haberleşme hizmeti içinde kodlu veya kriptolu haberleşme yapma usul ve esasları Kurum tarafından belirlenir.

Spektrum izleme ve denetimi

MADDE 40 – (1) Telsiz cihaz veya sistemlerinin belirlenen tekniklere ve usullere uygun olarak kurulmasının ve çalıştırılmasının denetimi, elektromanyetik girişimlerin tespiti ve giderilmesi, Devlet ve kişi güvenliğini ilgilendiren telsiz faaliyetleri konularında mevzuat dahilinde güvenlik birimleriyle işbirliği yapılması, ulusal ve uluslararası spektrum izleme,

denetleme ve denetlettirme faaliyetleri Kurum tarafından belirlenecek usul ve esaslar çerçevesinde yürütülür.

(2) Kurum, spektrum planlaması, frekans tahsis ve tescili, ücretlendirilmesi dahil spektrum yönetimi ile frekansların etkin ve verimli kullanımı için gerektiğinde tahsis edilen frekansın geri alınması ve yeniden satışı dahil spektrum ticareti ile spektrumun izlenmesi ve denetiminin gerektirdiği düzenlemeleri yönetmelikle yapmaya yetkilidir.

(3) Kurum, spektrum izleme ve denetleme faaliyetlerinde kullandığı her türlü araç, cihaz ve sistemler ile tesisler için emniyet ve muhafaza tedbirleri amacıyla gerek görmesi halinde her türlü riske karşı sigorta yaptırabilir.

(4) Kurum ulusal ve uluslararası spektrum izleme ve denetleme faaliyetlerini gerçekleştirmek üzere her türlü araç, cihaz ve sistemlerini uygun göreceği yerlerde ve mevzuatı dahilinde kurup işletebileceği gibi kurdurup işletilmesini de sağlayabilir.

(5) Sahil Güvenlik Komutanlığı, deniz yetki alanlarında bu Kanun kapsamındaki her türlü denetim ile spektrum izleme görevini yürütür.

Yabancılara uygulanacak işlemler

MADDE 41 – (1) Yabancı devletlerle yapılan anlaşmalara dayanılarak kurulmuş veya kurulacak telsiz cihaz veya sistemleri, varsa bu anlaşmalardaki özel hükümlere tabidir.

(2) Yabancı devletlerin Ülkemizdeki diplomatik temsilciliklerine, karşılıklılık esasına bağlı olarak, Dışişleri Bakanlığının uygun görüşüne istinaden telsiz cihaz veya sistemi kurma ruhsatı ve kullanma izni verilebilir.

Sahil telsiz istasyonları, deniz ve hava bandı telsiz sistemleri

MADDE 42 – (1) Deniz taşıtlarının karayla haberleşmesini sağlayan sahil telsiz istasyonlarının ve bu istasyonlar üzerinden yapılan seyir güvenliği haberleşmesi dahil telsiz haberleşme sistemlerinin kurulması ve işletilmesi hizmetleri Kıyı Emniyeti Genel Müdürlüğü bünyesindeki Telsiz İşletme Müdürlüğünce herhangi bir yetkilendirmeye tabi olmaksızın yürütülür.

(2) Her çeşit deniz ve hava bandı telsiz haberleşme sistemlerini ve sahil telsiz istasyonları üzerinden yapılan seyir güvenliği haberleşmesi dahil telsiz haberleşme sistemlerini kurma, kurdurma, kullanma izinlerini verme, ruhsatlandırma, deniz bandı telsiz haberleşme ve seyrüsefer cihazlarına çağrı kodu ve benzeri tahsis ve tescil işlemleri Telsiz İşletme Müdürlüğünce yürütülür. Telsiz İşletme Müdürlüğünün, yürütmekle görevli kılındığı hizmetlere ilişkin tarifesi, ilgili mevzuatı gereğince ilgili yönetim kurulunun onayıyla belirlenir.

Amatör telsizcilik

MADDE 43 – (1) Hiçbir maddi, kişisel veya siyasi çıkar gözetmeden, sadece kendi istek ve çabası ile telsiz iletişim teknikleri alanında kendini yetiştirmek amacıyla ulusal ve uluslararası amatör telsizcilik faaliyetinde bulunmak isteyenlere, Telsiz İşletme Müdürlüğü tarafından belirlenen esaslara ve ücretlere göre Amatör Telsizcilik Belgesi verilir.

Hava ve deniz telsiz haberleşmesinin uluslararası koordinasyonu

MADDE 44 – (1) Bu Kanunun 42 nci maddesi kapsamında, Telsiz İşletme Müdürlüğüne ait görevlere ilişkin uluslararası koordinasyon ve takip işlemleri Kurumca yürütülür.

Yasak bölgelerde yabancı uyrukluların kullanacakları telsiz cihazları

MADDE 45 – (1) Yasak bölgelerde bulunmalarına müsaade edilen yabancı uyruklulara verici, verici-alıcı ve radyo ve televizyon yayınlarını almaya yarayan cihazlar dışındaki alıcı telsiz cihazları için telsiz kurma ve kullanma izni ile telsiz ruhsatnamesi verilmesi Genelkurmay Başkanlığının müsaadesine bağlıdır.

Telsiz ücretleri

MADDE 46 – (1) Bu Kanun uyarınca telsiz cihaz ve sistemleri için alınacak telsiz ruhsatname ve yıllık kullanım ücretleri, teknik muayene ve benzeri hizmetler karşılığında alınacak ücretler bu Kanuna ekli ücret tarifesinde gösterilmiş olup, söz konusu ücretler Kuruma gelir kaydedilir. Kurumun önerisi ve Bakanlığın teklifi üzerine, bu Kanuna ekli ücret tarifesine hizmet kalemleri ilave etmeye veya çıkarmaya ve eklenen hizmet kalemlerine ilişkin ücretleri belirlemeye, Cumhurbaşkanı yetkilidir. Ücret tarifesinde belirtilen ücretleri gerektiğinde her bir ücret kalemini yüzde ellisine kadar azaltmaya veya her yıl bir önceki yıla ilişkin olarak Maliye Bakanlığınca belirlenecek yeniden değerleme oranını geçmemek kaydıyla artırmaya, Kurum yetkilidir.[1]

(2) Ancak, 10/12/2003 tarihli ve 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanununa ekli (I), (II) ve (III) sayılı cetvelde yer alan genel bütçe kapsamındaki kamu idareleri ve özel

bütçeli idareler ile düzenleyici ve denetleyici kurumlar, köy tüzel kişilikleri, Kıyı Emniyeti Genel Müdürlüğü, Kızılay, belediyeler ve Sosyal Güvenlik Kurumu tarafından kullanılan ve Dışişleri Bakanlığınca belirlenen yabancı devletlerin temsilciliklerine ait yetkilendirme kapsamı dışında olan her türlü telsiz cihaz ve sistemleri telsiz ruhsatnamesi ve yıllık kullanım ücretinden muaftır. **(Ek cümle: 28/11/2017-7061/98 md.)**[2] Ayrıca; iş ve hizmetlerin merkezî bir sunucu tarafından uzaktan izlenmesi ve yürütülmesine yönelik makineler arası veri aktarımına mahsus olan ve bunların yürütülmesi için zorunlu olanlar dışında sesli, görsel iletişim veya genel amaçlı internet erişimi için kullanılmayan telsiz cihazları ve abonelikleri de telsiz ruhsatname ve kullanma ücretlerinden muaf olup Kurum, muafiyet uygulanmasına ilişkin usul ve esas belirlemeye yetkilidir.[2]

(3) Kurumdan yetki almak suretiyle elektronik haberleşme hizmeti yürüten işletmeciler, kendi sistemlerine dahil her türlü abonenin bu Kanun uyarınca Kuruma ödemek zorunda olduğu telsiz ruhsatname ve yıllık kullanma ücretlerini, abonelerinden Kurum adına tahsil ederek, Kurum tarafından belirlenecek usuller çerçevesinde, Kurum hesaplarına devretmekle yükümlüdürler.

_____

(1) 2/7/2018 tarihli ve 703 sayılı Kanun Hükmünde Kararnamenin 205 inci maddesiyle bu fıkrada yer alan "Bakanlar Kurulu" ibaresi "Cumhurbaşkanı" şeklinde değiştirilmiştir.

(2) 28/11/2017 tarihli ve 7061 sayılı Kanunun 98 inci maddesiyle bu fıkraya eklenen cümle, aynı Kanunun 123 üncü maddesi uyarınca 1/1/2018 tarihinde yürülüğe girmiştir.

(4) **(Değişik: 28/11/2017-7061/98 md.)** Telsiz ücretleri Kurum tarafından belirlenen süre içerisinde Kurumun ilgili banka hesabına doğrudan ödenir. Telsiz ücretlerinin zamanında ödenmemesi halinde, anılan ücretler Kurumun bildirimi üzerine 6183 sayılı Kanun hükümleri uyarınca ilgili vergi dairesi tarafından tahsil edilerek Kurum hesabına aktarılır. Bu ücretlerin takip ve tahsilinde alacağın kesinleşmesi şartı aranmaz.

(5) Mobil elektronik haberleşme hizmeti sunan işletmecilerin faturalı abonelerinden (ön ödemeli aboneleri hariç olmak üzere) alınan ruhsatname ve kullanma ücretleri, işletmecinin sistemine abone olunan ay itibariyle geriye kalan aylar için yıl sonuna kadar eşit taksite bölünerek alınır.

(6) Yetkilendirme kapsamı dışında bulunan telsiz cihaz ve sistemlerine ait telsiz ruhsatname ve kullanım ücretleri, ruhsatlandırma süresine göre peşin alınır. Kurum tarafından belirlenen usul ve esaslar çerçevesinde belirlenen süre sonunda telsiz ruhsatname ve kullanım ücretlerinin ödenmemesi halinde söz konusu cihaz ve sistemlere ilişkin telsiz kurma ve kullanma izinleri ve telsiz ruhsatnameleri iptal edilir.

(7) **(Ek: 28/11/2017-7061/98 md.)** Kurum tarafından sayısı sınırlandırılarak ulusal çapta, kamuya açık mobil elektronik haberleşme hizmeti sunmak üzere imtiyaz sözleşmeleri ve/veya yetkilendirme belgelerine istinaden yetkilendirilen işletmeciler; bu Kanuna ekli ücret tarifesinin "1. TELSİZ RUHSATNAME ÜCRETLERİ" başlığı altında bulunan "b. Karasal mobil (cellular) telsiz telefon sistemi" başlıklı bölümünün (1) numaralı ve "2. TELSİZ KULLANMA ÜCRETLERİ (HER YIL İÇİN)" başlığı altında bulunan "b. Karasal mobil (cellular) telsiz telefon sistemleri" başlıklı bölümünün (1) numaralı sıraları kapsamında ödenmesi gereken ücretler yerine, aylık net satışlarının yüzde beşini aylık dönemler itibarıyla hesaplamak suretiyle, ilgili olduğu ayı izleyen ayın son işgünü mesai bitimine kadar telsiz ücreti olarak Kuruma öderler.[1]

DÖRDÜNCÜ KISIM
Tüketici ve Son Kullanıcı Hakları

Eşit hizmet alabilme hakkı

MADDE 47 – (1) İşletmeciler, sağladıkları elektronik haberleşme hizmetlerini benzer konumdaki tüketici ve son kullanıcılara eşit koşullarda ve ayrım gözetmeden sunmakla yükümlüdür. Kurum bu madde ile ilgili usul ve esasları belirler.

Tüketicinin ve son kullanıcının korunması

MADDE 48 – (1) Kurum, elektronik haberleşme hizmetlerinden yararlanan tüketici ve son kullanıcıların, hizmetlere eşit koşullarda erişebilmelerine ve hak ve menfaatlerinin korunmasına yönelik usul ve esasları belirler.

Şeffaflığın sağlanması ve bilgilendirme

MADDE 49 – (1) Kurum, son kullanıcı ve tüketicilerin azami faydayı elde edebilmeleri ve hizmetlerin şeffaflık ilkesine uygun olarak sunulabilmesi için hizmet seçenekleri, hizmet kalitesi, tarifeler ile tarife paketlerinin yayımlanmasına ve benzer hususlarda abonelerin bilgilendirilmesine yönelik olarak işletmecilere yükümlülükler getirebilir.

(2) İşletmeciler, özellikle hizmetler arasında seçim yapılırken ve abonelik sözleşmesi kurulurken tüketicilerin karar vermelerinde etkili olabilecek hususlar ile dürüstlük kuralı gereğince bilgilendirilmelerinin gerekli olduğu her durumda talep olmaksızın tüketicileri bilgilendirir.[(2)]

(3) Kurum bu maddenin uygulanmasına ilişkin usul ve esasları belirler.

---

(1) 28/11/2017 tarihli ve 7061 sayılı Kanunun 98 inci maddesiyle eklenen bu fıkranın; yine 7061 sayılı Kanunun 123 üncü maddesiyle 1/1/2018 tarihinden itibaren elde edilecek net satışlara uygulanmak üzere aynı tarihte yürürlüğe girmesi hüküm altına alınmıştır.

(2) 18/6/2020 tarihli ve 7247 sayılı Kanunun 9 uncu maddesiyle, bu fıkrada yer alan "imzalanırken" ibaresi "kurulurken" şeklinde değiştirilmiştir.

Abonelik sözleşmeleri [(1)]

MADDE 50 – (1) Tüketiciler, elektronik haberleşme hizmetine abone olurken bu hizmeti sağlayan işletmeciyle sözleşme yapma hakkına sahiptir. **(Ek cümleler:18/6/2020-7247/10 md.)** Sözleşme; yazılı olarak veya elektronik ortamda kurulur. Elektronik ortamda kurulacak sözleşmelerde, başvuru sahibinin kimliğinin doğrulanmasına imkân verecek şekilde, Kurum tarafından belirlenecek yöntemler kullanılır ve bunlara ilişkin usul ve esaslar Kurum tarafından belirlenir. Abonelik sözleşmelerinde asgari olarak elektronik haberleşme hizmeti sağlayan işletmecinin adı ve adresi, sunulacak hizmetler, teklif edilen hizmet kalitesi seviyeleri ve ilk bağlantının gerçekleştirilebilme süresi, sunulacak bakım ve onarım hizmetlerinin çeşitleri, uygulanacak tarifelerin içeriği ve tarifelerdeki değişiklikler hakkında güncel bilgilerin hangi yollardan öğrenilebileceği, sözleşmenin süresi, sona ermesi ve yenilenmesine ilişkin koşullar, işletmecinin kusurundan kaynaklanan nedenlerle sözleşmede belirtilen hizmet kalite seviyesinin sağlanamaması halinde tazminat ya da geri ödemeye ilişkin işlem, abone ile işletmeci arasında uzlaşmazlık çıkması halinde uygulanacak çözüm yöntemleri gibi bilgilere yer verilir.

(2) Kurum, re'sen veya şikayet üzerine abonelik sözleşmelerini işletmecilerden isteyebilir, inceler ve değiştirilmesi uygun görülen hususları işletmeciye bildirir. İşletmeciler Kurum düzenlemelerine uygun olarak gerekli değişiklikleri belirtilen sürede yapmakla yükümlüdür.

(3) Abonelik sözleşmelerinde yer alan ve tarafların sözleşmeden doğan hak ve yükümlülüklerinde, dürüstlük ilkesine aykırı düşecek biçimde abone aleyhine dengesizliğe neden olan hükümler geçersizdir.

(4) İşletmeci tarafından abonelik sözleşme koşullarında değişiklik yapıldığının aboneye bildirilmesinden sonra, abone herhangi bir tazminat ödemeden sözleşmeyi feshedebilme hakkına sahiptir. İşletmeciler, sözleşmede yapılacak değişiklikler yürürlüğe girmeden en az bir ay önce abonelerini bilgilendirmekle ve söz konusu değişikliklerin abone tarafından kabul edilmemesi halinde abonelerin herhangi bir tazminat ödemeden sözleşmeyi fesh edebilme haklarının bulunduğunu bildirmekle yükümlüdürler. Aboneler taleplerini bildirmek kaydıyla aboneliklerini her zaman sona erdirebilir.[2]

(5) **(Değişik: 23/10/2014-6563/14 md.)** İşletmeciler tarafından, sundukları hizmetlere ilişkin olarak abone ve kullanıcılarla, önceden izinleri alınmaksızın otomatik arama makineleri, fakslar, elektronik posta, kısa mesaj gibi elektronik haberleşme vasıtalarının kullanılması suretiyle pazarlama veya cinsel içerik iletimi gibi maksatlarla haberleşme yapılamaz. İşletmeciler, sundukları hizmetlere ilişkin olarak abone ve kullanıcılarıyla siyasi propaganda içerikli haberleşme yapamazlar.

(6) **(Ek: 23/10/2014-6563/14 md.)** İşletmeciler tarafından, abone ve kullanıcıların iletişim bilgilerinin bir mal ya da hizmetin sağlanması sırasında, bu tür haberleşmenin yapılacağına dair bilgilendirilerek ve reddetme imkânı sağlanarak edinilmiş olması hâlinde, abone ve kullanıcılarla önceden izin alınmaksızın aynı veya benzer mal ya da hizmetlerle ilgili pazarlama, tanıtım, değişiklik ve bakım hizmetleri için haberleşme yapılabilir.

(7) **(Ek: 23/10/2014-6563/14 md.)** Abone ve kullanıcılara, bu tür haberleşme yapılmasını reddetme ve verdikleri izni geri alma hakkı kolay ve ücretsiz bir şekilde sağlanır.

(8) Kurum bu maddenin uygulanmasına ilişkin usul ve esasları belirler. [1]

---

(1) 23/10/2014 tarihli ve 6563 sayılı Kanunun 14 üncü maddesiyle, bu maddeye (6) ve (7) numaralı fıkralar eklenmiş ve diğer fıkra buna göre teselsül ettirilmiştir.

(2) *18/6/2020 tarihli ve 7247 sayılı Kanunun 10 uncu maddesiyle, bu fıkranın üçüncü cümlesinde yer alan "yazılı olarak" ibaresi "taleplerini" şeklinde değiştirilmiştir.*

Kişisel verilerin işlenmesi ve gizliliğin korunması

MADDE 51 – (İptal: Anayasa Mahkemesi'nin 9/4/2014 tarihli ve E.: 2013/122 K.: 2014/74 sayılı Kararı ile.; Yeniden düzenleme: 27/3/2015-6639/32 md.)

(1) Kişisel verilerin işlenmesinde; hukuka ve dürüstlük kurallarına uygun olması, doğru ve gerektiğinde güncel olması, belirli, açık ve meşru amaçlar için işlenmesi, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ile işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi ilkelerine uyulur.

(2) Elektronik haberleşmenin ve ilgili trafik verisinin gizliliği esas olup, ilgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde, haberleşmeye taraf olanların tamamının rızası olmaksızın haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesi yasaktır.

(3) Elektronik haberleşme şebekeleri, haberleşmenin sağlanması dışında abonelerin/kullanıcıların terminal cihazlarında bilgi saklamak veya saklanan bilgilere erişim sağlamak amacıyla işletmeciler tarafından ancak ilgili abonelerin/kullanıcıların verilerin işlenmesi hakkında açık ve kapsamlı olarak bilgilendirilmeleri ve açık rızalarının alınması kaydıyla kullanılabilir.

(4) İşletmeciler şebekelerinin, abonelerine/kullanıcılarına ait kişisel verilerin ve sundukları hizmetlerin güvenliğini sağlamak amacıyla uygun teknik ve idari tedbirleri alır.

(5) Bu Kanunun 49 uncu maddesi kapsamında veya kamu yararının sağlanması amacıyla Kurum tarafından işletmecilere getirilen yükümlülüklerin yerine getirilebilmesi için kişisel veriler işlenebilir.

(6) Kişisel verilerin yurt dışına aktarılmasına ilişkin ilgili mevzuat hükümleri saklı kalmak kaydıyla, trafik ve konum verileri ancak ilgili kişilerin açık rızaları alınmak koşuluyla yurt dışına aktarılabilir.

(7) Trafik verileri; trafiğin yönetimi, arabağlantı, faturalama, usulsüzlük/dolandırıcılık tespitleri ve benzeri işlemleri gerçekleştirmek veya tüketici şikâyetleri ile arabağlantı ve faturalama anlaşmazlıkları başta olmak üzere, uzlaşmazlıkların çözümü amacıyla sadece işletmeci tarafından yetkilendirilen kişilerle sınırlı kalmak kaydıyla işlenir ve bu uzlaşmazlıkların çözüm süreci tamamlanıncaya kadar gizliliği ve bütünlüğü sağlanarak saklanır. Katma değerli elektronik haberleşme hizmetlerinin sunulması ya da elektronik haberleşme hizmetlerinin pazarlanması amacıyla ihtiyaç duyulan trafik verileri ile konum verileri anonim hâle getirilerek veya ilgili abonelerin/kullanıcıların açık rızalarının alınması ve sadece işletmeci tarafından

yetkilendirilen kişilerle sınırlı kalmak kaydıyla, belirtilen faaliyetlerin gerektirdiği ölçü ve sürede işlenebilir.

(8) İşletmeciler konum verilerinin işlenmesinde abonelere/kullanıcılara bu verilerin işlenmesini reddetme imkânı sağlar. İlgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde ancak acil yardım çağrıları ile 29/5/2009 tarihli ve 5902 sayılı Afet ve Acil Durum Yönetimi Başkanlığının Teşkilat ve Görevleri Hakkında Kanunda tanımlanan afet ve acil durum hâllerinde abonelerin/kullanıcıların açık rızası aranmaksızın konum verileri ve ilgili kişilerin kimlik bilgileri işletmeci tarafından yetkilendirilen kişilerle sınırlı olmak kaydıyla işlenebilir.

(9) Abone/kullanıcı şikâyetlerinin incelenmesi ve denetim faaliyetleri kapsamında trafik ve konum verileri ile kişisel veriler, belirtilen faaliyetlerle sınırlı olmak kaydıyla işlenebilir.

(10) Bu Kanun kapsamında sunulan hizmetlere ilişkin olarak;

a) Soruşturma, inceleme, denetleme veya uzlaşmazlığa konu olan kişisel veriler ilgili süreç tamamlanıncaya kadar,

b) Kişisel verilere ve ilişkili diğer sistemlere yapılan erişimlere ilişkin işlem kayıtları iki yıl,

c) Kişisel verilerin işlenmesine yönelik abonelerin/kullanıcıların rızalarını gösteren kayıtlar asgari olarak abonelik süresince,

saklanır. Veri kategorileri ile haberleşmenin yapıldığı tarihten itibaren bir yıldan az ve iki yıldan fazla olmamak üzere verilerin saklanma süreleri yönetmelikle belirlenir.

(11) **(Değişik:17/7/2019-7186/22 md.)** Tahsilata ilişkin riskin yönetilmesi ve kötü niyetli kullanımların önlenmesi amacıyla abonelerin elektronik haberleşme hizmetlerine ve elektronik kimlik bilgisini haiz cihazlara yönelik tarafların kendi sistemlerinde oluşan fatura tutarı ve ödeme bilgileri ile sahtecilik, dolandırıcılık riski içeren şüpheli veya zarar doğurucu vakalara ve işlem hareketlerine ilişkin kayıtlar, işletmeciler ve Kurumun MCKS'si arasında paylaşılabilir veya işlenebilir.

(12) Bu Kanun kapsamında kişisel verilerin gizliliğinin, güvenliğinin ve amacı doğrultusunda kullanılmasının temininden işletmeciler sorumludur.

(13) Bu maddenin uygulanmasına ilişkin usul ve esaslar Kurum tarafından belirlenir.

Hizmet kalitesi

MADDE 52 – (1) Kurum hizmet kalite seviyesine ilişkin olarak tüketici ve son kullanıcıların kapsamlı, yeterli ve anlaşılabilir bilgiye ulaşmasını sağlamak amacıyla, hizmet kalitesinin seviyesine ilişkin ölçütleri, işletmeciler tarafından yayınlanacak bilgilerin içeriğini, şeklini ve hizmet kalite seviyesine ilişkin diğer hususları belirleyebilir.

(2) İşletmeciler, Kurum tarafından elektronik haberleşme hizmetlerinin hizmet kalitesi ölçütlerine ilişkin her türlü bilgiyi ve hizmet kalite standartlarına uyumu istenen şekilde ve belirlenen sürede sağlamakla yükümlüdür. Kurum belirleyeceği usul ve esaslarla işletmeciler tarafından gönderilen hizmet kalitesine ilişkin bilgileri yayımlayabileceği gibi, işletmecilere yayımlama yükümlülüğü de getirebilir. Kurum bilgilerin doğruluğunu ve hizmet kalitesi ölçüt ve standartlarına uyumu denetleyebilir veya denetletebilir.

(3) Kurum işletmecilere, elektronik haberleşme hizmetlerine ve elektronik haberleşme alt yapı veya şebeke unsurlarına yönelik hizmet seviyesi taahhütleri hazırlama ve bu taahhütleri belirlenen biçimde ve sürede yayımlama yükümlülüğü getirebilir. Kurum, işletmecilerden, hizmet seviyesi taahhütlerinde değişiklik, iyileştirme ve düzeltme yapılmasını isteyebilir. İşletmeciler, söz konusu değişiklik, iyileştirme ve düzeltmeleri Kurum tarafından belirtilen sürede yerine getirmekle yükümlüdür.

(4) İşletmeciler, her hal ve şartta doğru faturalama yapma ve fatura içeriği ile ilgili ihtilaf durumunda ispat yükümlülüğündedirler.

(5) Kurum faturaların gönderimi, faturalarda bulunması gereken hususlar, ayrıntılı faturaların düzenlenmesi ile abone tarafından faturaların ödenmemesi halinde hizmetin kesilmesinde uygulanacak işlemleri ve bu maddeye ilişkin usul ve esasları belirler.

BEŞİNCİ KISIM
Onaylanmış Kuruluşlar ve Piyasa Gözetimi

Onaylanmış kuruluşlar, piyasa gözetimi ve denetimi

MADDE 53 – (1) Bu Kanun kapsamındaki cihazların Kurum tarafından yayımlanacak teknik düzenlemelere ve ilgili güvenlik koşullarına uygunluğu, bu konularda üretici ve dağıtıcıların yükümlülüğü, bu cihazların piyasa gözetimi ve denetiminde Kurumun yetki ve sorumluluğu ile Kurum tarafından belirlenecek onaylanmış kuruluşların sorumlulukları hususunda 4703 sayılı Kanunun ilgili hükümleri uygulanır.

(2) Kurum, piyasa gözetimi ve denetimi faaliyetlerinde gerekli gördüğü durumlarda gözetim ve denetime konu cihaza ilişkin uygunluk değerlendirme işlemlerinde yer almayan test, muayene ve/veya belgelendirme kuruluşlarının imkanlarından yararlanabilir; kendi laboratuvar imkanlarını da ücreti mukabili talep edenlerin istifadesine belirleyeceği usul ve esaslarla sunabilir. Ancak, piyasa gözetimi ve denetiminde nihai karar Kuruma aittir. Cihazın güvenli olmadığının tespit edilmesi halinde, test ve muayeneye ilişkin giderler üretici tarafından ödenir.

(3) Elektronik haberleşme cihazları, güvenli hale getirilmesinin imkansız olduğu durumlarda, masraflar üretici tarafından karşılanmak üzere, taşıdıkları risklere göre kısmen ya da tamamen Kurum tarafından bertaraf edilir veya ettirilir.

(4) Onaylanmış kuruluşlar ve piyasa gözetimi ve denetimi ile ilgili usul ve esaslar 4703 sayılı Kanun ve ilgili teknik düzenlemeler çerçevesinde Kurum tarafından belirlenir.

Yetki belgesi

MADDE 54 – (1) Kurum tarafından düzenlenmiş yetki belgesini haiz olmayan gerçek veya tüzel kişiler, ölçüm ve denetim hizmeti veremez.

(2) Bu maddenin uygulanmasına ve yetki belgesi verilmesine ilişkin usuller ile denetim yetki belgesi ücretleri Kurum tarafından düzenlenir.

Elektronik kimlik bilgisini haiz cihazlar

MADDE 55 – (1) Kurum tarafından izin verilmedikçe, abone kimlik ve iletişim bilgilerini taşıyan özel bilgiler veya cihazın teşhisine yarayan elektronik kimlik bilgileri yeniden oluşturulamaz, değiştirilemez, kopyalanarak çoğaltılamaz veya herhangi bir amaçla dağıtılamaz.

(2) Elektronik kimlik bilgisi değiştirilmiş cihaz, kart, araç veya gereçlerle, değişiklik yapılması amacına yönelik yazılım, her türlü araç veya gereçlerin ithalâtı, üretimi, dağıtımı veya tanıtımı yapılamaz, bulundurulamaz, aracılık edilemez.

(3) Elektronik kimlik bilgisi değiştirilmiş cihaz, kart, araç veya gereçlerle, değişiklik yapılması amacıyla kullanılabilen yazılım, her türlü araç veya gereçlere 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununun 127 nci maddesi hükümlerine göre el konulur.

Abone ve cihaz kimlik bilgilerinin güvenliği[1]

MADDE 56 – (1) Abone kimlik ve iletişim bilgilerini taşıyan özel bilgiler ile cihazların elektronik kimlik bilgilerini taşıyan her türlü yazılım, kart, araç veya gereç yetkisiz ve izinsiz olarak kopyalanamaz, muhafaza edilemez, dağıtılamaz, kendisine veya başkasına yarar sağlamak maksadıyla kullanılamaz.

(2) İşletmeci veya adına iş yapan temsilcisine abonelik kaydı sırasında abonelik bilgileri konusunda gerçek dışı belge ve bilgi verilemez.

(3) Abonelik tesisi için gerekli kimlik belgeleri örneği alınmadan işletmeci veya adına iş yapan temsilcisi tarafından abonelik kaydı yapılamaz.

(4) **(Ek: 6/2/2014-6518/104 md.)** Kişinin bilgisi ve rızası dışında işletmeci veya adına iş yapan temsilcisi tarafından abonelik tesisi veya işlemi veya elektronik kimlik bilgisini haiz cihazların kayıt işlemi yapılamaz ve yaptırılamaz, bu amaçla gerçeğe aykırı evrak düzenlenemez, evrakta değişiklik yapılamaz ve bunlar kullanılamaz.

(5) **(Ek: 6/2/2014-6518/104 md.)** Gerçeğe aykırı evrak düzenlemek veya değiştirmek suretiyle kişinin bilgi ve rızası dışında tesis edilmiş olan abonelikler kullanılamaz.

(6) Abonelik tesisine ilişkin usul ve esaslar Kurum tarafından yönetmelikle belirlenir. [1]

Teknik uyumluluk

MADDE 57 – (1) **(Değişik:17/7/2019-7186/23 md.)** İşletmeciler, elektronik kimlik bilgisi değiştirildiği tespit edilen, uluslararası dolaşım hizmetlerine yönelik düzenlemeler ve Kurum düzenlemelerine uymayan elektronik kimlik bilgisini haiz cihazlara, kayıp, kaçak veya çalıntı cihazlara, elektronik haberleşme hizmeti veremezler. Ancak, Kurumun MCKS'sinde kayıtlı iken elektronik kimlik bilgisi kopyalanmış gerçek cihazlar ve mobil haberleşme hizmeti sunan işletmeciler tarafından finansman borcu bulunduğu bildirilen cihazlar borcun devam ettiği süre boyunca sadece eşleştirme yapılan abone numaraları ile kullanılmak üzere kullanıma açılır. İşletmeciler finansman borcu ödenen cihazları, eşleştirme yapılan numara kısıtının kaldırılmasını teminen MCKS'ye bildirir.

(2) İşletmeciler, yukarıdaki fıkrada açıklanan yasal olmayan cihazların haberleşme şebekelerine bağlanılmalarını önlemek üzere MCKT sistemlerini Kurumdaki MCKS ile birlikte uyumlu olarak çalışır hâle getirmek, bununla ilgili teknik alt yapı ve sisteminin güvenliği ve güvenilirliğini sağlamak ve aksamaksızın işletmekle yükümlüdürler.

(3) **(Ek:17/7/2019-7186/23 md.)** Kurumun MCKS'sinde kayıtlı iken kesintisiz yedi yıl süreyle elektronik haberleşme şebekelerinden hizmet almayan cihazların elektronik kimlik bilgileri, kayıtlı olmaktan çıkarılır. Bu yedi yıllık sürenin hesaplanmasında bu maddenin yürürlüğe girdiği tarihten önceki süre de dikkate alınır. Bu suretle elektronik kimlik bilgileri kayıtlı olmaktan çıkarılan cihazların kullanıcılarının, Kurum düzenlemeleri çerçevesinde başvuru yapmaları hâlinde cihazların elektronik kimlik bilgileri tekrar kayıtlı hâle getirilir.

(4) **(Ek:17/7/2019-7186/23 md.)** Bu maddenin uygulanmasına ve cihaza ilişkin borcun ödenmemesi hâlinde cihazların MCKS üzerinden kullanıma kapatılmasına ilişkin usul ve esaslar Kurum tarafından belirlenir.

Bilgi ve ihbar merkezi

MADDE 58 – (1) Kurum, bu Kanunla verilen görevlerin ifasında ihtiyaç duyacağı işler için bilgi ve ihbar merkezi kurabilir. Bu merkezin işletilmesini kendisi yapabileceği gibi üçüncü kişilere de yaptırabilir. Kurum sistemine kayıtlı olan elektronik kimlik bilgisini haiz cihazı çalınan, yağmalanan, kaybeden veya her ne suretle olursa olsun rızası dışında elinden çıkan kişiler cihazının elektronik haberleşme bağlantısının kesilmesi için öncelikle bilgi ve ihbar merkezine başvururlar.

ALTINCI KISIM
Denetim, Kurumun Yetkisi, İdari Yaptırımlar

BİRİNCİ BÖLÜM
Denetim

Denetim

MADDE 59 – (1) Kurum re'sen veya kendisine intikal eden ihbar veya şikayet üzerine, bu Kanunda belirlenen görevleri ile ilgili olarak elektronik haberleşme sektöründe yer alan gerçek ve tüzel kişileri denetleyebilir, denetlettirebilir. Kurum, bu Kanunun kendisine verdiği görevleri yerine getirirken gerekli gördüğü hallerde, mahallinde de inceleme ve denetim yapabilir ve/veya yaptırabilir. Mülki amirler, kolluk kuvvetleri ve diğer kamu kurumlarının amir ve memurları inceleme veya denetimle görevlendirilenlere her türlü kolaylığı göstermek ve yardımda bulunmakla yükümlüdürler. İnceleme veya denetimle görevlendirilenler, inceleme

veya denetime giderken yanlarında denetimin konusunu, amacını ve yanlış bilgi verilmesi halinde idarî para cezası uygulanacağını gösteren bir yetki belgesi bulundururlar.

(1) 6/2/2014 tarihli ve 6518 sayılı Kanunun 104 üncü maddesiyle bu maddeye üçüncü fıkrasından sonra gelmek üzere dördüncü ve beşinci fıkralar eklenmiş ve mevcut dördüncü fıkrası altıncı fıkra olarak teselsül ettirilmiştir.

(2) Denetimle görevlendirilenler, denetime tabi olanlar veya tesisleri nezdinde, defterler de dahil olmak üzere her türlü evrak ve emtianın, elektronik ortamdaki bilgilerin, elektronik haberleşme alt yapısının, cihaz, sistem, yazılım ve donanımlarının incelenmesi, suret veya numune alınması, konuyla ilgili yazılı veya sözlü açıklama istenmesi, gerekli tutanakların düzenlenmesi, tesislerin ve işletiminin incelenmesi konularında yetkilidir. Denetime tabi tutulanlar, denetimle görevli kişilere her türlü kolaylığı göstermek, yukarıda sayılan hususlarla ilgili taleplerini belirlenen süre içinde yerine getirmek, cihaz, sistem, yazılım ve donanımları denetlemeye açık tutmak, denetim için gerekli alt yapıyı temin etmek ve çalışır vaziyette tutmak için gerekli önlemleri almak zorundadır. Aykırı davranışta bulunanlara bu Kanun ve ilgili mevzuat hükümlerine göre cezai işlem uygulanır.

(3) Kurum, bu Kanunun kendisine verdiği görevleri yerine getirirken, bu görevleri ile ilgili gerekli gördüğü bilgi ve belgeyi kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerden isteyebilir. Kurum gerektiğinde diğer kamu kurum ve kuruluşlarından denetim konusunda uzman personel talep edebilir.

(4) Kurum, belirlenecek esaslar dahilinde işletmecileri denetlettirebilir. Denetim yetkisi verilenler ve bağımsız denetim kuruluşları Kuruma sunacakları bilgi, belge, rapor ve mali tabloların bu Kanun ve mevzuat hükümlerine uygunluğu ve hesapların doğruluğundan ve genel kabul görmüş denetim ilke ve esaslarına göre inceleme ve denetiminden sorumludur. Bunlar, hazırladıkları raporlardaki yanlış ve yanıltıcı bilgi ve kanaatler nedeniyle doğabilecek zararlardan ve bu Kanun uyarınca yaptıkları faaliyetler dolayısıyla üçüncü kişilere verecekleri zararlardan sorumludurlar.

(5) Kurumun denetim faaliyetlerinde görevlendirilen personeli ile bu faaliyetlerin yönetim ve koordinasyonunu sağlayan görevlilerine görevleri sona erdiğinde, Kurumca, elektronik haberleşme sektöründe bağımsız denetçilik yapabileceğine ilişkin bir belge düzenlenir. Bunlar, Kurumdaki görevlerinden ayrılmalarını müteakip, 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanununun 48 inci maddesinin (A) bendinin (1), (4), (5) ve (7) numaralı alt bentlerinde belirtilen şartlar ile ceza veya disiplin soruşturması sonucunda memuriyetten çıkarılmış olmamak koşullarını korudukları sürece, elektronik haberleşme sektöründe bağımsız denetçi olarak görev alabilirler.

(6) Bu maddenin uygulanmasına ilişkin usul ve esaslar Kurum tarafından yönetmelikle belirlenir.

İKİNCİ BÖLÜM
Kurumun Yetkisi ve İdari Yaptırımlar

Kurumun yetkisi ve idarî yaptırımlar

MADDE 60 – (1) Kurum; mevzuata, kullanım hakkı ve diğer yetkilendirme şartlarına uyulmasını izleme ve denetlemeye, aykırılık halinde işletmecilere bir önceki takvim yılındaki net satışlarının yüzde üçüne kadar idarî para cezası uygulamaya, millî güvenlik, kamu düzeni veya kamu hizmetinin gereği gibi yürütülmesi ve kanunlarla getirilen hükümlerin uygulanması amaçlarıyla gerekli tedbirleri almaya, gerektiğinde tesisleri tazminat karşılığında devralmaya, belirlediği süre içerisinde yetkilendirme ücretinin ödenmemesi ya da ağır kusur halinde verdiği yetkilendirmeyi iptal etmeye yetkilidir. Ancak, Kurum, ulusal çapta verilecek frekans bandı kullanımını ihtiva eden ve sınırlı sayıda işletmeci tarafından yürütülmesi gereken elektronik haberleşme hizmetlerine ilişkin yetkilendirmelerin iptalini gerektiren hallerde Bakanlığın görüşünü alır.

(2) Kurum, işletmecinin faaliyete yeni başlamış olması halinde, ihlalin niteliği, ihlal neticesinde herhangi bir ekonomik kazanç elde edilip edilmemesi, iyi niyet ve gönüllü bildirim gibi ölçütleri de dikkate alarak önceden belirleyeceği usul ve esaslar çerçevesinde bin liradan bir milyon liraya kadar idarî para cezası ile bu Kanunda belirtilen diğer idarî yaptırımları uygulamaya yetkilidir.

(3) Kurum, kamu hizmetinin gerekleri ve kamu düzeninin korunması amacıyla yönetmelikle önceden belirleyeceği hallerde, işletmecinin faaliyetinin geçici olarak durdurulmasına ya da ihlalin önlenmesi için işletmeciye somut tedbirler uygulama zorunluluğu getirmeye de yetkilidir.

(4) Elektronik haberleşme hizmeti sunan bir işletmeci ile abonelik sözleşmesi yapan gerçek ve tüzel kişiler faaliyetlerinin gereği olarak aldıkları hizmeti üçüncü kişilere ücretli veya ücretsiz verebilir. Aboneler yararlandıkları hizmeti ticaret amacıyla üçüncü kişilere sunamazlar. Aksine davrananların abonelik sözleşmeleri iptal edilir.

(5) Kurumun belirlediği usul ve esaslar çerçevesinde elektronik haberleşme tesisleri ile ilgili bildirimlerin yapılmaması veya güvenlik sertifikası alınmadan kurulması veya Kurum veya Kurum tarafından yetki verilen kuruluşlarca yapılacak ölçümler sonucu Kurum tarafından belirlenen elektromanyetik alan şiddeti limit değere uygun bulunmaması hallerinde, bunların sahibine bu Kanuna ekli ücret tarifesinde belirlenen ruhsatname ücretinin elli katı idarî para cezası her bir cihaz için ayrı ayrı uygulanır. Bu Kanunun 46 ncı maddesinin ikinci fıkrasında telsiz ruhsatnamesi ve yıllık kullanım ücretinden muaf tutulanlar hakkında da bu madde hükümleri uygulanır. Bu fıkradaki idarî para cezaları Kurumun taşra teşkilatı tarafından da verilebilir.

(6) Bu Kanunun 53 üncü maddesinin birinci fıkrasına aykırılık hallerinde, 4703 sayılı Kanunun 12 nci maddesinde dağıtıcı, üretici ve onaylanmış kuruluşlar bakımından öngörülmüş bulunan idarî para cezaları bir katından dört katına kadar artırılarak uygulanır.

(7) Bu Kanunun 57 nci maddesinin birinci fıkrasına aykırı hareket edenlere, cihaz başına onbin liradan yirmibin liraya kadar; ikinci fıkrasına aykırı hareket edenlere onmilyon liraya kadar idarî para cezası verilir.

(8) Bu maddedeki idarî para cezaları Kurum tarafından verilir.

(9) **(Ek: 28/11/2017-7061/99 md.)** İşletmecinin tüketicilerden haksız olarak ücret tahsil ettiğinin tespiti hâlinde, idari yaptırım uygulama hakkı saklı kalmak kaydıyla, işletmeci bu tutarları tüketicilere iade etmekle yükümlüdür. İadeye ilişkin kararın Kurum tarafından işletmeciye tebliğ edildiği tarihten itibaren iki yıl içerisinde işletmecinin tüketiciye ulaşamaması veya Kurum tarafından haklı görülen herhangi bir nedenle işletmeci tarafından iadelerin gerçekleştirilememesi halinde, bu iade bedelleri evrensel hizmet gelirleri olarak genel bütçeye gelir kaydedilmek üzere Bakanlığın merkez muhasebe birimi hesabına yatırılır. Bu fıkranın uygulanmasına ilişkin usul ve esaslar Kurum tarafından belirlenir. [2]

(10) **(Ek: 15/8/2016-KHK-671/25 md.; Aynen kabul: 9/11/2016-6757/22 md.)** Anayasanın 22 nci maddesinde sayılan sebeplerden biri veya birkaçına bağlı olarak, gecikmesinde sakınca bulunan hâllerde Cumhurbaşkanlığı, alınması gereken tedbirleri belirler ve uygulanmak üzere Kuruma bildirir. Kurum Başkanı, Cumhurbaşkanlığının gerekli gördüğü tedbirlere ilişkin kararını derhal işletmecilere, erişim sağlayıcılara, veri merkezlerine ve ilgili içerik ve yer sağlayıcılara bildirir. Bu kararın gereği, derhal ve kararın bildirilmesi anından itibaren en geç iki saat içinde yerine getirilir. Bu karar, yirmidört saat içinde sulh ceza hâkiminin onayına sunulur. Hâkim kararını kırksekiz saat içinde açıklar, aksi halde karar kendiliğinden kalkar.[1][2][3]

(11) **(Ek: 15/8/2016-KHK-671/25 md.; Aynen kabul: 9/11/2016-6757/22 md.)** Kurum, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması ve bu saldırılara karşı caydırıcılık sağlamak için her türlü tedbiri alır veya aldırır. [(1)(2)]

(12) **(Ek: 15/8/2016-KHK-671/25 md.; Aynen kabul: 9/11/2016-6757/22 md.)** Kurum, görevi kapsamında ilgili yerlerden bilgi, belge, veri ve kayıtları alabilir ve değerlendirmesini yapabilir; arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanabilir, bunlarla irtibat kurabilir ve bu kapsamda diğer gerekli önlemleri alabilir veya aldırabilir. Kurum, bu fıkrada belirtilen görevlerin ifasında bakanlıklar, kurum ve kuruluşlar ile işbirliği içerisinde çalışır. Bu kapsamda Kurum tarafından istenen her türlü bilgi ve belge talebi; ilgili bakanlık, kurum ve kuruluşlar tarafından gecikmeksizin yerine getirilir. Bu fıkraya göre bilgi ve belge talebinde bulunulması ve bu taleplerin yerine getirilmesine ilişkin usul ve esaslar ile diğer hususlar Cumhurbaşkanlığınca belirlenir.[(1)(2)(3)]

(13) **(Ek: 15/8/2016-KHK-671/25 md.; Aynen kabul: 9/11/2016-6757/22 md.)** Gerçek kişiler ile özel hukuk tüzel kişileri, Kurumun bu maddedeki görevleri ile ilgili taleplerini, tabi oldukları mevzuat hükümlerini gerekçe göstermek suretiyle yerine getirmekten kaçınamazlar. İşletmeciler dışında Kurumun görevleri ile ilgili yükümlülüklerini yerine getirmeyenlere bu maddenin ikinci fıkrasındaki yaptırım uygulanır.[(1)(2)]

(14) **(Ek: 28/11/2017-7061/99 md.)** Eksik ödenen Kurum alacaklarının hesaplanmasında, işletmecilerce fazla ödendiği tespit edilen tutarlar, ödendikleri tarih esas alınarak mahsup edildikten sonra kalan tutar dikkate alınır. Bu takdirde mahsup suretiyle tahsil edilen Kurum alacağı, vadesinden sonra tahsil edilmişse tahsil tarihine kadar gecikme zammı uygulanır. [(2)]

(15) Bu maddenin uygulanmasına ve bu Kanunda öngörülen yükümlülüklerin işletmeciler tarafından yerine getirilmemesi halinde uygulanacak idarî para cezalarına ilişkin hususlar Kurum tarafından çıkarılacak yönetmelikle düzenlenir.[(1)(2)]

---

(1) 15/8/2016 tarihli ve 671 sayılı KHK'nin 25 inci maddesiyle sekizinci fıkradan sonra gelmek üzere "9,10,11,12" numaralı fıkralar eklenmiş ve sonraki mevcut fıkra 13 olarak teselsül ettirilmiş olup, daha sonra bu hüküm 9/11/2016 tarihli ve 6757 sayılı Kanunun 22 nci maddesiyle aynen kabul edilerek kanunlaşmıştır.

(2) 28/11/2017 tarihli ve 7061 sayılı Kanunun 99 uncu maddesiyle, mevcut sekizinci fıkrası ile onikinci fıkradan sonra gelmek üzere (9) ve (13) numaralı fıkralar eklenmiş ve mevcut fıkralar buna göre teselsül ettirilmiştir.

(3) 2/7/2018 tarihli ve 703 sayılı Kanun Hükmünde Kararnamenin 205 inci maddesiyle 60 ıncı maddenin onuncu fıkrasında yer alan "Başbakanlık" ibaresi "Cumhurbaşkanlığı" şeklinde, "Başbakanlığın" ibaresi "Cumhurbaşkanlığının" şeklinde ve onikinci fıkrasında yer alan "Başbakanlıkça" ibaresi "Cumhurbaşkanlığınca" şeklinde değiştirilmiştir.

İdarî para cezalarının uygulanması ve tahsili

MADDE 61 – (1) Kurum tarafından verilen idarî para cezaları, 6183 sayılı Kanun hükümlerine tabi olup, tebliğ tarihinden itibaren otuz gün içerisinde Kurum hesaplarına ödenir. Bu süre içerisinde ödenmeyen idarî para cezaları, Kurumun bildirimi üzerine ilgili vergi dairesince 6183 sayılı Kanun hükümlerine göre tahsil olunur. **(Mülga üçüncü cümle: 2/7/2012-6352/105 md.) (…)**

(2) Tahsil olan idarî para cezalarının tamamı Kurum hesaplarına aktarılır.

Dava hakkı

MADDE 62 –(1) **(Değişik: 2/7/2012-6352/70 md.)** İdarî yaptırım kararlarına karşı yetkili idare mahkemesinde dava açılabilir. Kurum kararlarına karşı açılan her türlü dava öncelikli işlerden sayılır. Kurulun kararları, Kurumun idarî denetimi sırasında yerindelik denetimine tabi tutulamaz.

(2) Kurum tarafından açılacak davalarda teminat aranmaz.

YEDİNCİ KISIM
Cezai Hükümler

Cezai hükümler

MADDE 63 – (1) Bu Kanunun 9 uncu maddesine aykırı olarak Kuruma bildirimde bulunmaksızın elektronik haberleşme hizmeti verenler ve/veya tesisleri kuranlar ve/veya işletenler hakkında bin günden on bin güne kadar adli para cezasına hükmolunur.

(2) Bu Kanunun 9 uncu maddesine aykırı olarak kullanım hakkı olmadan elektronik haberleşme hizmeti verenler, tesisi kuranlar ve/veya işletenler hakkında altı aya kadar hapis ve beş bin günden on beş bin güne kadar adli para cezasına hükmolunur.

(3) Elektronik haberleşme hizmeti vermek üzere yetkilendirilmiş bulunan işletmecilerin personelinin, 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun İkinci Kitabının İkinci Kısmının Dokuzuncu Bölümünde düzenlenen, özel hayata ve hayatın gizli alanına karşı suçları işlemesi halinde haklarında bu bölümde öngörülen cezalara hükmolunur. Ancak 137 nci maddeye göre yapılacak artırım bir kat olarak uygulanır.

(4) Kurma ve kullanma izni ile ruhsatname alınması gereken telsiz cihazı veya sistemlerini bu Kanunun 37 nci maddesine aykırı olarak, Kurumdan izin almaksızın satan, kuran, işleten ve kullananlar hakkında ikibin güne kadar adlî para cezası uygulanır. Bu cihazları, gerekli izinler alınmış olsa bile millî güvenliği ihlal amacıyla kullananlar eylemleri daha ağır cezayı gerektiren bir suç oluşturmadığı takdirde altı aydan bir yıla kadar hapis ve on bin güne kadar adli para cezası ile cezalandırılırlar.

(5) Kurum tarafından yetkilendirilen, izin verilen ve tahsis yapılan kişiler tarafından;

a) Telsiz sistemlerinin Kurumun düzenlemelerine ve verilen telsiz ruhsatnamesine uygun olmayan bir şekilde kurulması, işletilmesi, fiziki yerinin, frekansının ve diğer teknik özelliklerinin değiştirilerek amacı dışında kullanılması halinde aykırılığın giderilmesi için gerekli tedbirlerin Kurum tarafından belirlenecek sürede alınmaması,

b) Telsiz sistemlerinin Kurum düzenlemeleri ile belirlenen tekniklere ve usullere uygun olarak çalıştırılmaması sonucu her ne suretle olursa olsun diğer elektronik haberleşme sistemleri üzerinde elektromanyetik girişim veya diğer her türlü bozucu etkiye sebebiyet verildiğinin tespiti üzerine söz konusu elektromanyetik girişim veya bozucu etkilerin giderilmesi için gerekli tedbirlerin Kurum tarafından belirlenecek sürede alınmaması,

hallerinde, yüz günden az olmamak üzere adlî para cezası uygulanır.

(6) Bu Kanunun 39 uncu maddesine aykırı olarak kodlu ve kriptolu haberleşme yapan ve yaptıranlar beş yüz günden bin güne kadar adli para cezası ile cezalandırılır.

(7) Bu Kanunun 53 üncü maddesinin üçüncü fıkrasına aykırı olarak Kurum tarafından bertaraf ettirilmek üzere üretici, dağıtıcı veya kullanıcısına teslim edilen cihazların piyasaya arz edildiği veya kullanıldığının tespiti halinde sorumluları hakkında bin günden beş bin güne kadar adli para cezası verilir.

(8) Bu Kanunun 54 üncü maddesine aykırı hareket edenler hakkında beş bin güne kadar adli para cezası uygulanır.

(9) Bu Kanunun 55 inci maddesinin birinci ve ikinci fıkralarına aykırı hareket edenler hakkında bin günden on beş bin güne kadar adlî para cezasına hükmolunur.

(10) Bu Kanunun 56 ncı maddesinin birinci fıkrası hükümlerine aykırı hareket edenler bin günden beş bin güne kadar; ikinci, üçüncü, dördüncü ve beşinci fıkralarına aykırı hareket ederek bu işi bizzat yapanlar elli günden yüz güne kadar adli para cezası ile cezalandırılır.[1]

(11) Bu maddede tanımlanan suçların bir örgütün faaliyeti çerçevesinde işlenmesi halinde, verilecek cezalar yarısı oranında artırılır. Bu faaliyette bulunan tüzel kişi ise, hakkında 5237 sayılı Kanundaki bunlara özgü güvenlik tedbirlerine de hükmolunur.

SEKİZİNCİ KISIM
Son Hükümler

Tebligat

MADDE 64 – (1) Bu Kanun uyarınca Bakanlık ve Kurum tarafından ilgililere yapılacak tebliğler 11/2/1959 tarihli ve 7201 sayılı Tebligat Kanunu hükümlerine göre yapılır.

Atıflar ve uygulama

MADDE 65 – (1) Diğer mevzuatta, hizmet alanları itibariyle, 4/2/1924 tarihli ve 406 sayılı Telgraf ve Telefon Kanunu ve 5/4/1983 tarihli ve 2813 sayılı Telsiz Kanununa yapılan atıflar ile bu kanunların kendi içinde yapılan atıflar, konuları itibariyle bu Kanuna yapılmış sayılır.

(2) Diğer kanunların bu Kanuna aykırı hükümleri uygulanmaz.

(3) Diğer mevzuatta geçen "Telekomünikasyon Kurumu" ibaresinden "Kurum"; "Telekomünikasyon Kurulu" ibaresinden de "Kurul" anlaşılır.

Yürürlükten kaldırılan hükümler

MADDE 66 – (1) 406 sayılı Kanunun 1 inci maddesinin birinci fıkrası, yedinci fıkrası ve dokuzuncu fıkrasının ilk cümlesi; ek 17 nci, ek 19 uncu, ek 21 inci, ek 22 nci, ek 23 üncü, ek 24 üncü, ek 28 inci, ek 29 uncu, ek 30 uncu maddeleri; ek 32 nci maddesinin dördüncü ve altıncı fıkraları; ek 33 üncü maddesi; ek 35 inci maddesinin ikinci fıkrası; ek 36 ncı, ek 37 nci, geçici 3 üncü, 35 inci ve 36 ncı maddeleri dışındaki madde ve hükümleri ek ve değişiklikleriyle birlikte yürürlükten kaldırılmıştır.

(2) 2813 sayılı Kanunun 5 inci ve 8 inci maddeleri; ek 2 nci maddesinin birinci, ikinci, üçüncü ve beşinci fıkraları; 35 inci ve 36 ncı maddeleri dışındaki diğer hükümleri ek ve değişiklikleriyle birlikte yürürlükten kaldırılmıştır.

---

(1) 6/2/2014 tarihli ve 6518 sayılı Kanunun 105 inci maddesi ile bu fıkrada yer alan "ikinci fıkrası hükümlerine aykırı hareket edenler yirmi günden yüz güne kadar; üçüncü fıkrası hükümlerine aykırı hareket edenler yüz günden beş yüz güne kadar" ibaresi "ikinci, üçüncü, dördüncü ve beşinci fıkralarına aykırı hareket ederek bu işi bizzat yapanlar elli günden yüz güne kadar" şeklinde değiştirilmiştir.

(3) 27/1/2000 tarihli ve 4502 sayılı Telgraf ve Telefon Kanunu, Ulaştırma Bakanlığının Teşkilat ve Görevleri Hakkında Kanun, Telsiz Kanunu ve Posta, Telgraf ve Telefon İdaresinin Biriktirme ve Yardım Sandığı Hakkında Kanun ile Genel Kadro ve Usulü Hakkında Kanun Hükmünde Kararnamenin Eki Cetvellerde Değişiklik Yapılmasına Dair Kanunun 26 ncı, geçici 1 inci, geçici 5 inci, geçici 6 ncı, geçici 7 nci, geçici 8 inci maddeleri yürürlükten kaldırılmıştır.

(4) 12/5/2001 tarihli ve 4673 sayılı Telgraf ve Telefon Kanunu, Posta, Telgraf ve Telefon İdaresinin Biriktirme ve Yardım Sandığı Hakkında Kanun ile Ulaştırma Bakanlığının Teşkilat ve Görevleri Hakkında Kanunda Değişiklik Yapılması Hakkında Kanunun geçici 1 inci, geçici 2 nci, geçici 4 üncü maddeleri yürürlükten kaldırılmıştır.

Değiştirilen hükümler

MADDE 67 – (1) (4/2/1924 tarihli ve 406 sayılı Kanun ile ilgili olup yerine işlenmiştir.)

(2) (5/4/1983 tarihli ve 2813 sayılı Kanun ile ilgili olup yerine işlenmiştir.)
(3) (9/4/1987 tarihli ve 3348 sayılı Kanun ile ilgili olup yerine işlenmiştir.)
(4) (9/4/1987 tarihli ve 3348 sayılı Kanun ile ilgili olup yerine işlenmiştir.)
(5) (14/7/1965 tarihli ve 657 sayılı Kanun ile ilgili olup yerine işlenmiştir.)
(6) (16/6/2005 tarihli ve 5369 sayılı Kanun ile ilgili olup yerine işlenmiştir.)
(7) (4/5/2007 tarihli ve 5651 sayılı Kanun ile ilgili olup yerine işlenmiştir.)

Siber Güvenlik Kurulu

EK MADDE 1 – (Ek: 6/2/2014-6518/106 md.)

(1) **(Mülga fıkra: 2/7/2018-KHK-703/205 md.)**

(2) Kurulun görevleri şunlardır:

a) Siber güvenlik ile ilgili politika, strateji ve eylem planlarını onaylamak ve ülke çapında etkin şekilde uygulanmasına yönelik gerekli kararları almak.

b) Kritik altyapıların belirlenmesine ilişkin teklifleri karara bağlamak.

c) Siber güvenlikle ilgili hükümlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşları belirlemek.

Ç) Kanunlarla verilen diğer görevleri yapmak.

(3) **(Mülga fıkra: 2/7/2018-KHK-703/205 md.)**

EK MADDE 2- (Ek: 2/7/2018-KHK-703/205 md.)

(1) Mevzuatta Siber Güvenlik Kuruluna yapılmış olan atıflar, Cumhurbaşkanınca belirlenen kurul veya mercie yapılmış sayılır.

Uygulama

GEÇİCİ MADDE 1 – (1) Bu Kanunda öngörülen düzenlemelerin yürürlüğe gireceği tarihe kadar mevcut düzenlemelerin bu Kanuna aykırı olmayan hükümlerinin uygulanmasına devam edilir. Kurum, bu Kanunun İkinci Kısım Birinci Bölümünde yer alan yetkilendirme ile ilgili hükümler yürürlüğe girinceye kadar mevcut mevzuat uyarınca yetkilendirme yapabilir. Bu Kanunun yürürlüğe girdiği tarihe kadar, işletmecilerin ilgili mevzuatına uygun olarak sahip oldukları geçiş hakları devam eder.

(2) Bu Kanunun yürürlüğe girmesinden önce Kurum tarafından verilmiş ancak henüz tahsili gerçekleşmemiş olan idarî para cezaları hakkında da 61 inci madde hükmü uygulanır.

Yetkilendirmede geçiş süreci

GEÇİCİ MADDE 2 – (1) Bu Kanunun yürürlüğe girdiği tarihten önce telekomünikasyon ruhsatı veya genel izin ile yetkilendirilmiş olan işletmeciler, bu Kanun uyarınca Kuruma bildirimde bulunmuş veya gerekli olduğu durumlarda yetkilendirmelerindeki süre ile sınırlı olarak kullanım hakkı almış sayılırlar.

(2) Bu Kanunun yürürlüğe girdiği tarihten önce Kurumla imzalanmış olan görev ve imtiyaz sözleşmeleri; süre bitimi, fesih, iptal veya başkaca herhangi bir nedenle sona ermelerine kadar mevcut hükümleri uyarınca geçerliliklerini devam ettirirler. 406 sayılı Kanunun 1 inci maddesinin son fıkrasında yer alan tanımlar ilgili olduğu sözleşmenin konusu itibariyle bu fıkra uygulamasında geçerliliklerini sürdürürler.

(3) Bu Kanunun yürürlüğe girdiği tarihten önce yetkilendirmeye tabi olmayan elektronik haberleşme hizmetleri için Kurum tarafından sistem kurma ve kullanma izni verilmiş olan kullanıcıların kaynak kullanım hakları devam eder.

Telsiz ruhsatlarının yenilenmesi

GEÇİCİ MADDE 3 – (1) Özel kanunlarının verdiği yetkiye göre telsiz cihaz ve sistemleri kullanan kamu kurum ve kuruluşları hariç, bu Kanunun yürürlüğe girmesinden önce, telsiz cihaz ve sistemleri kullanan diğer kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler bu Kanunun 37 nci maddesinde belirtilen yönetmeliğin yayımı tarihinden itibaren altı ay içinde gerekli belgelerle birlikte Kuruma başvurarak durumlarını bu Kanun hükümlerine uygun hale getirirler.

(2) Kurum, söz konusu kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin durumlarını inceleyerek uygun olanların telsiz ruhsatnamelerini yeniler. Uygun olmayanların ve süresi içinde başvuru yapmayanların telsiz ruhsatnamelerini iptal eder.

(3) 2813 sayılı Kanun çerçevesinde telsiz kullanım ve ruhsatname ücretlerinin tahsili ile ilgili olarak yetkilendirmeleri ve özel protokolleri uyarınca işletmecilere getirilmiş olan tahsil ve Kuruma ödeme yükümlülüğü çerçevesinde tahakkuk ettirilmiş olanlar dışında, bu Kanunun yürürlüğe girmesinden önce 2813 sayılı Kanunun uygulamasından doğan ve her ne sebeple olursa olsun tahsil edilmemiş veya tahsili mümkün olmayan, miktarı ne olursa olsun genel bütçeye dahil daireler, katma bütçeli idareler, il özel idareleri, belediyeler ve köy tüzel kişilikleri tarafından kullanılan her türlü telsiz tesis ve sistemlerindeki cihazlar için tahakkuk ettirilmiş alacaklar ile yargı kararı ile kesinleşenler hariç gerçek ve tüzel kişiler tarafından kullanılan her türlü telsiz tesis ve sistemlerindeki cihazlar için tahakkuk ettirilmiş yüzelli lira ve altında kalan Kurum alacakları ve bunların fer'ilerinin tahsilinden herhangi bir işleme gerek kalmaksızın vazgeçilmiş sayılır. Bunlara ilişkin açılmış olan davalar ve yapılmış olan takipler iptal edilir.

Görev sözleşmeleri ve devir

GEÇİCİ MADDE 4 – (1) Kurum ile Kıyı Emniyeti Genel Müdürlüğü arasında imzalanmış bulunan görev sözleşmesi herhangi bir işleme gerek kalmaksızın iptal edilmiş sayılır ve bu görev sözleşmesindeki hizmetler ile bu Kanunla Telsiz İşletme Müdürlüğüne verilen görevler herhangi bir yetkilendirmeye tabi olmaksızın yürütülmeye devam eder. Kıyı Emniyeti Genel Müdürlüğü, 5369 sayılı Kanun kapsamında evrensel hizmet yükümlüsü bir işletmeci olarak sayılmaya devam eder.

(2) Bu Kanunun 42 nci ve 43 üncü maddeleriyle Telsiz İşletme Müdürlüğüne devredilen görev ve işlere ilişkin Kurumun tüm hak, alacak ve borçları, sözleşme, taahhüt ve yükümlülükleri, leh ve aleyhe açılmış ve açılacak olan dava ve icra takipleri, bu maddenin yürürlüğe girdiği tarihten itibaren altı ay içerisinde Kıyı Emniyeti Genel Müdürlüğü ile Kurum arasında yapılacak protokoller ile Telsiz İşletme Müdürlüğüne devredilir. Bu devre ilişkin bütün devir, temlik ve intikal işlemleri ve bu işlemlerle ilgili olarak düzenlenecek her türlü sözleşme, protokol ve kağıtlar, katma değer vergisi ve damga vergisi dahil her türlü vergi, resim, harç ve benzeri mali yükümlülüklerden istisnadır.

Abonelik kayıtlarının güncellenmesi

GEÇİCİ MADDE 5 – (1) GSM mobil telefon hizmeti sunan işletmeciler nezdinde tutulan abonelik kayıtlarının tam, doğru ve güncel bilgilerden oluşmasını teminen, tüm abonelik kayıtları bu Kanunun yayımından itibaren bir yıl içinde güncellenir. Bu kapsamda ilgili işletmeciler nezdindeki bilgi ve belgelerinde eksiklik ve yanlışlıkları bulunan tüm aboneler, bu süre içerisinde kimliklerini ispatlayıcı belgelerle birlikte ilgili işletmeciye başvururlar. Başvuru esnasında abonelerden kimliklerini ispata yarar belgelerin birer örneği ile birlikte bireysel abonelerden Türkiye Cumhuriyeti kimlik numaraları, kurumsal abonelerden ise vergi numaraları alınır. Bu madde kapsamında bilgileri güncellenemeyen hatların elektronik haberleşme şebekesi ile bağlantısı kesilir.

(2) Bu Kanunda tanımlanan son kullanıcılar, kullanmakta oldukları hatları, bir kereye mahsus olmak üzere verilen süre içerisinde, hiçbir vergi, resim, harç ve benzeri mali yükümlülüğe tabi olmaksızın kendi üzerlerine kaydettirmek için ilgili işletmeciyle abonelik sözleşmesi akdedebilir. Söz konusu hatların eski abonelerinin yapılan işleme bir yıllık zamanaşımı süresi içinde itiraz hakları saklıdır.

(3) Bu maddenin uygulanmasına ilişkin düzenlemeler Kurum tarafından yapılır.

Elektronik kimlik bilgisi değiştirilen ve borcu bulunan cihazlar

GEÇİCİ MADDE 6 – (Ek:17/7/2019-7186/24 md.)

(1) Kurumun MCKS'sinde kayıtlı olmakla birlikte bu maddenin yürürlüğe girdiği tarihten önce elektronik kimlik bilgisi değiştirilmiş olan cihazlar ile Kurumun uluslararası dolaşım hizmetleri çerçevesinde yaptığı düzenlemelere uymayan cihazlara elektronik haberleşme hizmeti verilmesi dört ay içinde engellenir. Bu cihazların kullanıcılarının, bu maddenin yürürlüğe girdiği tarihten itibaren bir yıl içinde Kurum düzenlemeleri çerçevesinde başvuru yaparak iki yüz elli Türk lirası tutarındaki kayıt ücretini genel bütçeye gelir kaydedilmek üzere Hazine ve Maliye Bakanlığı muhasebe birimi hesabına yatırmaları hâlinde, cihazların elektronik kimlik bilgisi ilgili abonenin numaraları ile eşleştirilerek kullanılabilir.

(2) Bu maddeyi ihdas eden Kanunla, bu Kanunun 57 nci maddesinin birinci fıkrasında yapılan değişiklik uyarınca finansman borcu bulunduğu bildirilen cihazların kısıtlanmasına ilişkin hüküm, bu maddenin yürürlük tarihinden sonraki iş ve işlemlere uygulanır.

Yürürlük

MADDE 68 – (1) Bu Kanunun İkinci Kısım Birinci Bölümünde yer alan yetkilendirme ile ilgili hükümler Kanunun yayımından altı ay sonra, diğer hükümleri yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 69 – (1) Bu Kanun hükümlerini Bakanlar Kurulu yürütür.

TÜRKİYE CUMHURİYETİ CUMHURBAŞKANLIĞI
DİJİTAL DÖNÜŞÜM OFİSİ

BİLGİ ve İLETİŞİM GÜVENLİĞİ REHBERİ

TEMMUZ 2020

SUNUŞ

Günümüz dünyasında dijital teknolojilerin baş döndürücü bir hızla gelişimi, ekonomik ve sosyal hayatın yanında güvenlik tanım ve kavramlarını da etkileyerek geleceğe dönük güvenlik bakış açılarını kökten değiştirmiştir.

Toplumların hayatına yön verebilme potansiyeli bulunan verinin dijital ortama taşınmasıyla, siber tehdit ve saldırıların doğası da değişmiştir. Geçmişte daha sade yöntemler, basit amaçlar ve belirli yetkinlikte kişiler tarafından gerçekleştirilen siber saldırılar artık devletler düzeyinde, otomatize edilmiş, daha sık, karmaşık, yıkıcı, tespiti zor ve hedef odaklı olmaya başlamıştır. Son dönemde yaşanan hadiseler, ülkenin sınırlarını korumak kadar ülkenin verisinin ve dijital altyapılarının korunmasının önemini bize göstermiştir.

Şüphesiz dünyanın hiçbir yerinde bu alanda yüzde yüz güvenlikten bahsetmek mümkün değildir. Ancak insan, teknoloji, organizasyon yapısı, yasal düzenleme ile ulusal ve uluslararası işbirliği boyutlarının her birinde atılacak doğru ve bilinçli adımlarla yıkıcı etkilerden korunmak mümkündür. Bilgi sistemlerinde karşılaşılan güvenlik risklerinin azaltılması, etkisiz kılınması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik türdeki verilerin güvenliğinin sağlanması amacıyla, kamu kurumları ve kritik altyapı hizmeti veren işletmelerce uyulması gereken Bilgi ve İletişim Güvenliği tedbirlerini içeren, 06.07.2019 tarih ve 30823 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren 2019/12 sayılı Cumhurbaşkanlığı Genelgesi yasal düzenleme boyutunda ülke çapında bilgi güvenliği seviyesini artırmaya yönelik önemli bir adım olmuştur.

Genelgenin yürürlüğe girmesini müteakiben, Dijital Dönüşüm Ofisi Başkanlığı koordinasyonunda, Bilgi ve İletişim Güvenliği Rehberi hazırlama çalışmaları başlatılmıştır. Yaklaşık 1 yıl süren çalışmalar kapsamında; 5 günlük bir çalıştay gerçekleştirilmiş, 16 Bakanlık ile 51 Kurum ve Kuruluştan 240 uzmanın katkısı alınmış, 200 saati aşan 70'in üzerinde çalışma toplantısında 2660 görüş ve öneri değerlendirilmiş, ulusal ve uluslararası yayınlar incelenmiştir.

Bilgi ve iletişim güvenliği alanında ülkemize özgün ilk referans doküman olma niteliği taşıyan ve geniş bir katılımla ilgili tüm paydaşların katkısı alınarak hazırlanan Bilgi ve İletişim Güvenliği Rehberi; ihtiyaçlar, gelişen teknoloji, değişen şartlar ile ulusal politika ve stratejiler göz önünde bulundurularak güncellenmeye devam edecektir.

Güçlü ekonomiler için güçlü teknolojilerin önem kazandığı çağımızda bugünden atacağımız adımlar ve alacağımız önlemler yarının dünyasında teknolojiyi takip eden değil teknolojiye yön veren bir ülke olabilmemiz için oldukça önemlidir. Bu bağlamda Rehber, yerli ve milli siber güvenlik ürün ve çözümlerinin kullanımının yaygınlaştırılmasını sağlayarak üretim gücümüze destek olacak, siber güvenlik alanında dünya ile rekabet edebilecek teknoloji üretebilmenin önünü açacaktır.

Rehber, bilgi ve iletişim güvenliği alanındaki büyük bir boşluğu doldurmakla birlikte, siber saldırılara karşı mukavemetimizi artıracak, bilgi güvenliği ve siber güvenlikte ülke seviyesinin uluslararası arenada yükselmesinde önemli bir rol alacaktır. Bunula birlikte ulusal verimizin güvenliğine, kritik altyapı ve sistemlerimizin sürdürülebilirliğine katkı sağlayacak, milli güvenlik stratejilerimiz ve hedeflerimizi gerçekleştirmek için doğru adımlarla yol almamızı sağlayacaktır.

Dr. Ali Taha KOÇ
Dijital Dönüşüm Ofisi Başkanı

KISALTMALAR

Kısaltma	Açıklama
API	Application Programming Interface / Uygulama Programlama Arayüzü
ASLR	Address Space Layout Randomization / Adres Alanı Düzeni Rastgele Seçimi
BDDK	Bankacılık Düzenleme ve Denetleme Kurumu
BT	Bilgi Teknolojisi
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CAPTCHA	Completely Automated Public Turing Test to Tell Computers and Humans Apart / İnsan ve Bilgisayar Ayrımı Amaçlı Tam Otomatik Genel Turing Test
COMSEC	Communication Security / Haberleşme Güvenliği
CORS	Cross-Origin Resource Sharing / Kökler Arası Kaynak Paylaşımı
CSRF	Cross-Site Request Forgery / Siteler Arası İstek Sahteciliği
DEP	Data Execution Prevention / Veri Yürütme Engellemesi
DDO	Cumhurbaşkanlığı Dijital Dönüşüm Ofisi
DHCP	Dynamic Host Configuration Protocol / Dinamik Bilgisayar Yapılandırma Protokolü
DKIM	Domain Keys Identified Mail / Alan Adı Anahtarıyla Tanımlanmış E-Posta
DMZ	Demilitarized Zone / Sivil Bölge
DNS	Domain Name System / Alan Adı Sistemi
DoS	Denial of Service / Hizmet Engelleme
DDoS	Distributed Denial of Service / Dağıtık Hizmet Engelleme
EAP	Extensible Authentication Protocol / Genişletilebilir Kimlik Doğrulama Protokolü
EBYS	Elektronik Belge Yönetim Sistemi
EKS	Endüstriyel Kontrol Sistemi
EPDK	Enerji Piyasası Düzenleme Kurumu
FTP	File Transfer Protocol / Dosya Transfer Protokolü
G2B	Government to Business / Devletten Kuruma
G2G	Government to Government / Devletten Devlete
GPS	Global Positioning System / Küresel Konumlama Sistemi
HDD	Hard Disk Drive / Sabit Disk Sürücüsü
HIDS	Host Intrusion Detection System / Bilgisayar Tabanlı Saldırı Tespit Sistemi
HIPS	Host Intrusion Prevention System / Bilgisayar Tabanlı Saldırı Önleme Sistemi
HMI	Human Machine Interface / Makine ile İnsan Arasında Bilgi Aktarımı Sağlayan Arayüz
HSTS	HTTP Strict Transport Security / HTTP Sıkı Aktarım Güvenliği
HSM	Hardware Security Module / Donanımsal Güvenlik Modülü
HTML	Hypertext Markup Language / Standart Metin İşaretleme Dili
HTTP	Hypertext Transfer Protocol / Bağlantılı Metin Aktarım Protokolü
HTTPS	Hypertext Transfer Protocol Secure / Güvenli Bağlantılı Metin Aktarım Protokolü
IEC	International Electrotechnical Commission / Uluslararası Elektroteknik Komisyonu
IED	Intelligent Electronic Device / Akıllı Elektronik Cihaz
IMAPs	Internet Message Access Protocol Secure / Güvenli İnternet Mesaj Erişim Protokolü
IoT	Internet of Things / Nesnelerin İnterneti
IP	Internet Protocol / İnternet Protokolü
IPS	Intrusion Prevention System / Saldırı Önleme Sistemi
IPSec	IP Security / İnternet Protokolü Güvenliği
ISO	International Organization for Standardization / Uluslararası Standartlar Örgütü
LAN	Local Area Network / Yerel Ağ Bağlantısı
LDAP	Lightweight Directory Access Protocol / Hafif Dizin Erişim Protokolü
LUN	Logical Unit Number / Mantıksal Birim Numarası
MAC	Media Access Control Address / Ortam Erişim Kontrol Adresi
MMS	Manufacturing Message Specification / Üretim Mesaj Spesifikasyonu

Kısaltma	Açıklama
NAC	Network Access Control / Ağ Erişim Kontrolü
NES	Nitelikli Elektronik Sertifika
NFC	Near Field Communication / Yakın Alan İletişimi
NTP	Network Time Protocol / Ağ Zaman Protokolü
OCSP	Online Certificate Status Protocol / Çevrimiçi Sertifika Durum Protokolü
OT	Operasyonel Teknolojiler
PCMCIA	Personal Computer Memory Card International Association / Kişisel Bilgisayar Bellek Kartı Uluslararası Birliği
PLC	Programmable Logic Controller / Programlanabilir Mantıksal Denetleyici
PoC	Proof of Concept / Demo ve Kavram İspatı
POP3	Post Office Protocol / Posta İleti Protokolü
PRNG	Pseudo Random Numerator Generator / Varsayımsal Rastsal Sayı Üreteci
SAM	Sorumluluk Atama Matrisi
REST	Representational State Transfer / Temsili Durum Transferi
RTU	Remote Terminal Unit / Uzak Terminal Ünitesi
SAN	Storage Area Network / Depolama Alanı Ağı
SCADA	Supervisory Control And Data Acquisition / Merkezi Kontrol ve Veri Toplama
SCAP	Security Content Automation Protocol / Güvenlik İçeriği Otomasyon Protokolü
SFTP	Secure File Transfer Protocol / Güvenli Dosya Transfer Protokolü
SMB	Server Message Block / Sunucu İleti Bloğu
SMS	Short Message Service / Kısa Mesaj Hizmeti
SMTP	Simple Mail Transfer Protocol / Basit Posta Aktarım Protokolü
SMTPS	Secure Simple Mail Transfer Protocol / Güvenli Basit Posta Aktarım Protokolü
SOME	Siber Olaylara Müdahale Ekibi
SPF	Sender Policy Framework / Gönderen Politika Çerçevesi
SPK	Sermaye Piyasası Kurulu
SQL	Structured Query Language / Yapısal Sorgulama Dili
SSD	Solid State Disk / Katı Hal Sürücüsü
SSH	Secure Shell / Güvenli Kabuk
SSL	Secure Sockets Layer / Güvenli Soket Katmanı
TCP	Transmission Control Protocol / Gönderi Kontrol Protokolü
TEE	Trusted Execution Environment / Güvenilir İşletim Ortamı
TEMPEST	Telecommunications Electronics Material Protected from Emanating Spurious Transmissions / Elektromanyetik İletimlerin Yayılımından Korunan Telekomünikasyon Elektronik Malzemesi
TLS	Transport Layer Security / Taşıma Katmanı Güvenliği
TRNG	True Random Number Generator / Gerçek Rassal Sayı Üreteci
TRSM	Tamper Resistant Security Module / Kurcalamaya Dayanıklı Güvenlik Modülü
TS	Türk Standardı
UDP	User Datagram Protocol / Kullanıcı Veri Bloğu Protokolü
UPS	Uninterruptible Power Supply / Kesintisiz Güç Kaynağı
URL	Uniform Resource Locator / Tek Düzen Kaynak Konum Belirleyicisi
USB	Universal Serial Bus / Evrensel Seri Veri Yolu
USOM	Ulusal Siber Olaylara Müdahale Merkezi
VLAN	Virtual Local Area Network / Sanal Yerel Alan Ağı
VPN	Virtual Private Network / Sanal Özel Ağ
WAF	Web Application Firewall / Uygulama Güvenlik Duvarı
WebDAV	Web Distributed Authoring and Versioning / Web Dağıtımlı Yayın ve Sürümleme
WiFi	Wireless Fidelity / Kablosuz Bağlantı Alanı
XML	Extensible Markup Language / Genişletilebilir İşaretleme Dili
XSS	Cross Site Scripting / Siteler Arası Betik Çalıştırma

TANIMLAR

Tanım	Açıklama
Delfi Metodu	Bir karar alma durumuna ilişkin uzman görüşlerinin sistematik ve etkileşimli bir şekilde ele alınmasını sağlayan bir yöntem
Denetim Kaydı	Bir bilgi varlığına kimin eriştiğini veya erişmeye çalıştığını ve erişim sağlayan kullanıcının hangi işlemleri gerçekleştirdiğini gösteren kayıtlar
Genelge	06.07.2019 Tarihli ve 30823 Sayılı Resmi Gazete'de yayımlanan 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi
Gizlilik Dereceli Bilgi/Veri	Bilmesi gereken kişiler dışındakilere açıklanması veya verilmesi, millî güvenlik ve ülke menfaatleri bakımından sakıncalı görülen ve haiz olduğu önem derecelerine göre "ÇOK GİZLİ", "GİZLİ", "ÖZEL" veya "HİZMETE ÖZEL" şeklinde sınıflandırılan bilgi/veri
İlgili Kişi	6698 sayılı Kişisel Verilerin Korunması Kanunu ile tanımlanan kişisel verisi işlenen gerçek kişi
İz Kaydı	Operasyonel bir işlemin başlangıcından bitişine kadar adım adım takip edilmesini sağlayacak kayıtlar
Kritik Bilgi/Veri	• Güvenlik zafiyeti oluşması durumunda yasal yaptırımlara neden olabilecek, içeriğinin yetkisiz personel veya kişiler tarafından görülmesinin kuruma çok ciddi maddi veya manevi zarar vereceği her türlü bilgi/veri, • Kritiklik derecesi 3 olarak hesaplanan varlıkların işlediği veriler, • 24.03.2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ile tanımlanan özel nitelikli kişisel veriler
Kurum	Kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmeler
Kurumsal SOME Kurulum ve Yönetim Rehberi	Ulaştırma ve Altyapı Bakanlığı tarafından yayımlanmış en güncel "Kurumsal SOME Kurulum ve Yönetim Rehberi" dokümanı
Rehber	Bilgi ve İletişim Güvenliği Rehberi
Varlık	Elektronik ve/veya fiziksel ortamlarda yer alan; iletişim yoluyla aktarılabilen bilgiyi içeren; kurumun iş süreçleri açısından değer taşıyan tüm bilgi ve bilgi işleme olanakları, bilgiyi kullanan ve taşıyan personel ile bilgiyi barındıran fiziksel mekânlar
Varlık Grubu	Varlıkların içerdiği verinin kritikliği göz önünde bulundurularak, aynı grup altında değerlendirilmek üzere sınıflandırılan varlıklar bütünü
Varlık Grubu Ana Başlığı	Her varlık grubunun özelliği dikkate alınarak yapılan sınıflandırma
Kritik Altyapı	İşlediği bilgi/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar
Kritik Altyapı Sektörleri	Ulusal Siber Güvenlik Stratejisinde belirlenen kritik altyapı sektörleri

GİRİŞ

1. BÖLÜM

1. GİRİŞ

Kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmelerin bilgi ve iletişim güvenliği kapsamında genel olarak alması gereken tedbirleri belirlemek için 06.07.2019 tarih ve 30823 sayılı Resmi Gazete'de Bilgi ve İletişim Güvenliği Tedbirleri konulu 2019/12 sayılı Cumhurbaşkanlığı Genelgesi yayımlanmıştır. Yayımlanan Genelge doğrultusunda Cumhurbaşkanlığı Dijital Dönüşüm Ofisi koordinasyonunda paydaşların katılımıyla Bilgi ve İletişim Güvenliği Rehberi hazırlanmıştır.

Genelge kapsamında yer alan maddelerin Rehberde yer alan tedbirlerle eşleştirilmesini gösteren tablo EK-A'da sunulmuştur.

1.1. Amaç ve Kapsam

Rehberin temel amacı; bilgi güvenliği risklerinin azaltılması, ortadan kaldırılması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik bilgi/verinin güvenliğinin sağlanması için asgari güvenlik tedbirlerinin belirlenmesi ve belirlenen tedbirlerin uygulanması için yürütülecek faaliyetlerin tanımlanmasıdır.

Rehber, bilgi işlem birimi barındıran veya bilgi işlem hizmetlerini sözleşmeler çerçevesinde üçüncü taraflardan alan, devlet teşkilatı içerisinde yer alan kurum ve kuruluşlar ile kritik altyapı hizmeti veren işletmeleri kapsamaktadır.

Rehberin uygulanması sonucu elde edilmesi beklenenler somutlaştırılarak 12 hedef tanımlanmıştır. Şekil 1'de gösterilen hedefler aşağıda listelenmiştir:

1. Yerli ve milli ürün kullanımının teşvik edilmesi
2. Rehberi uygulayacak kurum ve kuruluşlarda yapılacak mükerrer çalışmaların ve yatırımların önüne geçilmesi
3. Güvenlik tedbirlerinin üç seviyeli olacak şekilde derecelendirilmesi ve varlık gruplarına güvenlik dereceleri ile uyumlu asgari güvenlik tedbirlerinin uygulanması
4. Rehberin güvenlik tedbirleri ile ilgili detayların izlenebilirliğinin sağlanacak şekilde yapılandırılması
5. Güvenlik tedbirlerinin ürün ve teknoloji bağımsız olarak uygulanabilir olması
6. Güvenlik tedbirlerinin uygulanıp uygulanmadığının denetlenebilmesi
7. Güvenlik tedbirlerinin birbirinden bağımsız şekilde uygulanabilirliğini sağlayacak şekilde gruplandırılması ve rehberin modülerliğinin sağlanması
8. Tedbirlerin teknik olarak tüm kurum ve kuruluşlar tarafından uygulanabilir olması
9. İhtiyaçlar, gelişen ve değişen şartlar dikkate alınarak rehberin sürdürülebilirliğinin sağlanması
10. Rehberin format ve içeriğinin özgün olması
11. Rehberin hem güvenlik tedbirlerini uygulayacak personele hem de bu tedbirlerin uygulanıp uygulanmadığını kontrol edecek denetçilere hitap etmesi
12. Rehber içeriğinin bilgi güvenliği çerçevesinde oluşturulmuş mevzuat ve rehberler ile ulusal/uluslararası standartlara uyumlu olması

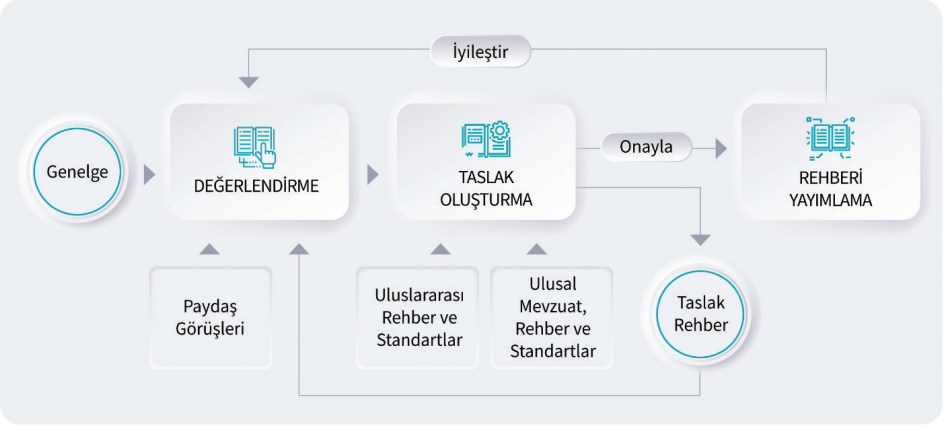
Şekil 1. Bilgi ve İletişim Güvenliği Rehberinin Hedefleri

1.2. Rehberin İçeriği ve Güncelleme Süreci

Rehberin içeriği; amaç ve hedefler doğrultusunda, ulusal/uluslararası standartlar ve rehberler, iyi uygulama örnekleri ile güncel mevzuat göz önünde bulundurularak oluşturulmuştur. EK-B'de rehber içeriğinin uluslararası standartlar ve yayımlı kılavuzlar ile eşleştirilmesini gösteren tablo yer almaktadır. Rehberin içeriği aşağıda listelenen dört ana bölümden oluşmaktadır:

- **Bilgi ve İletişim Güvenliği Rehberi Uygulama Süreci:** Rehberde yer alan tedbirlerin uygulanabilmesini sağlamak amacı ile rehber uygulama süreci tanımlanmıştır. Rehber uygulama süreci, bilgi güvenliği yönetim süreçlerine alternatif olarak uygulanacak bir süreç olarak hazırlanmamış olup mevcut bilgi güvenliği yönetim süreçlerine teknik olarak katkı sağlayacak tedbirleri ve faaliyetleri içermektedir. Kurumlar rehber uygulama süreci ile tanımlanan faaliyetleri, mevcut bilgi güvenliği yönetim süreçleri kapsamında ve uyarlama yaparak yürütmelidir.
- **Varlık Gruplarına Yönelik Güvenlik Tedbirleri:** Tanımlanan her bir varlık grubuna dâhil olduğu ana başlığa göre uygulanacak olan asgari güvenlik tedbirleri belirlenmiş ve detaylandırılmıştır.
- **Uygulama ve Teknoloji Alanlarına Yönelik Güvenlik Tedbirleri:** Varlık grupları özelinde tanımlanan güvenlik tedbirlerine ek olarak, uygulama ve teknoloji alanlarına özel güvenlik tedbirleri tanımlanmış ve detaylandırılmıştır. Her bir varlık grubu için ilgili uygulama ve teknoloji alanları belirlenmeli ve belirlenen alanlar için tanımlanan güvenlik tedbirleri de ilgili varlık gruplarına uygulanmalıdır.
- **Sıkılaştırma Tedbirleri:** İşletim sistemi, veri tabanı ve sunucular için sıkılaştırma tedbirlerini içermektedir.

Rehber, yaşayan bir doküman olacak şekilde; ihtiyaçlar, gelişen teknoloji ve değişen şartlar göz önünde bulundurularak sürekli güncellenecektir. Rehberin güncellenmesi için Şekil 2'de tanımlanan sürecin işletilmesi planlanmaktadır. Rehberin eski sürümlerine ve güncel sürümüne https://www.cbddo.gov.tr adresinden erişilebilir olması sağlanacaktır.



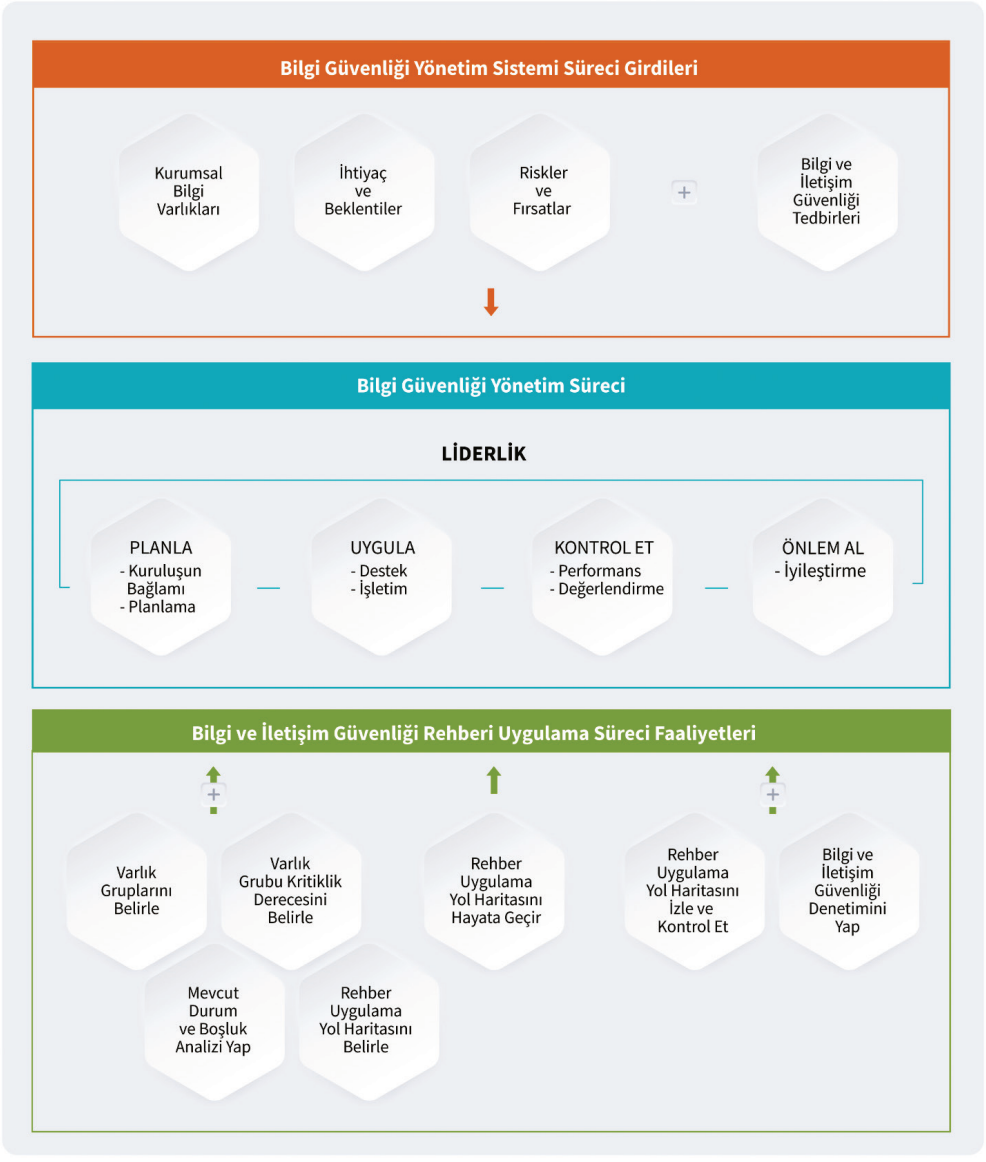
Şekil 2. Rehber Güncelleme Süreci

1.3. Rehber Uyum Planı

Kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmeler tarafından, Bilgi ve İletişim Güvenliği Rehberi Uygulama Süreci'nin ve tanımlanan güvenlik tedbirlerinin uyum planı çerçevesinde ele alınması gerekmektedir. Uyum planı kapsamında yapılacak çalışmalar ve zaman planlamaları Şekil 3'te yer almaktadır. Uygulama yol haritası, uyum planında tanımlanan zaman dilimleri çerçevesinde oluşturulmalıdır.

Şekil 3. Rehber Uyum Planı

Kurumlar rehber uygulama sürecini, yürüttükleri bilgi güvenliği yönetim süreçlerine entegre etmeli ve bilgi güvenliği risk yönetimi faaliyetleri kapsamında rehberde tanımlanan tedbirleri uygulamalıdır. Bilgi ve İletişim Güvenliği Rehberi Uygulama Süreci kapsamında gerçekleştirilmesi gereken çalışmalar ile Bilgi Güvenliği Yönetim Sistemi ana maddeleri arasındaki ilişki Şekil 4'te yer almaktadır.



Şekil 4. Rehber ve Bilgi Güvenliği Yönetim Sistemi İlişkisi

Rehberin 2. Bölümünde rehber uygulama süreci açıklanmıştır. Bu süreç kapsamında kullanılacak anket EK-C.1 olarak sunulmuştur. Bölüm 3'te varlık gruplarına yönelik tedbirlere, Bölüm 4'te de uygulama ve teknoloji alanına yönelik tedbirlere yer verilmiştir. Bölüm 3, 4 ve 5'te yer alan güvenlik tedbirleri açıklanırken tedbirler gruplandırılmış ve tedbir alt başlıkları oluşturulmuştur.

Tedbir ana başlıkları; amacı, önemi ve uygulama adımları ile açıklanmış olup, tedbir alt başlıkları ise aşağıdaki başlıklarda detaylandırılmıştır:

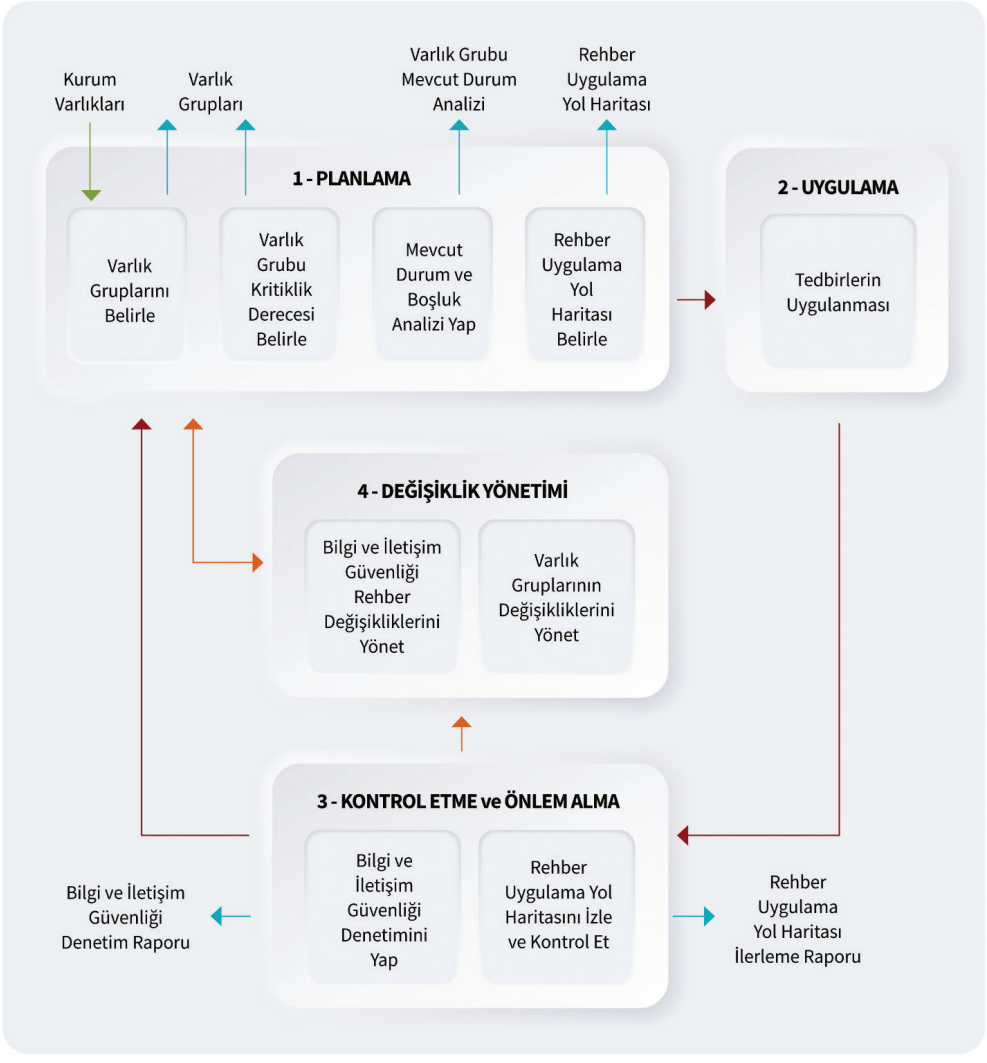
- **Tedbirler:** Alınması gereken tedbirleri seviyelendirerek listeler.
- **Denetim Maddeleri:** Grupta yer alan güvenlik tedbirlerinin uygulanıp uygulanmadığının kontrolü için kullanılabilecek denetim yöntemlerini ve soru örneklerini içerir. Tedbir maddeleri özelinde tanımlanan denetim yöntem önerileri; mülakat, gözden geçirme, güvenlik denetimi, sızma testi ve kaynak kod analizi yöntemlerini içermektedir. Denetim yöntemlerine ilişkin açıklamalar aşağıda yer almaktadır.
    - Mülakat: Denetim yapılan birim kapsamında söz konusu çalışmaların nasıl gerçekleştirildiği bilgisinin ilgili kurum personeli ile yüz yüze görüşülerek edinilmesidir. Gerekli görülmesi durumunda dokümantasyon inceleme çalışması ile desteklenmektedir.
    - Gözden Geçirme: Denetim yapılan birim kapsamında söz konusu çalışmalara yönelik güvenlik gereksinimleri göz önünde bulundurularak detaylı ve sistematik olarak yapılan incelemedir.
    - Güvenlik Denetimi: Bilgi teknolojileri ve güvenlik sistemlerine ait kuralların, sıkılaştırma ve yapılandırma çalışmalarının teknik olarak denetlenmesidir. Gerekli görülmesi durumunda otomatik araç kullanımı ile desteklenmektedir.
    - Sızma Testi: Bilgi teknolojileri ve güvenlik sistemleri kapsamında güvenlik açıklarının tespit edilmesini sağlayan, yetkin kişiler tarafından ve yasalara uygun olarak gerçekleştirilen güvenlik testleridir.
    - Kaynak Kod Analizi: Güvenli yazılım geliştirme konusunda uzman kişiler tarafından kaynak kodların incelenmesi ve güvenlik açıklarının tespit edilmesini sağlayan denetim çalışmasıdır. Gerekli görülmesi durumunda otomatik araç kullanımı ile desteklenmektedir.

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ UYGULAMA SÜRECİ

2. BÖLÜM

2. BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ UYGULAMA SÜRECİ

Bilgi ve İletişim Güvenliği Rehberi Uygulama Süreci Şekil 5'te tanımlanmıştır. Süreç; planlama, uygulama, kontrol etme ve önlem alma ile değişiklik yönetimi alt süreçlerinden oluşmaktadır.



Şekil 5. Bilgi ve İletişim Güvenliği Rehberi Uygulama Süreci

Planlama kapsamında özet olarak; kurum varlıklarının gruplandırılması, gruplama sonucu elde edilen varlık gruplarının kritiklik derecelendirmesinin yapılması, bu varlık grubuna uygulanması gereken güvenlik tedbirlerinin mevcut durumunun analizi ve boşluk analizinin yapılarak yol haritasının hazırlanması faaliyetleri yürütülür. Yol haritasına uygun olarak yürütülecek çalışmalar uygulama alt sürecinde gerçekleştirilir. Rehber kapsamında yürütülen çalışmaların izlenmesi ve kontrolü faaliyetleri, kontrol etme ve önlem alma süreci kapsamında gerçekleştirilir. Kontrol etme ve önlem alma fazında ayrıca, rehberde yer alan tedbirlerin uygulanma durumunu tespit edebilmek için iç ve dış denetim faaliyetleri yürütülür. Rehberdeki güncellemelere uyum için yapılacak değişikliklerin belirlenmesi, kurum varlık gruplarında gerçekleşecek değişikliklerin (varlık grubu içeriğinin değişmesi, yeni varlık

gruplarının tanımlanması, varlık grubu kritiklik derecesinin değişmesi vb.) rehberde tanımlanan tedbirlerle uyumunun sağlanması çalışmaları değişiklik yönetimi kapsamında ele alınır.

Sonraki alt başlıklarda Şekil 5'te tanımlanan fazlar ve bu süreçler kapsamında yürütülecek faaliyetler açıklanmaktadır. Tablo 1'de SAM rollerine ilişkin kısaltmaların açıklamaları yer almaktadır. Alt süreçler kapsamında gerçekleştirilecek faaliyetler ve her bir faaliyet için örnek roller özelinde tanımlanmış sorumluluklar Tablo 2'deki SAM tablosu ile belirtilmektedir.

Tablo 1. SAM Rolleri Açıklamaları

Kısaltma	Açıklaması
S	Sorumlu: Görevi gerçekleştiren personel
O	Onaylayan: Görevi durdurabilen, devam ettirebilen, son kararı verebilen ve hesap veren personel
D	Danışılan: Görev yapılmadan önce bilgisine başvurulması gereken personel
B	Bilgilendirilen: Görev yapıldıktan sonra görevin bittiği konusunda bilgilendirilen personel

Tablo 2'de roller; iç paydaş ve dış paydaş olmak üzere iki kategori altında ele alınmakta olup, ilgili personelin üstlendiği veya o kişiye atanan görev olarak ifade edilmektedir. Alt süreçler doğrultusunda gerçekleştirilecek çalışmalar ise faaliyet olarak tanımlanmakta olup, her bir rolün faaliyetler özelinde tanımlanan sorumluluk ve yetki alanları yer almaktadır.

Tablo 2. Bilgi ve İletişim Güvenliği Rehberi Uygulama Süreci için Sorumluluk Atama Matrisi

No.	FAALİYET ADI	ROL ADI												
		İÇ PAYDAŞLAR								DIŞ PAYDAŞLAR				
		Kurumun En Üst Düzey Yöneticisi	Bilgi Güvenliği Yöneticisi	Bilgi Sistemleri Yöneticisi	İç Denetçi	İlgili Birim Yöneticileri	İlgili Birim Uzman Personeli	Kurumsal SOME Yöneticisi	Varlık Grubu Koordinatörü	Dış Denetim Personeli	DDO	Bağlı/İlgili/İlişkili Üst Kurum	İlgili Düzenleyici ve Denetleyici Kurum	Teknik Danışman
1	Varlık Gruplarını Belirle	O	S	S	B	S	S	B	D					D
2	Varlık Grubu Kritiklik Derecesi Belirle	O	S	S		S	S	B	D					D
3	Mevcut Durum ve Boşluk Analizi Yap	O	S	S	B	S	S	S	D					D
4	Rehber Uygulama Yol Haritası Belirle	O	S	S		B	S	S	D					D
5	Rehber Uygulama Yol Haritasını Hayata Geçir	O	S	S		S	S	S	B					
6	Bilgi ve İletişim Güvenliği Denetimi Yap	O	B	B	S	B		B	D	S	S,B	B	B	
7	Rehber Uygulama Yol Haritasını İzle ve Kontrol Et	O	S	S		S	S	S	B					D
8	Bilgi ve İletişim Güvenliği Rehber Değişikliklerini Yönet	O	S	S	B	S	S	B	D					D
9	Varlık Gruplarının Değişikliklerini Yönet	O	S	S	B	S	S	B	D					D

Tablo 2'de adı geçen rollerin açıklamaları aşağıda verilmiştir:

Kurumun En Üst Düzey Yöneticisi: Kurum hiyerarşisinde bilgi güvenliğinin sağlanmasından ve yönetiminden sorumlu en üst mevkide yer alan kişi.

Bilgi Güvenliği Yöneticisi: Kurumda bilgi güvenliğinin sağlanmasından ve yönetiminden sorumlu personel.

Bilgi Sistemleri Yöneticisi: Kurumda bilgi sistemlerinin yönetiminden sorumlu personel/birim yöneticisi.

İç Denetçi: Kurumda iç denetimi gerçekleştiren personel.

İlgili Birim Yöneticileri: Kurumda, Rehber uygulama sürecinde yer alan aşamaları gerçekleştirme hususunda sorumluluk alacak birim yöneticileri.

İlgili Birim Uzman Personeli: Rehber uygulama sürecinde yer alan aşamaları gerçekleştirme hususunda sorumluluk alacak birim personeli.

Kurumsal SOME Yöneticisi: Kurumda bulunan siber olaylara müdahale ekibinin yöneticisi.

Varlık Grubu Koordinatörü: Rehber uygulama sürecinde yer alan aşamalarda bilgi birikimine danışılan ve bu aşamaları koordine eden personel.

Dış Denetim Personeli: Rehber uygulama sürecinin ve güvenlik tedbirlerinin kurumda uygulanıp uygulanmadığını denetleyen üçüncü taraf denetçiler.

DDO: Cumhurbaşkanlığı Dijital Dönüşüm Ofisi

Bağlı/İlgili/İlişkili Üst Kurum: Kurumun bağlı/ilgili/ilişkili olduğu üst kurum (Ör. Bakanlıklar).

İlgili Düzenleyici ve Denetleyici Kurum: BDDK, EPDK, SPK ve BTK gibi düzenleyici/denetleyici kurumlar.

Teknik Danışman: Rehber uygulama sürecinde bilgi birikimine danışılan üçüncü taraf personel.

2.1. Planlama

2.1.1. Varlık Gruplarının Belirlenmesi

Rehber kapsamında yürütülen çalışmalarda varlıkların belirlenen başlıklar altında toplanarak gruplandırılması ve bu gruplar dikkate alınarak tedbirlerin uygulanması gerekmektedir. Rehber; elektronik ortamda yer alan bilgi/verinin depolandığı, aktarıldığı, işlendiği bilgi işleme olanakları, bilgi işleme olanaklarını kullanan personel ile bilgi işleme olanaklarını barındıran fiziksel ortamlara ilişkin varlıkları kapsamaktadır.

Rehberde tanımlanan varlık grubu ana başlıkları aşağıda listelenmiştir:

- Ağ ve Sistemler
- Uygulamalar
- Taşınabilir Cihaz ve Ortamlar
- Nesnelerin İnterneti (IoT) Cihazları
- Fiziksel Mekânlar
- Personel

Rehberde tanımlanan varlık grubu başlıkları, kurumların tanımlayacakları varlık grupları ve bilgi güvenliği kapsamında yönetilen varlıklar arasındaki ilişki Şekil 6'da tanımlanmıştır.

Şekil 6. Varlıklar, Varlık Grupları ve Varlık Ana Başlıkları

Hâlihazırda, kurumlar tarafından bilgi güvenliği yönetim süreci kapsamında tüm varlıklar belirlenmekte ve bu varlıklar için alınması gereken güvenlik önlemleri uygulanmaktadır. Varlık grupları belirlenirken aşağıdaki hususların dikkate alınması önerilmektedir:

- Tüm kurumsal varlıkların hangi varlık grubu ana başlığı altında yer alacağının belirlenmesi
- Tüm kurumsal varlıkların mümkün olduğunca tek bir varlık grubunda yer almasının sağlanması (Birden fazla varlık grubu tarafından adreslenmesi gereken kurumsal varlıklar, kritiklik derecesi en yüksek olan varlık grubu üzerinden değerlendirilmeli ve dâhil edildiği tüm varlık grupları ile ilgili tedbir maddeleri kurumsal varlık için ele alınmalıdır.)
- Varlık gruplarının tanımlanması için kullanılacak alt kırılımların kurumsal ihtiyaçlar doğrultusunda belirlenmesi (kurum hizmet alanları, kurum organizasyon yapısı, teknolojiler, uluslararası iyi örnekler, BT altyapıları vb.)
- Aynı güvenlik izolasyonunda yer alan varlıkların mümkün olduğunca aynı varlık grubuna dâhil edilmesi
- Farklı güvenlik seviyesine sahip olması gereken varlıkların farklı varlık gruplarında olacak şekilde gruplandırılması
- Aynı seviyede güvenlik tedbirlerinin uygulanacağı düşünülen varlık gruplarının birleştirilerek varlık grubu sayısının azaltılması
- Her bir varlık grubu ana başlığı altında yer alan varlık gruplarının sayılarının yönetilebilecek sayıda olması

Tanımlanan her bir varlık grubu için ilişkili uygulama ve teknoloji alanına yönelik güvenlik tedbiri ana başlıkları seçilir. Uygulama ve teknoloji alanı ana başlıkları altındaki tedbirler için ilgili varlık grubuna atanan kritiklik derecesi göz önünde bulundurulur. Aşağıda örnek bir kurumda varlık grubu belirleme çalışmaları sonucu elde edilebilecek varlık grubu listesi yer almaktadır:

- Ağ ve Sistem varlık grubu ana başlığı
  - Merkez bina açık ağ ve BT sistemi (1 adet)
  - Felaket kurtarma merkezi ağ ve BT sistemi (1 adet)
  - Kapalı ağ ve BT sistemi (1 adet)
  - Test ağ ve BT sistemi (1 adet)
  - OT sistemi (1 adet)
  - A tipi taşra ağ ve BT sistemi (5 adet)
  - B tipi taşra ağ ve BT sistemi (8 adet)

- Uygulama varlık grubu ana başlığı
  - E-devlet üzerinden erişilebilen G2G uygulama (5 adet)
  - Kritik veri işleyen G2B uygulama (15 adet)
  - Kritik veri işleyen kurum içi uygulama (20 adet)
  - Kritik veri işlemeyen kurum içi uygulama (60 adet)

- Taşınabilir Cihaz ve Ortam varlık grubu ana başlığı
  - İdari yöneticilerin kullandığı tablet ve cep telefonları (40 adet)
  - Sistem yöneticilerin kullandığı dizüstü bilgisayarlar (20 adet)
  - Yazılım geliştiricilerin kullandığı dizüstü bilgisayarlar (30 adet)
  - Personelin kullandığı taşınabilir ortamlar (USB cihazı) (400 adet)

- Nesnelerin İnterneti (IoT) Cihazları varlık grubu ana başlığı
  - Sistem odası kameraları (10 adet)
  - Ortam sensör cihazları (nem, gaz, sıcaklık) (30 adet)

- Fiziksel Mekânlar varlık grubu ana başlığı
  - Merkez bina veri merkezi (1 adet)
  - Felaket kurtarma merkezi (1 adet)
  - A tipi taşra veri merkezi (5 adet)
  - B tipi taşra veri merkezi (8 adet)
  - İdari yönetici odası (2 adet)
  - Sistem yöneticisi odası (3 adet)
  - Personel odası (100 adet)

- Personel varlık grubu ana başlığı
  - Üst yönetici (5 personel)
  - Birim yöneticisi ve daire başkanı (40 personel)
  - Sistem yöneticisi (20 personel)
  - Yazılım geliştirici (40 personel)
  - Son kullanıcı (1500 personel)
  - Altyüklenici personeli (10 personel)

2.1.2. Varlık Grubu Kritiklik Derecesinin Belirlenmesi

Varlık gruplarının belirlenmesinin ardından bu varlık gruplarının hangi kritiklik derecesine sahip olduğu belirlenmelidir. Her bir varlık grubunun kritiklik derecesi, işlenen verinin gizlilik, bütünlük ve erişilebilirlik açısından kritikliği ile oluşabilecek güvenlik ihlallerinin etki alanları dikkate alınarak belirlenecektir. Bu kapsamda kullanılacak boyutlar Şekil 7'de tanımlanmıştır.

Şekil 7. Kritiklik Derecesi Belirlemek için Kullanılan Boyutlar

Kritiklik derecesi belirleme boyutları aşağıda özetlenmiştir:

- İşlenen veri ile ilgili boyutlar
    - **Gizlilik**: Bilginin yetkisiz kişilerin erişimine karşı korunması
    - **Bütünlük**: Bilginin tam ve doğru olma durumunun korunması
    - **Erişilebilirlik**: Bilginin yetkili kişilerce ulaşılabilir ve kullanılabilir durumda olması
- Etki alanı ile ilgili boyutlar
    - **Bağımlı Varlıklar**: Varlık grubuna bağımlı olan diğer varlıklar üzerindeki etkisi
    - **Etkilenen Kişi Sayısı**: Bilgi güvenliği ihlal olayı meydana geldiğinde etkilenebilecek kişi sayısı
    - **Kurumsal Sonuçlar**: Bilgi güvenliği ihlal olayı meydana geldiğinde karşılaşılacak kurumsal durum

- **Sektörel Etki**: Varlık grubunun hizmet verdiği sektöre etkisi
- **Toplumsal Sonuçlar**: Bilgi güvenliği ihlal olayı meydana geldiğinde karşılaşılacak toplumsal durum

Bu boyutlar dikkate alınarak bir anket formu oluşturulmuş ve EK-C.1'de sunulmuştur. Her bir varlık grubu için bu anket formu doldurularak ilgili varlık grubunun kritiklik derecesi belirlenmelidir. "Varlık Grubu Kritiklik Derecelendirme Anketi" olarak tanımlanan anket her bir varlık grubu özelinde rehber uyumluluk denetimi kapsamında kontrol edilecektir. İlgili varlık grubu için uygulanması gereken tedbir maddeleri, varlık grubu için belirlenmiş olan kritiklik derecesi göz önünde bulundurularak belirlenir.

Varlık grubu kritiklik derecesi belirleme aşamasında aşağıdaki adımlar takip edilir:

- Her bir varlık grubu için EK-C.1'de yer alan anket formu ilgili paydaşların katılımı ile doldurulur. Anket çalışması kapsamında varlıkların sahipleri, sistem yöneticileri, geliştiriciler, kullanıcı temsilcileri, yöneticileri ve kurumun sahip olduğu en yetkin personel katılım sağlamalıdır. Anket doldurma çalışmalarında Delfi metodunun kullanılması önerilmektedir. Anket çalışması aşağıda yer alan Delfi metodu uygulama adımları izlenerek gerçekleştirilmelidir.
    1. Anketin uygulanacağı uzman kişiler belirlenir.
    2. Anket uzman kişiler tarafından doldurulur.
    3. Anket sonuçları değerlendirilir.
    4. Tüm katılımcılar bir fikir üzerinde ortak karar verene kadar anket uygulanmaya devam edilir ve 2. adıma dönülür.
    5. Tüm anket sonuçlarına göre uzlaşılan karar uygulanır.
- Her varlık grubu için doldurulan anket sorularının cevapları için anket formunda yer alan puanlar toplanarak anket puanı hesaplanır. Tablo 3 kullanılarak anket puanına karşılık gelen kritiklik derecesi belirlenir. Belirlenen derece, varlık grubunun kritiklik derecesi olarak kullanılır.

Tablo 3. Anket Puanına Karşılık Gelen Kritiklik Derecesi

Anket Puanı	Varlık Grubu Kritiklik Derecesi
Anket puanı 18'den küçük ise	Derece 1
Anket puanı 18 (dâhil) ile 28 arasında ise	Derece 2
Anket puanı 28 ve daha yüksek ise	Derece 3

- Varlık grubu içinde yer alan tüm varlıklara aynı güvenlik tedbirlerinin uygulanacağı dikkate alınarak anket sonuçları tekrar değerlendirilir. Gerekli görülmesi durumunda varlık grupları güncellenerek anket çalışmaları tekrarlanır.
- Kritiklik derecesi tanımlanan her bir varlık grubu için kritiklik dereceleri ile uygulama ve teknoloji alanlarına yönelik güvenlik tedbirlerinin uygulanma durumlarının kayıt altına alındığı EK-C.2'de yer alan form doldurulur.

Aşağıdaki maddelerde kritiklik derecesinin belirlenmesi ile ilgili çeşitli örnekler verilmektedir.

- Tablo 4'te örnek iki varlık grubu için uygulanan anketler sonucunda elde edilen puanlar ve toplam anket puanları verilmiştir. Tablo 3 kullanılarak varlık grubu 1'in kritiklik derecesinin "Derece 2" ve varlık grubu 2'nin kritiklik derecesinin "Derece 3" olduğu belirlenir.

Tablo 4. Varlık Grubu Kritiklik Derecesinin Belirlenmesi

Anket Sorusu	Varlık Grubu 1 İçin Puan	Varlık Grubu 2 İçin Puan
1. Soru	3	5
2. Soru	3	5
3. Soru	3	5
4. Soru	2	4
5. Soru	3	5
6. Soru	3	3
7. Soru	3	5
8. Soru	2	6
	22 (Anket Puanı)	**38 (Anket Puanı)**

- Tablo 5'te örnek bir kuruma ait varlık gruplarının anket çalışmaları sonucunda elde edilen kritiklik derecelerine ve varlık grubu ana başlıklarına göre dağılımı gösterilmektedir.

Tablo 5. Alt Varlık Gruplarının Kritiklik Derecesinin Belirlenmesi

Varlık Grubu Ana Başlıkları	Varlık Grubu Sayıları			
	Derece 1	Derece 2	Derece 3	Toplam
Ağ ve Sistemler	2	1	4	7
Uygulamalar	-	2	2	4
Taşınabilir Cihaz ve Ortamlar	1	-	3	4
Nesnelerin İnterneti (IoT) Cihazları	-	2	-	2
Fiziksel Mekânlar	2	3	3	8
Personel	-	3	3	6

- Tablo 6'da varlık grubu 1, varlık grubu 2'ye ait varlık grupları ile uygulama ve teknoloji alanlarına ve sıkılaştırma tedbirlerine yönelik uygulanması gereken tedbir ana başlıkları ve tedbir maddeleri için ilgili seviyeler yer almaktadır.

Tablo 6. Varlık Gruplarına Yönelik Tedbir Uygulanabilirlik Örnek Çalışması

Varlık Grubu Ana Başlığı	**Varlık Grubu No**	**Varlık Grubu Adı**	**Uygulama ve Teknoloji Alanlarına Yönelik Güvenlik Tedbirleri** (Her varlık grubu için aşağıdaki başlıkların uygulanabilir (U) / Uygulanabilir Değil (UD) olduğunu belirtiniz.)						**Sıkılaştırma Tedbirleri** (Her varlık grubu için aşağıdaki başlıkların uygulanabilir (U) / Uygulanabilir Değil (UD) olduğunu belirtiniz.)			**Kritiklik Derecesi (Derece 1/ Derece 2/ Derece 3)**
			Kişisel Verilerin Güvenliği	**Anlık Mesajlaşma Güvenliği**	**Bulut Bilişim Güvenliği**	**Kripto Uygulamaları Güvenliği**	**Kritik Altyapılar Güvenliği**	**Yeni Geliştirmeler ve Tedarik**	**İşletim Sistemi Sıkılaştırma Tedbirleri**	**Veri Tabanı Sıkılaştırma Tedbirleri**	**Sunucu Sıkılaştırma Tedbirleri**	
Uygulamalar	1	Kritik Verileri İşlemeyen Kurum İçi Uygulama	U	U	U	U	UD	U	U	UD	U	Derece 2
	2	Kritik Verileri İşleyen Kurum İçi Uygulama	U	U	UD	U	UD	U	U	UD	U	Derece 3

2.1.3. Mevcut Durum ve Boşluk Analizi

Varlık gruplarının kritiklik dereceleri dikkate alınarak Bölüm 3, 4 ve 5'te yer alan güvenlik tedbirlerinin hangilerinin uygulanması gerektiğinin belirlenmesi ve belirlenen güvenlik tedbirlerine göre mevcut durumun tespiti için detaylı çalışma yapılmalıdır. Rehberde tanımlanan güvenlik tedbirleri aşağıda yer alan üç ana başlık altında sınıflandırılmıştır.

Varlık gruplarına yönelik güvenlik tedbirleri ana başlıkları:

- Ağ ve Sistem Güvenliği
- Uygulama ve Veri Güvenliği
- Taşınabilir Cihaz ve Ortam Güvenliği
- Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği
- Personel Güvenliği
- Fiziksel Mekânların Güvenliği

Uygulama ve teknoloji alanlarına yönelik güvenlik tedbirleri ana başlıkları:

- Kişisel Verilerin Güvenliği
- Anlık Mesajlaşma Güvenliği
- Bulut Bilişim Güvenliği
- Kripto Uygulamaları Güvenliği
- Kritik Altyapılar Güvenliği
- Yeni Geliştirmeler ve Tedarik

Sıkılaştırma faaliyetlerine yönelik güvenlik tedbirleri ana başlıkları:

- İşletim Sistemi Sıkılaştırma Tedbirleri
- Veri Tabanı Sıkılaştırma Tedbirleri
- Sunucu Sıkılaştırma Tedbirleri

Bölüm 3, 4 ve 5 ana başlıklarının altında yer alan her bir güvenlik tedbiri temel, orta ve ileri seviye olarak derecelendirilmiştir. Varlık grubuna uygulanacak tedbirler aşağıdaki sınıflandırmaya göre belirlenir.

- **1. Seviye Tedbirler:** Kritiklik derecesi 1 olan varlık gruplarında yer alan tüm varlıklara temel seviye güvenlik tedbirleri uygulanır.
- **2. Seviye Tedbirler:** Kritiklik derecesi 2 olan varlık gruplarında yer alan tüm varlıklara temel seviye güvenlik tedbirlerine ek olarak orta seviye güvenlik tedbirleri uygulanır.
- **3. Seviye Tedbirler:** Kritiklik derecesi 3 olan varlık gruplarında yer alan tüm varlıklara temel ve orta seviye güvenlik tedbirlerine ek olarak ileri seviye güvenlik tedbirleri uygulanır.

Her bir varlık grubu kapsamında mevcut durum tespiti için analiz çalışmaları gerçekleştirilir. Bu kapsamda aşağıdaki adımlar takip edilir:

- Her bir varlık grubu için öncelikle Bölüm 3'ten ilgili güvenlik tedbirleri ana başlığı (Ağ ve Sistem Güvenliği, Uygulama ve Veri Güvenliği, Personel Güvenliği vb.) seçilir. Seçilen başlıkta yer alan tedbirlerden varlık grubunun kritiklik derecesine uygun olan tedbirler belirlenir.
- Her varlık grubunda yer alan varlıklar dikkate alınarak Bölüm 4 ve 5'te yer alan güvenlik tedbiri ana başlıkları (Bulut Bilişim Güvenliği, Kişisel Verilerin Güvenliği, İşletim Sistemi Sıkılaştırma, Veri Tabanı Sıkılaştırma vb.) seçilir. Seçilen başlıklarda yer alan tedbirlerden, varlık grubunun kritiklik derecesine uygun olan tedbirler belirlenir.
- Varlık grupları için belirlenen tüm tedbirler ile ilgili mevcut durum analiz edilir ve varlık grubu mevcut durum analiz raporu hazırlanır. Mevcut durum analizi çalışmaları kapsamında teknik çalışma, toplantı, otomatik araç ile durum tespiti, dokümantasyon inceleme vb. faaliyetler gerçekleştirilebilir. Varlık grubuna bir tedbirin uygulanıp uygulanmadığı tespit edilirken öncelikle aşağıdaki sınıflandırmaya göre uygulama durumuna karar verilir ve mevcut durum ile ilgili açıklayıcı bilgi yazılır.
    - Tedbir varlık grubunda yer alan tüm varlıklara uygulanmakta ise "tamamen"
    - Tedbir varlık grubunda yer alan varlıkların çoğuna uygulanmakta fakat bazı varlıklara kısmen uygulanmakta veya henüz uygulanmamakta ise "çoğunlukla"
    - Tedbir varlık grubunda yer alan bir kısım varlığa uygulanmakta veya tedbir kısmen uygulanmakta ise "kısmen"
    - Tedbir hiç uygulanmamakta ise "hiç"
    - Tedbirin teknik olarak uygulanma ihtimali bulunmuyorsa "uygulanamaz"
- Her bir varlık grubu için yapılan değerlendirmeler EK-C.3'te yer alan form ile kayıt altına alınır.
- Varlık grupları için hazırlanan mevcut durum analizi raporlarından faydalanılarak varlık grubunun kritiklik derecesi ile uyumlu tedbirler seçilir. Seçilen tedbirlerden uygulanmayan veya kısmen uygulananlar listelenerek boşluk analizi çalışması gerçekleştirilir.

Örnek olarak, bir kurumda "kurum iç uygulamaları" olarak tanımlanan bir varlık grubunun kritiklik derecesinin "Derece 2" olduğu görülmüştür. Bu varlık grubu için mevcut durum analizi çalışması için aşağıdaki adımlar gerçekleştirilir:

- Bu varlık grubu Uygulama Varlık Grubu Ana Başlığı altında olduğu için Bölüm 3'ten "Uygulama ve Veri Güvenliği" başlığı seçilir. Bu başlık altında yer alan tüm tedbirlerden 1. ve 2. seviye tedbirler listelenir.
- Bu varlık grubunda yer alan uygulamalar kişisel veri işlediği ve bulut servisleri kullandığı düşünüldüğünde Bölüm 4'ten "Kişisel Verilerin Güvenliği" ve "Bulut Bilişim Güvenliği" başlıkları seçilir. Seçilen bu başlıklar altında yer alan tedbirlerden 1. ve 2. seviye tedbirler listelenir.

- Bu varlık grubunda yer alan uygulamaların; işletim sistemi, veri tabanı ve web sunucusu kullandığı düşünüldüğünde Bölüm 5'ten "İşletim Sistemi Sıkılaştırma Tedbirleri", "Veri Tabanı Sıkılaştırma Tedbirleri" ve "Sunucu Sıkılaştırma Tedbirleri" başlığı seçilerek, bu başlıklar altında yer alan tedbirlerden 1. ve 2. seviye tedbirler listelenir.
- Önceki adımlarda belirlenen tedbirlerin tümü için mevcut durumuna karar verilir. Bu kapsamda her bir tedbirin varlık grubunda yer alan tüm varlıklara uygulanıp uygulanmadığı tespit edilerek raporlanır. Çalışma sonucunda varlık grubu mevcut durum analizi raporu hazırlanır.
- Varlık grupları için hazırlanan mevcut durum analiz raporlarından faydalanılarak boşluk analizi gerçekleştirilir. 1. ve 2. seviye tedbirleri içeren ilgili uygulama adımlarından gerçekleştirilmeyenler veya kısmen gerçekleştirilenler listelenerek raporlanır.

2.1.4. Rehber Uygulama Yol Haritasının Hazırlanması

Boşluk analizi sonucunda tespit edilen eksikliklerin giderilmesi için gereken faaliyetler belirlendikten sonra planlama yapılır. Planlamalar kapsamında ilgili tüm yasal, düzenleyici ve sözleşmeden doğan gereksinimler dikkate alınır.

Rehber uygulama yol haritası kapsamında yapılacak çalışmalar belirlenir. Çalışmalar, aşağıdaki gruplarla sınırlı olmamakla birlikte şu şekilde gruplandırılabilir:

- Yetkinlik kazanımı ve eğitimler
- Ürün tedariki
- Hizmet alımı
- Danışmanlık
- Geliştirme / yeniden geliştirme
- Tasarlama / yeniden tasarlama
- Sıkılaştırma
- Sürüm güncelleme
- Dokümantasyon
- Kurumsal süreç iyileştirme

Yapılacak çalışmalar belirlendikten sonra her çalışma için 2-3 aylık dönemler halinde hedefler belirlenir ve gerekli kaynak tahsisi (personel, bütçe, fiziksel ortam vb.) için planlama yapılır. Uygulama yol haritası kapsamında yapılan planlamalar EK-C.4'te yer alan form ile kayıt altına alınır.

Kurum, boşluk analizi sonucunda uygulanması gereken ilave tedbirler kapsamındaki herhangi bir gereksinimi; üst yönetim tarafından onaylanmış teknik kısıtlamalar ve iş gereksinimlerinden dolayı rehberde tanımlandığı şekli ile karşılayamaması durumunda telafi edici kontroller uygulayabilir. Telafi edici kontroller, yerine uygulandıkları tedbir maddeleri ile aynı amaç ve etkiye sahip olmaları durumunda kullanılabilir olarak kabul edilecektir. Uygulanmasına karar verilen her bir telafi edici kontrol EK-C.5'te yer alan form ile kayıt altına alınmalıdır.

Bilgi güvenliğinde en zayıf halkanın insan faktörü olduğu göz önünde bulundurulduğunda, hem güvenlik tedbirlerinin uygulanmasında hem de uygulanan güvenlik tedbirlerinin denetlenmesinde görev alacak kurum personelinin belirli bir yetkinliğe sahip olması önem arz etmektedir. Bu çerçevede, bilgi güvenliği ile ilgili eğitimler kaynaklar dâhilinde planlanmalı ve personelin gelişimi hakkında ışık tutacak ölçüm mekanizmaları hayata geçirilmelidir. Eğitimlerin sadece teorik bilgi vermekten ziyade, personelin ilgili alanda pratik becerisini arttıracak uygulamaları içermesi önemlidir. Bu kapsamda planlanacak eğitimlerde, laboratuvar ortamının bulunması ve bu ortamda katılımcıların öğrendikleri bilgiyi beceriye dönüştürmesi sağlanmalıdır.

Rehberin uygulanması için yürütülecek çalışmalara dâhil olacak personele yetkinlik kazandırmak amacıyla rehberde bulunan uygulama adımları ve denetim tablolarının nasıl ele alınacağıyla ilgili olarak çeşitli uygulama çalıştaylarının düzenlenmesi veya bu kapsamda gerçekleştirilecek çalışmalara katılım sağlanması gerekmektedir.

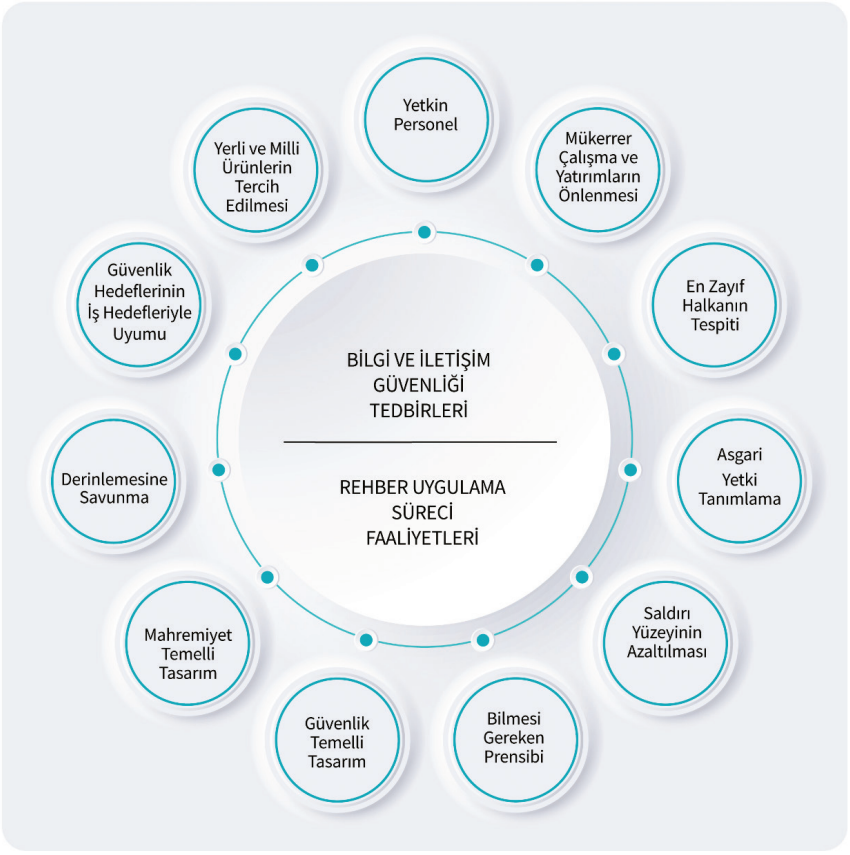
Bu kapsamda gerçekleştirilen tüm çalışmalar rehber uygulama yol haritası olarak dokümante edilecektir.

2.2. Uygulama

Rehber uygulama yol haritası, dönemsel olarak belirlenen hedefler dikkate alınarak planlanan şekilde kurum personeli tarafından hayata geçirilecektir. Bu kapsamda yol haritasında belirlenen tedarik, hizmet alımı, yeniden tasarım vb. tüm çalışmaların gerekli kaynak ihtiyaçlarının tahsis faaliyetleri önceliklendirilmelidir.

2.2.1. Bilgi ve İletişim Güvenliği Temel Prensipleri

Yol haritasının planlanması ve uygulanması aşamalarında gerçekleştirilecek tüm çalışmalarda Şekil 8'de yer alan temel prensipler dikkate alınmalıdır.



Şekil 8. Temel Prensipler

- **Yetkin Personel:** Yol haritasını uygulayacak ve denetim faaliyetlerini yürütecek personel bilgi güvenliği, siber güvenlik veya kişisel verilerin korunması konularında temel eğitimleri almış olmalıdır.
- **Güvenlik Temelli Tasarım (Security by Design):** Güvenlik tasarım aşamasında dikkate alınmalı ve tasarım aşamasında güvenlik tasarımı yapılmalıdır.
- **Mahremiyet Temelli Tasarım (Privacy by Design):** Kişisel veri güvenliği tasarım aşamasında dikkate alınmalı ve tasarım aşamasında güvenlik tasarımı yapılmalıdır.
- **Derinlemesine Savunma (Defence in Depth):** Varlıkların güvenliği ihtiyaçlar dikkate alınarak birden fazla savunma katmanı ile sağlanmalıdır.
- **Saldırı Yüzeyinin Azaltılması:** Saldırıya maruz kalınabilecek alanların en aza indirilmesi sağlanmalıdır.
- **Asgari Yetki Tanımlama:** Bir işin gerçekleştirilmesi için yeterli ve en az yetkiyle çalıştırılması sağlanmalıdır.
- **En Zayıf Halkanın Tespiti:** Yapılan çalışmalarda ve tasarımlarda en zayıf halkanın tespit edilerek güçlendirilmesi için planlama yapılmalıdır.
- **Güvenlik Hedeflerinin İş Hedefleriyle Uyumu:** Güvenlik hedefleriyle iş hedeflerinin birbirleriyle uyumu sağlanmalıdır.
- **Yerli ve Milli Ürünlerin Tercih Edilmesi:** İhtiyaç duyulan güvenlik gereksinimlerinin karşılanması durumunda yerli ve milli ürünler tercih edilmelidir.
- **Mükerrer Çalışma ve Yatırımların Önlenmesi:** Mükerrer çalışma ve yatırımların önüne geçilecek şekilde çalışmalar yürütülmelidir.
- **Bilmesi Gereken Prensibi:** Herhangi bir konu veya işi, görev ve sorumlulukları gereği; öğrenme, inceleme, gereğini yerine getirme ve koruma sorumluluğu bulunanlar yetkileri düzeyinde bilgi sahibi olmalıdır.

2.3. Kontrol Etme ve Önlem Alma

2.3.1. Rehber Uygulama Yol Haritasının İzlenmesi ve Kontrol Edilmesi

Rehber uygulama yol haritası çalışmalarının ilerleme durumlarının takibi ve hazırlanan plandan sapmaların tespit edilerek gerekli önlemlerin alınması ile ilgili faaliyetlerin yürütülmesi gerekmektedir. Ayrıca uygulama yol haritası çalışmaları yürütülürken karşılaşılacak sorun ve risklerin yönetimi de gerçekleştirilmelidir.

Dönem sonlarında uygulama yol haritasında yürütülen çalışmalar, planlanan hedeflerden sapmalar, sorun ve riskler, alınan önlemler hakkında bilgileri içeren yol haritası ilerleme raporları hazırlanmalıdır.

2.3.2. Bilgi ve İletişim Güvenliği Denetimi

Rehberin uygulanmasına ilişkin denetimler, gerekli mekanizmalar oluşturularak, yılda en az bir kez olmak üzere iç denetim yolu ile gerçekleştirilir. Denetim faaliyetleri Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından hazırlanan ve https://www.cbddo.gov.tr adresinde yayımlanan Bilgi ve İletişim Güvenliği Denetim Rehberi esas alınarak yürütülür.

2.4. Değişiklik Yönetimi

2.4.1. Rehber Değişikliklerinin Yönetilmesi

Bilgi ve İletişim Güvenliği Rehberi; ihtiyaçlar, gelişen teknoloji, değişen şartlar ile Ulusal Siber Güvenlik Stratejisi ve Eylem Planlarında yapılacak değişiklikler göz önünde bulundurularak güncellenecektir. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından rehberde yapılacak değişiklikler sürekli izlenerek kurum tarafından mevcut rehber uygulama yol haritası güncellenir veya yeni bir yol haritası hazırlanması için çalışmalar yürütülür.

2.4.2. Varlık Gruplarının Değişikliklerinin Yönetilmesi

Kurumun varlık grupları ile uygulama ve teknoloji alanlarında oluşabilecek değişiklikler aşağıdakilerle sınırlı olmamakla birlikte sürekli izlenmelidir.

- Yeni varlık gruplarının oluşturulması
- Varlık gruplarında yer alan varlıkların değişmesi
- Mevcut varlık grupları yerine farklı varlık gruplarının tanımlanması
- Varlık gruplarının kritiklik derecelerinin değişmesi
- Varlık gruplarına uygulanacak uygulama ve teknoloji alanlarının değişmesi
- Varlık gruplarını etkileyen mevzuat, standart veya ikincil düzenlemelerin değişmesi

Kurumsal ihtiyaçlar ve gelişmeler dikkate alınarak varlık grupları ile uygulama ve teknoloji ya da sıkılaştırma tedbirleri kapsamında gerçekleşecek bir değişiklik tespit edildiğinde tekrar planlama yapılarak yeni yol haritasının oluşturulması veya mevcut yol haritasının güncellenmesi gerekmektedir.

VARLIK GRUPLARINA YÖNELİK GÜVENLİK TEDBİRLERİ

3. BÖLÜM

3. VARLIK GRUPLARINA YÖNELİK GÜVENLİK TEDBİRLERİ

Varlık grubuna yönelik güvenlik tedbirleri, varlık grubu ana başlık gruplarına uygun olarak başlıklara ayrılarak tanımlanmıştır. Rehberde tanımlanan varlık grubu ana başlıkları ve varlık gruplarında yer alabilecek örnek varlıklar aşağıda listelenmiştir:

- Ağ ve Sistemler: Kurumsal ağ, sunucu, donanım, güvenlik cihazı, kimlik yönetim ve doğrulama sistemi, veri sızıntısı önleme sistemi vb. varlıkların oluşturduğu mantıksal / fiziksel gruplar
- Uygulamalar: Kurumsal olarak geliştirilen veya tedarik edilen yazılımların oluşturduğu mantıksal gruplar
- Taşınabilir Cihaz ve Ortamlar: Kurumsal olarak kullanılan taşınabilir dizüstü bilgisayar, tablet, telefon vb. cihazlar ile taşınabilir ortam (CD, USB disk vb.) grupları
- Nesnelerin İnterneti (IoT) Cihazları: Kurumsal ortamlarda kullanılan sensör, kamera vb. cihaz grupları
- Personel: Kurum bünyesinde görev yapan personel / uzman grupları
- Fiziksel Mekânlar: Bilgi güvenliği kapsamında yönetilen kurumsal sunucu odası, felaket kurtarma merkezi, personel odası vb. fiziksel mekânların grupları

3.1. Ağ ve Sistem Güvenliği

Amaç

Bu güvenlik tedbiri ana başlığının amacı, ağ ve sistem güvenliği çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. “Ağ ve Sistem Güvenliği” ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Donanım Varlıklarının Envanter Yönetimi
- Yazılım Varlıklarının Envanter Yönetimi
- Tehdit ve Zafiyet Yönetimi
- E-Posta Sunucusu ve İstemcisi Güvenliği
- Zararlı Yazılımlardan Korunma
- Ağ Güvenliği
- Veri Sızıntısı Önleme
- İz ve Denetim Kayıtlarının Tutulması ve İzlenmesi
- Sanallaştırma Güvenliği
- Siber Güvenlik Olay Yönetimi
- Sızma Testleri ve Güvenlik Denetimleri
- Kimlik Doğrulama ve Erişim Yönetimi
- Felaket Kurtarma ve İş Sürekliliği Yönetimi
- Uzaktan Çalışma

3.1.1. Donanım Varlıklarının Envanter Yönetimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.1.1	1	Donanım Envanterinin Yönetimi	Veri saklama, işleme ve iletme yeteneği olan tüm donanımların güncel bir envanteri tutulmalı, yalnızca yetkilendirilmiş personelin varlık envanterine erişimi mümkün kılınmalıdır.
3.1.1.2	1	Donanım Envanter İçeriğinin Yönetimi	Donanım envanteri en az; her bir donanımın ağ adresini, donanım adresini, makine adını, seri numarasını, markasını, modelini, destek alınan tedarikçi sözleşme bilgilerini (bakım süresi, kapsamı vb.), donanımın sorumlusunu, sorumlu kişinin birimini ve donanımın kurum tarafından onaylı olup olmadığı bilgisini içermelidir. Donanım envanter içeriğinde yapılan değişiklikler kayıt altına alınmalıdır.
3.1.1.3	1	Donanım Envanterine Kaydedilmemiş Donanımların Yönetimi	Yeni tedarik edilen ya da ağa yeni bağlanacak donanımların, donanım varlık envanterine kaydı yapılmadan kurum ağına bağlanmamasına yönelik politika ve prosedürler oluşturulmalı ve uygulanmalıdır.
3.1.1.4	2	Aktif Keşif Araçlarının Kullanılması	Kurum ağına bağlı cihazları tanımlamak ve donanım varlık envanterindeki değişiklikleri takip etmek için aktif keşif araçları kullanılmalıdır.
3.1.1.5	2	DHCP Kayıt Mekanizması ile Yeni Donanımların Tespiti	Kurumun donanım envanterini güncel tutmak için tüm DHCP sunucularında ya da IP adres yönetim araçlarında kayıt mekanizmasının kullanımı sağlanmalıdır.
3.1.1.6	2	Kullanım Ömrünü Tamamlayan Cihazların Veri Depolama Üniteleri	Kullanım ömrünü tamamlayan cihazların veri depolama üniteleri (HDD, SSD, USB, disk, harici bellek vb.) güvenli bir şekilde imha edilmelidir. Kurum içinde tekrar kullanılması durumunda ise veri kurtarmaya imkân sağlamayacak şekilde güvenli silme işlemine tabi tutulduktan sonra kullanıma alınmalıdır.
3.1.1.7	2	Kurum Ağı Bağlantı Noktalarında Kimlik Denetimi Yapılması	Sadece onaylı donanımların kurum ağına bağlanabilmesi için, 802.1x standardı veya NAC çözümleri kullanılarak kurum ağına bağlanan cihazlara kimlik denetimi yapılmalıdır.
3.1.1.8	3	Donanım Varlıklarının Kimlik Denetimi için İstemci Sertifikalarının Kullanılması	Destekleyen cihazlarda, kurumun güvenli ağlarına bağlanan donanım varlıklarının kimlik denetimi için istemci sertifikaları kullanılmalıdır. Sertifika, yetkilendirilmiş personel tarafından güvenli alanda oluşturulmalıdır. Sertifikanın anahtar uzunluğu, tipi (NES/NES olmayan) ve oluşturulma yöntemi bilgi güvenliği gereksinimleri doğrultusunda seçilmelidir. Oluşturulan sertifika güvenli alanda saklanmalı ve sertifika yaşam döngüsünün takibi yapılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.1.9	3	Sabit Disk Güvenliği	Kurum tarafından satın alınan kullanıcı bilgisayarlarına ait sabit diskler, veri kurtarmaya imkân sağlamayacak şekilde güvenli silme işlemine tabi tutulduktan sonra sistemlere dâhil edilmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.1.1	Donanım Envanterinin Yönetimi	Mülakat, Gözden Geçirme	Kurum bünyesinde detaylı ve güncel bir donanım envanteri tutulmakta mıdır? Envanter yönetim süreci tanımlanmış mıdır? Donanım envanterine hangi personelin erişim yetkisi bulunmaktadır?
3.1.1.2	Donanım Envanter İçeriğinin Yönetimi	Mülakat, Gözden Geçirme	Donanım envanterinde; her bir donanım için ağ adresi, donanım adresi, makine adı, seri numarası, marka, model, donanımın sorumlusu ve donanımın kurum tarafından onaylı olup olmadığı bilgisi tutulmakta mıdır? Donanım envanterinde yer alan varlıklara ait hangi bilgiler detaylandırılmaktadır? Donanım envanter içeriğinde yapılan değişiklikler kayıt altına alınmakta mıdır?
3.1.1.3	Donanım Envanterine Kaydedilmemiş Donanımların Yönetimi	Mülakat, Güvenlik Denetimi	Donanım varlık envanterine kaydedilmemiş olan donanımlar kurum ağına nasıl bağlanmaktadır? Donanım envanterinde yer almayan donanımların yönetimi ile ilgili politika/prosedür bulunmakta mıdır? İlgili politika/prosedürler uygulanmakta mıdır?
3.1.1.4	Aktif Keşif Araçlarının Kullanılması	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Kurumda, ağa bağlanılan cihazları tanımak ve donanım envanterindeki değişiklikleri takip etmek amacıyla aktif keşif araçları kullanılmakta mıdır? Aktif keşif araçları ile keşif işlemi en son ne zaman yapılmıştır? Keşif sonuçları nasıl analiz edilmektedir? Keşif sonuçları nasıl saklanmaktadır?
3.1.1.5	DHCP Kayıt Mekanizması ile Yeni Donanımların Tespiti	Mülakat, Güvenlik Denetimi	Kuruma ait DHCP sunucularında kayıt tutulmakta mıdır? Tespit edilen yeni donanımlar, donanım envanterine kontrollü olarak eklenmekte midir? Varsa IP adres yönetimi aracında ilgili kayıt tutulmakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.1.6	Kullanım Ömrünü Tamamlayan Cihazların Veri Depolama Üniteleri	Mülakat, Gözden Geçirme	Kullanım ömrünü tamamlayan cihazların imha edilmesine veya tekrar kullanılmasına yönelik bir politika/prosedür tanımlanmış mıdır? İlgili politika/prosedür uygulanmakta mıdır? Cihazların veri depolama ünitelerini güvenli silmek amacıyla hangi yöntemler kullanılmaktadır? Kullanım ömrünü tamamlayan cihazların veri depolama ünitelerini imha etmek için hangi yöntemler kullanılmaktadır?
3.1.1.7	Kurum Ağı Bağlantı Noktalarında Kimlik Denetimi Yapılması	Mülakat, Sızma Testi	Port seviyesinde erişim kontrolü yapılmakta mıdır? Kurum ağına bağlanan cihazlar için 802.1x veya NAC çözümleri kullanılarak kimlik denetimi yapılmakta mıdır?
3.1.1.8	Donanım Varlıklarının Kimlik Denetimi için İstemci Sertifikalarının Kullanılması	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Kuruma ait güvenli ağlara bağlanan hangi donanımlar için istemci sertifikası ile kimlik doğrulaması yapılmaktadır? Sertifika, yetkilendirilmiş personel tarafından güvenli bir alanda oluşturulmakta mıdır? Sertifikanın anahtar uzunluğu, tipi (NES/NES olmayan) ve oluşturulma yöntemi seçilirken bilgi güvenliği gereksinimleri dikkate alınmakta mıdır? Oluşturulan sertifika güvenli alanda saklanmakta mıdır? Sertifika yaşam döngüsünün takibi yapılmakta mıdır?
3.1.1.9	Sabit Disk Güvenliği	Mülakat, Gözden Geçirme	Kurum tarafından temin edilen ve kullanıcı bilgisayarlarında kullanılması planlanan sabit diskleri sisteme dâhil etmek amacıyla bir süreç tanımlanmış ve uygulanmakta mıdır? Temin edilen sabit diskler, sisteme dâhil edilmeden önce hangi güvenli silme işlemlerine tabi tutulmaktadır?

3.1.2. Yazılım Varlıklarının Envanter Yönetimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.2.1	1	Yazılım Envanterinin Yönetimi	Kurumda kullanılan tüm yazılımların (işletim sistemleri, donanım yazılımları, üçüncü parti yazılımlar, uygulama yazılımları vb.) güncel bir listesi tutulmalı ve listeye yalnızca yetkilendirilmiş personelin erişimi mümkün kılınmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.2.2	1	Yazılım Envanter İçeriğinin Yönetimi	Yazılım envanter yönetim araçlarında, kurum tarafından yetkilendirilen işletim sistemleri dâhil olmak üzere en az; yazılımların adı, sürümü, yayımcısı, destek alınan tedarikçi sözleşme bilgileri (bakım süresi, kapsamı vb.), lisans bilgileri ve edinim tarihi bilgileri, yazılımın yüklendiği donanımlar kayıt altına alınmalı ve izlenebilir olmalıdır. Yazılım envanter içeriğinde yapılan değişiklikler kayıt altına alınmalıdır.
3.1.2.3	1	Yazılımın Üreticisi Tarafından Desteklenmesi	Kurumun onaylı yazılım envanterine yalnızca üreticisi tarafından desteklenen yazılımlar dâhil edilmelidir. Yazılım envanterinde kayıtlı olan yazılımlar için güncelleme desteği devamlılığı sağlanmalıdır. Üreticisi tarafından sunulan destek hizmeti sona ermiş ancak iş gereksinimleri sebebi ile kullanılması gereken yazılımlar, yazılım envanterinde "üretici tarafından desteklenmeyen" olarak etiketlenmelidir.
3.1.2.4	1	Yazılım Envanterine Kaydedilmemiş Yazılımların Yönetimi	Kurum tarafından onaylanmayan yazılımların kullanılmasına yönelik politika ve prosedürler oluşturulmalı ve uygulanmalıdır.
3.1.2.5	2	Yazılım Envanteri Yönetim Araçlarının Kullanımı	Kurum sistemlerindeki tüm yazılımlar için envanter yönetim araçları kullanılmalıdır. Söz konusu envanter yönetim araçları, yazılımların mevcut durumları ile ilgili raporlama yeteneğine sahip olmalıdır.
3.1.2.6	3	Yazılım ve Donanım Envanterinin Entegre Edilmesi	Yazılım ve donanım envanteri birbirleri ile entegre edilmelidir. Entegre edilen envanter merkezi olarak yönetilmelidir.
3.1.2.7	3	Beyaz Liste Yönetimi	Kurum uygulama beyaz liste yönetimi yazılımı kullanmalıdır. Uygulama tarafından en az aşağıda yer alan kısıtlamalar devreye alınmalıdır. Yalnızca onaylı yazılım kütüphanelerinin (* .dll, * .ocx, * .so vb.) yüklenmesi Yalnızca onaylı ve dijital olarak imzalanmış betik dosyalarının (* .ps1, * .py, makrolar vb.) çalıştırılması.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.2.1	Yazılım Envanterinin Yönetimi	Mülakat, Gözden Geçirme	Kurum bünyesinde detaylı ve güncel bir yazılım envanteri tutulmakta mıdır? Envanter yönetim süreci tanımlanmış mıdır? Yazılım envanterine hangi personelin erişim yetkisi bulunmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.2.2	Yazılım Envanter İçeriğinin Yönetimi	Mülakat, Gözden Geçirme	Yazılım envanterinde yazılımlara ait isim, versiyon, lisans bilgileri ve edinim tarihi gibi bilgiler tutulmakta mıdır? Yazılım envanterinde, yazılımların yüklü olduğu donanım veya sanallaştırma ortamının kaydı tutulmakta mıdır? Yazılım envanter içeriğinde yapılan değişiklikler kayıt altına alınmakta mıdır?
3.1.2.3	Yazılımın Üreticisi Tarafından Desteklenmesi	Mülakat, Gözden Geçirme	Kurumda kullanılan yazılımların üretici tarafından desteklendiği takip edilmekte midir? Desteklenmeyen yazılımlar envanterde yer almakta mıdır? Desteklenmeyen yazılımlar envanterde nasıl etiketlenmektedir?
3.1.2.4	Yazılım Envanterine Kaydedilmemiş Yazılımların Yönetimi	Mülakat, Gözden Geçirme	Kurum tarafından onaylanmayan yazılımların kullanımı ile ilgili süreç ve sistem bulunmakta mıdır?
3.1.2.5	Yazılım Envanteri Yönetim Araçlarının Kullanımı	Mülakat, Gözden Geçirme	Kurumda kullanılan yazılımların envanterini otomatik olarak oluşturmak için hangi yazılım envanter araçları kullanılmaktadır? Kullanılan yazılım envanteri yönetim aracı hangi özelliklere sahiptir?
3.1.2.6	Yazılım ve Donanım Envanterinin Entegre Edilmesi	Mülakat, Gözden Geçirme	Yazılım envanter sistemi ve donanım envanter sistemi entegre midir?
3.1.2.7	Beyaz Liste Yönetimi	Mülakat, Güvenlik Denetimi, Sızma Testi	Uygulama beyaz liste yönetimi için yazılım kullanılmakta mıdır? Beyaz liste yazılımı, *.dll, *.ocx gibi sadece onaylı kütüphanelerin yüklenmesine ya da *.ps1, *.py gibi sadece onaylı betiklerin çalışmasına olanak sağlamakta mıdır?

3.1.3. Tehdit ve Zafiyet Yönetimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.3.1	1	Yazılım Güncelleme Araçlarının Kullanımı	Tüm sistemlerdeki yazılımların, mevcut iş gereksinimlerini karşılayacak ve yazılım üreticisi tarafından sağlanan en kararlı ve güncel güvenlik sürümleri ile çalıştırılmakta olduğu otomatik yazılım güncelleme araçları kullanılarak kontrol edilmelidir. Otomatik yazılım güncelleme araçlarının kullanılamadığı durumlarda uzman personel tarafından manuel olarak gerekli kontroller periyodik olarak yapılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.3.2	1	Zararlı Yazılımların Engellenmesi	Zararlı yazılımların kuruma ait ve/veya kurum tarafından yönetilen kullanıcı uç nokta cihazları ve altyapı bileşenleri üzerinde çalışmasını, kaydedilmesini ve aktarılmasını engellemek için politikalar/prosedürler tanımlanmalı ve işletilmelidir. Personelin beyaz listede bulunan uygulamalar haricinde uygulama kurmasının engellenmesine yönelik politika/prosedür oluşturulmalıdır. Politika/prosedürün uygulanmasını temin etmek üzere gerekli teknolojik altyapılar ve uyarı mekanizmaları aktif edilmelidir.
3.1.3.3	1	Zafiyet/Yama Yönetimi	Kurumsal uygulamaların, kurum ağının ve sistem bileşenlerinin güvenlik açıklarının zamanında tespit edilmesi için uygulanacak politikalar ve süreçler tanımlanmalıdır. Zafiyet ve yama yönetimine ilişkin değişiklikler, tanımlanmış değişiklik yönetimi süreci üzerinden kontrollü olarak gerçekleştirilmelidir.
3.1.3.4	1	Yüksek ve Üzeri Seviyede Zafiyet İçeren Sunucu/Uygulamaların Yalıtılması	Yüksek ve üzeri seviyede zafiyet barındıran sunucu ve uygulamalar, diğer sistemlerden fiziksel ya da mantıksal olarak izole edilmelidir. İzolasyon yapılamadığı durumlarda söz konusu sunucu ve uygulamalarda katmanlı güvenlik prensibine uygun şekilde güvenliğin artırılması sağlanmalıdır.
3.1.3.5	1	Son Kullanıcıların Yetkisiz Program Ekleme/Kaldırma İşlemlerinin Engellenmesi	Son kullanıcıların, güvenlik sıkılaştırmaları kapsamında kurum tarafından uygulanması gerekli görülen konfigürasyonlara müdahale etmemesi ve beyaz listede bulunan programlar haricinde program kurmalarının engellenmesi için son kullanıcı hesaplarının yerel yönetici yetkileri kaldırılmalıdır. Bk. Tedbir No: 5.1.3.4
3.1.3.6	1	Güvenlik Açıkları için Risk Analizi Tabanlı Önceliklendirme	Tespit edilen güvenlik açıklarının giderilmesi için hazırlanan aksiyon planına yönelik önceliklendirme risk analizi tabanlı yapılmalıdır.
3.1.3.7	1	Güvenlik Sıkılaştırmalarının Yapılması	Kurumsal uygulamalar (web, DNS, e-posta, FTP vb. ile diğer uygulamalar) ve kurum ağındaki bileşenler, işletim sisteminin ve paket yazılımların kurulumuyla gelen varsayılan güvenlik ayarlarıyla kullanılmamalıdır. Kullanıma alınmadan önce bilgi güvenliği gereksinimleri dikkate alınarak gerekli güvenlik sıkılaştırmaları yapılmalıdır. Bk. Bölüm 5
3.1.3.8	2	İşletim Sistemi Yama Yönetimi Araçlarının Kullanımı	Güvenlik güncellemeleri başta olmak üzere işletim sistemlerine yönelik güncellemelerin ve yamaların üreticisi tarafından bildirilen en kararlı, güncel ve güvenilir sürüm dikkate alınarak yapıldığı, otomatik yazılım güncelleme araçları ile kontrol edilmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.3.9	2	Zafiyet Tarama Araçlarının Kullanımı	Kurum ağında yer alan tüm sistemler (test sistemleri de dâhil olmak üzere) güvenlik içeriği otomasyon protokolü (SCAP) uyumlu güvenlik zafiyeti tarama aracı kullanılarak periyodik olarak taranmalıdır. Güvenlik taramaları için oluşturulan hesaplar farklı bir amaç için kullanılmamalı, en az yetki ve bilmesi gereken prensibi doğrultusunda yetkilendirme yapılarak ilgili erişim kayıtları tutulmalıdır. Güvenlik taramaları için oluşturulan hesaplar düzenli olarak kontrol edilmeli ve izlenmelidir. Zafiyet tarama araçları, güvenlik açıklarına yönelik yapılan doğrulama faaliyetleri öncesi ve sonrası durumu içerecek şekilde raporlama yapmalıdır. Üretilen raporların güvenliği sağlanmalı ve raporlara sadece yetkili personel erişim sağlamalıdır.
3.1.3.10	2	Aktif Portların, Servislerin ve Protokollerin Varlık Envanterinde Tutulması	Aktif bağlantı portları, servisler ve protokoller donanım ve yazılım varlık envanterinde yer alan varlıklar ile eşleştirilmelidir. Kurum sistemlerinin tümünü kapsayacak şekilde port, servis ve protokol taramaları gerçekleştirilmeli, açık ve kullanımına ihtiyaç olmayan portların tespit edilmesi durumunda alarm üreten mekanizmalar devreye alınmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.3.1	Yazılım Güncelleme Araçlarının Kullanımı	Mülakat, Güvenlik Denetimi	Kurumda kullanılan yazılımların güvenlik güncellemeleri zamanında yapılmakta mıdır? Bu güncellemelerin devreye alınıp alınmadığı, yazılım güncelleme araçları vasıtasıyla otomatik olarak kontrol edilmekte midir? Yazılım güncelleme araçlarının kullanılmadığı durumlarda güncellemelere yönelik kontroller nasıl yapılmaktadır?
3.1.3.2	Zararlı Yazılımların Engellenmesi	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Zararlı yazılımların engellenmesi ve beyaz liste denetim yöntemi için nasıl bir süreç işletilmektedir? Beyaz liste nasıl oluşturulmuştur? Kullanıcıların yazılım yükleme yetkisi var mıdır? Kurum bilgi sistemleri altyapısında zararlı yazılımları engellemek için hangi mekanizma/yöntemler kullanılmaktadır? Kurum bilgi sistemleri altyapı bileşenlerinde hangi sıkılaştırma önlemleri devreye alınmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.3.3	Zafiyet/Yama Yönetimi	Mülakat, Gözden Geçirme	Zafiyet ve yama yönetimine ilişkin politikalar/süreçler tanımlanmış mıdır? İlgili politika/süreçler işletilmekte midir? Zafiyet ve yama yönetimine ilişkin değişiklikler nasıl ele alınmaktadır?
3.1.3.4	Yüksek ve Üzeri Seviyede Zafiyet İçeren Sunucu/Uygulamaların Yalıtılması	Mülakat, Güvenlik Denetimi	Yüksek ve üzeri seviyede zafiyet içeren sunucu ve uygulamalar diğer sistemlerden fiziksel ve/veya mantıksal olarak izole edilmekte midir? Yüksek ve üzeri seviyede zafiyet içeren sunucu ve uygulamaların diğer sistemlerden fiziksel ve/veya mantıksal olarak izole edilememesi durumunda hangi önlemler alınmaktadır?
3.1.3.5	Son Kullanıcıların Yetkisiz Program Ekleme/Kaldırma İşlemlerinin Engellenmesi	Mülakat, Güvenlik Denetimi	Program ekleme, kaldırma ve konfigürasyon işlemleri nasıl yapılmaktadır? Yerel yönetici hakkına sahip olan hesaplar nasıl yönetilmektedir?
3.1.3.6	Güvenlik Açıkları için Risk Analizi Tabanlı Önceliklendirme	Mülakat, Gözden Geçirme	Tespit edilen güvenlik açıklarının giderilmesi ile ilgili aksiyon planlamaları kapsamında önceliklendirme nasıl yapılmaktadır?
3.1.3.7	Güvenlik Sıkılaştırmalarının Yapılması	Mülakat, Güvenlik Denetimi, Sızma Testi	Güvenli olarak kabul edilmeyen ve/veya varsayılan konfigürasyon ile çalışan kurumsal uygulama var mıdır? Kurumsal uygulamaları ve kurum ağındaki diğer bileşenleri devreye alma sürecinde nasıl bir sıkılaştırma süreci izlenmektedir?
3.1.3.8	İşletim Sistemi Yama Yönetimi Araçlarının Kullanımı	Mülakat, Güvenlik Denetimi	Kurumda kullanılan işletim sistemlerinin kritik güvenlik güncellemeleri/yamaları zamanında yapılmakta mıdır? Bu güncellemeler/yamalar yazılım güncelleme araçları vasıtasıyla otomatik olarak takip edilmekte midir?
3.1.3.9	Zafiyet Tarama Araçlarının Kullanımı	Mülakat, Güvenlik Denetimi	Kurumdaki sistemler düzenli olarak zafiyet taramalarından geçirilmekte midir? Güvenlik taramaları için oluşturulan hesaplar taramalar dışında başka faaliyetler için kullanılmakta mıdır? Bu hesapların yetkileri sadece belirli IP adreslerinden gerekli makinelere bağlanabilecek şekilde kısıtlanmış mıdır? Bu hesaplar düzenli olarak kontrol edilmekte midir? Geçmişte tespit edilen zafiyetlerin giderilip giderilmediği sonraki taramalarda kontrol edilmekte midir? Zafiyet tarama raporları nasıl muhafaza edilmektedir?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.3.10	Aktif Portların, Servislerin ve Protokollerin Varlık Envanterinde Tutulması	Mülakat, Güvenlik Denetimi, Sızma Testi	Aktif bağlantı portları, servisleri ve protokolleri varlık envanterindeki donanım ve yazılım varlıklarıyla eşleştirilmekte midir? Kuruma ait sistemlerde kullanımına ihtiyaç olmayan ve onaylanmamış servislerin, port ve protokollerin çalışıp çalışmadığı kontrol edilmekte midir? Kullanımına ihtiyaç olmayan portların tespiti için düzenli tarama yapılmakta mıdır?

3.1.4. E-Posta Sunucusu ve İstemcisi Güvenliği

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.4.1	1	Tekrar Yayınlama (Relay) İşleminin Engellenmesi	Tekrar yayınlama (relay) işlemine, belirlenen IP adresleri dışında izin verilmemeli ve e-posta hizmet protokollerinden kullanılmayanlar kapatılmalıdır.
3.1.4.2	1	SMTP Kimlik Doğrulaması Kullanımı	E-posta gönderiminde kullanıcı adı ve parola kullanılarak kimlik doğrulaması yapılmalıdır.
3.1.4.3	1	Kurum Tarafından Onaylanan İnternet Tarayıcıları ve E-Posta İstemcilerinin Kullanımı	Kurum tarafından onaylanmış, üretici tarafından desteği devam eden kararlı ve güncel sürüme sahip internet tarayıcıları ile e-posta istemcileri kullanılmalıdır.
3.1.4.4	1	E-posta İçeriğindeki Zararlı Bağlantılara (URL) Erişimin Engellenmesi	E-posta içeriğindeki zararlı bağlantılara erişim engellenmelidir.
3.1.4.5	1	İstenmeyen E-posta (Spam) Koruması	Spam e-postaları engellemek üzere DNS tabanlı filtreleme ve kara liste yöntemleri uygulanmalıdır.
3.1.4.6	1	Servis Dışı Bırakma Saldırıları (DoS) Koruması	E-posta bombardımanı ve bağlantı temelli servis dışı bırakma saldırılarına karşı SMTP sunucusunda bağlantı sayısı sınırlama vb. yöntemler ile koruma sağlanmalıdır.
3.1.4.7	1	E-posta İçerik Kontrollerinin Yapılması	Gelen/giden tüm e-posta hesaplarına ait içerikler, istenmeyen e-postalar ve e-posta ile yayılabilecek zararlı yazılımlara karşı güvenliği sağlamak amacıyla SMTP Gateway vb. sistemler kullanılarak kontrol edilmelidir.
3.1.4.8	1	Sahte ya da Değiştirilmiş E-Postaların Engellenmesi	Sahte ya da bütünlüğü bozulmuş e-postaların geçerli etki alanlarına sızma ihtimalini azaltmak için SPF, DKIM vb. teknoloji ve standartlar kullanılmalıdır.
3.1.4.9	1	Risk İçeren İzinsiz ve/veya Çalıştırılabilir Dosya Türlerinin Engellenmesi	Kurum politikaları ile belirlenmiş olan risk içeren izinsiz ve/veya çalıştırılabilir dosya türleri içeren e-posta veya e-posta ekleri engellenmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.4.10	1	Zararlı Yazılımdan Korunma Uygulamalarının Kullanılması	Bk. Tedbir No: 3.1.5.1
3.1.4.11	1	Güvenlik Sıkılaştırmalarının Yapılması	E-posta sunucuları, varsayılan ayarlarıyla kullanılmamalı ve kullanıma alınmadan önce tüm sunucuların güvenlik sıkılaştırmaları yapılmalıdır. Bk. Bölüm 5
3.1.4.12	1	E-Posta İletişim Güvenliğinin Sağlanması	İstemci ve e-posta sunucuları arasındaki iletişimde bilinen zafiyet içermeyen güvenilir SSL/TLS sürümleri ile birlikte güvenli e-posta iletişim protokolleri (SMTPs, POP3s, IMAPs, HTTPs vb.) kullanılmalıdır. Bk. Tedbir No: 3.2.9.1
3.1.4.13	1	E-Posta Sunucu Mimarisi	E-posta sunucuları internetten gelebilecek her türlü saldırıları önlemek üzere katmanlı güvenlik tasarımı prensiplerine göre yapılandırılmalıdır.
3.1.4.14	1	Üçüncü Taraflardan Temin Edilen E-Posta Hizmetleri	Üçüncü taraflardan temin edilen e-posta hizmetlerinin güvenliği garanti altına alınmalıdır. Bk. Bölüm 4.3
3.1.4.15	2	Onaylı İnternet Tarayıcısı ve E-Posta İstemcisi Eklentilerinin Kullanımı	Sadece kurum tarafından onaylı internet tarayıcısı ve e-posta istemcisi eklentileri kullanılmalıdır.
3.1.4.16	2	E-Posta İstemcilerinde Betik Kodlarının Kullanımını Sınırlama	E-posta istemcilerinde sadece kurum tarafından izin verilen betik kodları çalıştırılmalıdır.
3.1.4.17	2	E-Posta Alışverişlerinin Şifreli ve İmzalı Yapılması	Kurum politikalarına göre gizlilik dereceli bilgi/veri içeren e-posta alışverişleri şifreli ve imzalı olarak yapılmalıdır. E-posta alışverişleri şifreli ve imzalı olarak yapıldığı durumda kullanılan sertifikalar kuruma özel olarak üretilmelidir.
3.1.4.18	2	E-Posta Sunucularına Uzaktan Erişim	E-posta sunucularına uzaktan yapılacak erişimlerde çok faktörlü kimlik doğrulama mekanizmaları kullanılmalıdır.
3.1.4.19	3	E-Posta Eklerinin Kum Havuzlarında Çalıştırılması	Kuruma dışarıdan gelen e-posta ekleri çok katmanlı güvenlik analizinden (içerik analizi, beyaz liste/kara liste, imza tabanlı anti-virüs, anti-malware taramaları vb.) geçirilmelidir. Bu aşamadan sonra hala kategorilendirilmemiş e-posta ekleri kum havuzunda çalıştırılmalıdır. Kum havuzu çözümlerinde dosyalar yurt içinde yerleşik olan sunucularda taranmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.4.1	Tekrar Yayınlama (Relay) İşleminin Engellenmesi	Mülakat, Güvenlik Denetimi	E-posta tekrar yayınlama (relay) işlemine belirli IP adresleri dışında izin verilmekte midir? İzin verilen IP adreslerinden oluşan liste düzenli olarak kontrol edilmekte ve güncellenmekte midir? E-posta hizmet protokollerinden kullanılmayanlar kapatılmakta mıdır?
3.1.4.2	SMTP Kimlik Doğrulaması Kullanımı	Mülakat, Güvenlik Denetimi	E-posta gönderiminde kimlik doğrulaması yapılmakta mıdır?
3.1.4.3	Kurum Tarafından Onaylanan İnternet Tarayıcıları ve E-Posta İstemcilerinin Kullanımı	Mülakat, Güvenlik Denetimi	Kurumda kullanılan internet tarayıcıları ve e-posta istemcileri üretici tarafından desteklenmekte midir? Üretici tarafından desteği devam eden internet tarayıcıları ve e-posta istemcileri harici yazılımların kullanılması gerektiği durumlar nasıl yönetilmektedir?
3.1.4.4	E-Posta İçeriğindeki Zararlı Bağlantılara (URL) Erişimin Engellenmesi	Güvenlik Denetimi	Zararlı bağlantılara erişimi engellemek için hangi önlemler alınmaktadır?
3.1.4.5	İstenmeyen E-Posta (Spam) Koruması	Güvenlik Denetimi	Spam e-postaları engellemek üzere DNS tabanlı filtreleme ve kara liste kullanılmakta mıdır?
3.1.4.6	Servis Dışı Bırakma Saldırıları (DoS) Koruması	Güvenlik Denetimi	E-posta bombardımanı ve bağlantı temelli servis dışı bırakma saldırıları nasıl engellenmektedir?
3.1.4.7	E-Posta İçerik Kontrollerinin Yapılması	Güvenlik Denetimi	Gelen/giden tüm e-posta içerikleri nasıl kontrol edilmektedir?
3.1.4.8	Sahte ya da Değiştirilmiş E-Postaların Engellenmesi	Mülakat, Güvenlik Denetimi	Sahte ya da bütünlüğü bozulmuş e-postaların geçerli etki alanlarına sızma ihtimalini azaltmak için hangi kontroller uygulanmaktadır?
3.1.4.9	Risk İçeren İzinsiz ve/veya Çalıştırılabilir Dosya Türlerinin Engellenmesi	Mülakat, Güvenlik Denetimi	İzinsiz ve/veya çalıştırılabilir dosya türleri içeren e-posta eklerine yönelik hangi kontroller uygulanmaktadır?
3.1.4.10	Zararlı Yazılımdan Korunma Uygulamalarının Kullanılması	Mülakat, Güvenlik Denetimi	Bk. Denetim No: 3.1.5.1
3.1.4.11	Güvenlik Sıkılaştırmalarının Yapılması	Mülakat, Sızma Testi	E-posta sunucularına yönelik hangi güvenlik sıkılaştırma çalışmaları yapılmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.4.12	E-Posta İletişim Güvenliğinin Sağlanması	Güvenlik Denetimi, Sızma Testi	İstemci ve e-posta sunucuları arasındaki iletişimde hangi protokoller kullanılmaktadır?
3.1.4.13	E-Posta Sunucu Mimarisi	Mülakat, Gözden Geçirme, Güvenlik Denetimi	E-posta sunucu yapılandırmaları kapsamında katmanlı güvenlik tasarımı prensipleri dikkate alınmakta mıdır?
3.1.4.14	Üçüncü Taraflardan Temin Edilen E-Posta Hizmetleri	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Üçüncü taraflardan temin edilen e-posta hizmetlerinin güvenliği kapsamında hangi kontroller uygulanmaktadır?
3.1.4.15	Onaylı İnternet Tarayıcısı ve E-Posta İstemcisi Eklentilerinin Kullanımı	Mülakat, Güvenlik Denetimi	Kurum tarafından onaylanmamış internet tarayıcısı ve/veya e-posta istemcisi eklentilerinin kullanılmasını engellemeye yönelik hangi kontroller uygulanmaktadır?
3.1.4.16	E-Posta İstemcilerinde Betik Kodlarının Kullanımını Sınırlama	Mülakat, Güvenlik Denetimi	E-posta istemcilerinde betik kodlarının çalıştırılması sınırlandırılmakta mıdır?
3.1.4.17	E-posta Alışverişlerinin Şifreli ve İmzalı Yapılması	Mülakat, Güvenlik Denetimi, Sızma Testi	Kurum politikalarına göre gizlilik dereceli bilgi/veri içeren e-posta alışverişleri şifreli ve imzalı olarak yapılmakta mıdır? Şifreli ve imzalı e-posta alışverişleri için kullanılan sertifikalar kuruma özel olarak üretilmekte midir?
3.1.4.18	E-Posta Sunucularına Uzaktan Erişim	Mülakat, Güvenlik Denetimi	E-posta sunucularına uzaktan yapılacak erişimler için hangi kontroller uygulanmaktadır?
3.1.4.19	E-Posta Eklerinin Kum Havuzlarında Çalıştırılması	Mülakat, Güvenlik Denetimi	Kuruma dışarıdan gelen e-posta eklerine yönelik hangi güvenlik analizleri yapılmaktadır? İlgili dosyalar nasıl ve nerede taranmaktadır?

3.1.5. Zararlı Yazılımlardan Korunma

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.5.1	1	Zararlı Yazılımdan Korunma Uygulamalarının Kullanılması ve Merkezi Olarak Yönetilmesi	İstemci ve sunucu sistemlerinin tamamında zararlı yazılımdan korunma uygulamaları kullanılmalı ve zararlı yazılımdan korunma uygulamalarında en güncel yama dosyalarının bulunması ve imza veri tabanının güncel olması sağlanmalıdır. Zararlı yazılımdan korunma uygulamalarına ait politikalar merkezi olarak yönetilmelidir.
3.1.5.2	1	Taşınabilir Disklerin Zararlı Yazılım Taramalarından Geçirilmesi	Kurumdaki tüm bilgisayarlar, taşınabilir diskleri otomatik olarak zararlı yazılım taramasından geçirecek şekilde yapılandırılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.5.3	1	Cihazların Otomatik Kod Çalıştırmasına İzin Vermemesi	Kurumdaki tüm bilgisayarlar, taşınabilir ortamlarda otomatik kod çalıştırılmasına izin vermeyecek şekilde yapılandırılmalıdır.
3.1.5.4	1	Zararlı Yazılımdan Korunma Uygulamalarının Yapılandırılması ve Güncel Tutulması	Zararlı yazılımlardan korunma uygulaması üretici veya ilgili kurum tarafından önerilen şekilde yapılandırılmalı ve güncel tutulmalıdır.
3.1.5.5	1	İşletim Sistemlerinin Güvenlik Mekanizmalarının Etkinleştirilmesi	Bk. Tedbir No: 5.1.1.12
3.1.5.6	2	Zararlı Yazılımdan Korunma Uygulamalarına Ait Kayıtların Merkezi Olarak Tutulması	Tüm zararlı yazılım tespitleri, merkezi yönetim ve kayıt sunucularına iletilmelidir.
3.1.5.7	3	DNS Sorgularının Kayıtlarının Tutulması	Zararlı IP adreslerine erişimin denetlenmesi için DNS sorguları kayıt altına alınmalıdır.
3.1.5.8	3	Komut Satırı Kayıtlarının Tutulması	Kurumda, kullanıcı tarafından PowerShell ve Bash gibi komut satırı kullanılarak yapılan işlemler denetlenmeli ve merkezi olarak kayıt altına alınmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.5.1	Zararlı Yazılımdan Korunma Uygulamalarının Kullanılması ve Merkezi Olarak Yönetilmesi	Mülakat, Güvenlik Denetimi	Kurum bünyesinde hangi zararlı yazılımdan korunma uygulamaları kullanılmaktadır? Zararlı yazılımdan korunma uygulamalarına ait politikalar merkezi olarak yönetilmekte midir?
3.1.5.2	Taşınabilir Disklerin Zararlı Yazılım Taramalarından Geçirilmesi	Mülakat, Güvenlik Denetimi	Kurumdaki tüm bilgisayarlar taşınabilir diskleri otomatik olarak zararlı yazılım taramasından geçirecek şekilde yapılandırılmakta mıdır?
3.1.5.3	Cihazların Otomatik Kod Çalıştırmasına İzin Vermemesi	Mülakat, Güvenlik Denetimi	Kurumdaki tüm bilgisayarlar taşınabilir ortamlarda otomatik kod çalıştırılmasına izin vermeyecek şekilde yapılandırılmakta mıdır?
3.1.5.4	Zararlı Yazılımdan Korunma Uygulamalarının Yapılandırılması ve Güncel Tutulması	Mülakat, Güvenlik Denetimi	Kurumda kullanılan zararlı yazılımdan korunma uygulamaları, üreticisi veya ilgili kurum tarafından önerilen şekilde yapılandırılmış mıdır? Yazılımın imza veri tabanı düzenli aralıklarla güncellenmekte midir?
3.1.5.5	İşletim Sistemlerinin Güvenlik Mekanizmalarının Etkinleştirilmesi	Mülakat, Güvenlik Denetimi	Bk. Denetim No: 5.1.1.12

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.5.6	Zararlı Yazılımdan Korunma Uygulamalarına Ait Kayıtların Merkezi Olarak Tutulması	Mülakat, Güvenlik Denetimi	Kurumda tespit edilen zararlı yazılım bilgileri merkezi yönetim ve kayıt sunucularına iletilmekte midir?
3.1.5.7	DNS Sorgularının Kayıtlarının Tutulması	Gözden Geçirme	Kurumda DNS sorguları kayıt edilmekte midir?
3.1.5.8	Komut Satırı Kayıtlarının Tutulması	Gözden Geçirme	Kurumda, PowerShell ve Bash gibi komut satırından yapılan şüpheli işlemler denetlenmekte midir? Bu işlemler merkezi olarak kayıt altına alınmakta mıdır?

3.1.6. Ağ Güvenliği

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.6.1	1	Ağ Topolojisi	Kurum ağlarına ait topolojiler güvenli bir şekilde tutulmalı ve güncelliği kontrol edilmelidir.
3.1.6.2	1	Ağ Cihazlarının Güvenli Konfigürasyonu	Ağ cihazları endüstri standartları, en iyi uygulamalar ve üretici tavsiyelerine uygun olarak yapılandırılmalıdır. Varsayılan parola ve kullanıcı adları değiştirilmelidir. Ağ altyapısındaki cihazlar ağ üzerinden yönetilebilir olmalıdır. Yönetimsel erişimlerde komut satırına, konsol erişimine parola ile giriş sağlanmalıdır. Güvenli protokoller ile yönetimsel işlemler gerçekleştirilmelidir.
3.1.6.3	1	Ağ Cihazlarında Güvenlik Güncellemelerinin Yapılması	Tüm ağ cihazlarında güvenlikle ilgili güncellemelerin üretici tarafından yayımlanan kararlı ve güncel sürümü kullanılmalıdır.
3.1.6.4	1	Kara Liste veya Beyaz Liste Kullanımı	Kara liste veya beyaz liste kullanılarak varlıkların ağ erişimleri sınırlandırılmalıdır.
3.1.6.5	1	İzin Verilmeyen Trafiğin Engellenmesi	Kurum ağ sınırlarından sadece izin verilen kaynaklardan izin verilen hedeflere, izin verilen port ve protokoller ile trafiğin akışı sağlanmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.6.6	1	Ağların İzole Edilmesi	Kablolu ve kablosuz ağlar, bilgi güvenliği gereksinimleri doğrultusunda katmanlara ayrılmalıdır. Yalnızca yetkili sistemlerin, belirli sorumluluklarını yerine getirmek amacıyla gerekli diğer sistemlerle iletişim kurabilmelerini sağlamak için oluşturulan LAN/VLAN'lar arasında erişim denetimi yapılmalıdır. İstemcilerin yer aldığı ağlar ile sunucu/uygulamaların yer aldığı ağlar ayrılmalıdır. Sunucu ağında istemci yer almamalıdır. Yönetimsel işlemler için ayrı yönetim ağları kullanılmalıdır.
3.1.6.7	1	DoS/DDoS Koruması	Kurumun internete açık hizmetleri için olası DoS/DDoS saldırılarına karşı servis dışı kalmasını önlemek, iş sürekliliğini sağlamak amacıyla en az aşağıdaki önlemler alınmalıdır. • Güvenlik ürünleri üzerinde DoS/DDoS saldırılarına özel konfigürasyonların yapılması • DDoS engelleme sistemlerinin sınırları ve yeteneklerinin düzenli aralıklarla test edilmesi ve sürekli iyileştirilmesi/güncellenmesi • DDoS koruma için bir servis sağlayıcıdan hizmet temin edilmiş ise; servis sağlayıcıdan yukarıdaki şartlara göre hizmet verildiğine dair taahhüt alınması, tedarik şartname ve sözleşmelerinde bu hususların belirtilmesi
3.1.6.8	1	İnternet Ortamından Kurum İçi Kaynaklara Erişim	İnternet ortamından kurum içi kaynaklara kontrol dışı erişim engellenmelidir. İnternet ortamından kurum içi kaynaklara erişim gerekli ise VPN teknolojileri kullanılmalıdır. Uzaktan erişimlerin kurum politika ve prosedürlerine uygun olarak, kısıtlı süre ve yetkilerle yapılması sağlanmalıdır.
3.1.6.9	1	Kablosuz Erişim Noktalarının Envanterinin Tutulması	Kurum ağına bağlı yetkili kablosuz erişim noktalarının envanteri tutulmalı ve güncelliği sağlanmalıdır.
3.1.6.10	1	Misafir Ağı Yönetimi	Kurum ağı ile fiziksel ve/veya mantıksal olarak izole edilmiş bir misafir ağı oluşturulmalıdır. Misafirlerin, misafir ağına bağlanmaları öncesinde kimlik bilgilerini doğrulayan mekanizmalar devreye alınmalı ve misafirler tarafından misafir ağı üzerinden yapılan tüm erişimler kayıt altına alınmalıdır. Misafir cihazlarının yalnızca misafir ağına erişimleri mümkün kılınmalıdır.
3.1.6.11	1	Yerel Güvenlik Duvarı Ayarlarının Yapılması	Tüm sunucu ve istemcilerde yerel güvenlik duvarı yapılandırılmalıdır. Bu yapılandırma en az yetki prensibi göz önüne alınarak yapılmalıdır. Yapılandırma varsayılan reddetme (default deny) kuralını içermelidir. Tüm açık portlara ilişkin güvenlik duvarı kuralları yazılmalıdır.
3.1.6.12	1	IP Telefon Kullanımı	IP telefon kullanılması durumunda ilgili sistem, altyapı sağlayıcısı veya kurum tarafından güvenlik duvarları ile korunmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.6.13	1	IP Telefon Sistemlerine Ait İz Kayıtlarının Tutulması	IP telefon sistemlerinin iz kayıtları tutulmalıdır. İlgili kayıtlar düzenli aralıklarla bir sunucuda yedeklenmelidir. Bk. Tedbir No: 3.1.8.1
3.1.6.14	1	IP Telefon Kullanımında Parola Politikası	IP telefon sisteminde kullanılacak parolalar güçlü olmalı ve periyodik olarak güncellenmelidir. Bk. Tedbir No: 3.2.1.8
3.1.6.15	2	Ağ Erişim Denetimleri	Bk. Tedbir No: 3.1.1.7
3.1.6.16	2	Ağ Cihazlarına Ait Yapılandırmaların Dokümante Edilmesi	Kurum ağ cihazlarına ait güvenlik yapılandırmaları; ağ trafiğini düzenleyen kurallara ait tanımlar, kullanılma amacı ve kuralı tanımlayan kişi bilgisi yer alacak şekilde dokümante edilmeli ve güncelliği sağlanmalıdır.
3.1.6.17	2	Ağ Paketlerinin Kaydedilmesi	Kurum tarafından gerekli görülen durumlarda, belirlenen kaynak(lar) ve hedef(ler) arasındaki tüm ağ trafiğinin izlenebilmesi için (pcap vb. formatlarda tüm ağ paketlerinin alınabilmesi) kayıt mekanizmaları oluşturulmalıdır. İhtiyaç duyulması durumunda (güvenlik ihlali, şüpheli ağ trafiği vb.) bu mekanizmalar kullanılarak kurum tarafından belirlenen zaman aralığında ilgili trafik kaydı incelenebilmelidir.
3.1.6.18	2	Ağ Sınır Cihazlarında Kayıt Tutulması	Ağ sınır cihazlarındaki bağlantı trafiği, kullanıcı işlemleri gibi bilgiler kayıt altına alınmalıdır.
3.1.6.19	2	Ağ Tabanlı Saldırı Tespit/Engelleme Sistemi Kullanımı	Saldırıları tespit etmek ve engellemek için ağ tabanlı saldırı tespit ve engelleme sistemleri kullanılmalıdır.
3.1.6.20	2	Uygulama Katmanında Filtreleme Yapılması	İnternetten gelen veya internete giden tüm ağ trafiği, yetkisiz bağlantıları engellemek için uygulama katmanında filtreleme ve kimlik doğrulaması yapılarak iletilmelidir.
3.1.6.21	2	Ağ Tabanlı URL Filtreleri Kullanımı	Kurumdaki sistemlerin, kurum tarafından onaylanmayan ve mevzuat gereği erişimi yasak olan web sitelerine bağlanmasını engelleyen ağ tabanlı URL filtreleri uygulanmalıdır.
3.1.6.22	2	URL Kategori Hizmeti Kullanımı	URL sınıflandırma servisleri kullanılmalıdır. Bu servislerin kullandığı listeler güncel tutulmalıdır. Kategorilendirilmemiş siteler varsayılan olarak engellenmelidir.
3.1.6.23	2	URL'lerin Kayıt Altına Alınması	Potansiyel olarak zararlı etkinlikleri tanımlamak ve saldırıya uğramış sistemlerin belirlenmesine yardımcı olmak için sistemlerden gelen tüm isteklere ait URL'ler kaydedilmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.6.24	2	Kurum Ağına Bağlı Kablosuz Erişim Noktalarının Tespiti	Kurum ağına bağlı yetkisiz kablosuz erişim noktalarının tespit edilmesini ve alarm üretilmesini sağlayan ağ tabanlı keşif araçları kullanılmalıdır.
3.1.6.25	2	İstemcilerin Kablosuz Ağ Erişimlerinin Sınırlandırılması	İstemciler, iş gereksinimleri doğrultusunda yalnızca yetkilendirilmiş kablosuz ağlara erişim sağlamalıdır.
3.1.6.26	2	Eşler Arası Kablosuz Ağ Erişiminin Engellenmesi	Eşler arası (Peer to Peer) kablosuz ağ erişimine olanak sağlayan yöntemler (ad hoc yöntemi vb.) engellenmelidir.
3.1.6.27	2	Kablosuz Çevre Birimleri Aracılığı ile Yapılan Erişimin Engellenmesi	Cihazların, kablosuz çevre birimleri aracılığı ile yapacakları yetkisiz erişimler (bluetooth, NFC vb.) engellenmelidir.
3.1.6.28	2	Uygulama Seviyesi Saldırıların Engellenmesi	Kurum ağının uygulama seviyesi saldırılara karşı korunması için gerekli yapılar (WAF, IPS, DDoS vb.) uygun şekilde konumlandırılmalı, test edilmeli ve sürekli iyileştirilmelidir. Bu amaçla bir servis sağlayıcıdan hizmet temin edilmiş ise; servis sağlayıcıdan yukarıdaki şartlara göre hizmet verildiğine dair taahhüt alınmalı, tedarik şartname ve sözleşmelerinde bu hususlar belirtilmelidir.
3.1.6.29	2	IP Telefon Erişim Kontrol Listeleri	IP telefon sistemlerinde erişim kontrol listeleri kullanılmalı ve kimlik sahteciliği saldırılarına karşı önlem alınmalıdır.
3.1.6.30	3	Ağ Cihazlarının Yapılandırma Yönetimi	Ağ cihazı mevcut yapılandırmaları, onaylanmış ve olması gereken güvenlik yapılandırma içerikleri ile karşılaştırılmalı ve herhangi bir uyumsuzluk tespit edildiğinde alarm üreten mekanizmalar devreye alınmalıdır.
3.1.6.31	3	Ağ Cihazlarının Yönetimi	Ağ cihazlarının yönetimi, çok faktörlü kimlik doğrulama mekanizmaları kullanılarak şifreli ağ trafiği üzerinden yapılmalıdır. Ağ yönetimi için gerekli işlemler, bu amaç için tahsis edilen ve internet erişimi olmayan makineler üzerinden yapılmalıdır.
3.1.6.32	3	Kuruma Uzaktan Bağlanan Cihazların Yönetimi	Kuruma uzaktan bağlanacak cihazların; zararlı yazılımdan korunma, işletim sistemi ve uygulama güncelliği vb. hususlar kapsamında kurum politikalarına uygunluğu güvenli uzaktan bağlantı sağlayan sistemler üzerinden (VPN vb.) kontrol edilmelidir. Kurum politikasına uymayan cihazlara bağlantı izni verilmemelidir.
3.1.6.33	3	Kripto Ağ Cihazlarının Kullanımı	Kritik ağ ortamları arasındaki iletişim için kripto ağ cihazları kullanılmalıdır.
3.1.6.34	3	Kablosuz İletişim Güvenliği	Kritik veri kablosuz ağ üzerinde taşınırken çok faktörlü kimlik doğrulaması gerektiren kimlik doğrulama protokollerinin (EAP/TLS vb.) bilinen zafiyet içermeyen güvenilir sürümleri kullanılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.6.35	3	Kablosuz Çevre Birimleri Kullanımının Engellenmesi	Kritik veri işleyen, internete herhangi bir erişimi bulunmayan kapalı ağlarda kablosuz fare ve klavye gibi çevre birimlerinin kullanılması engellenmelidir.
3.1.6.36	3	Veri Transferi	Düzenli veri aktarımı ihtiyacı bulunan kritik seviyeli ağlarda veri diyotu, hava boşluğu şeklinde çalışan güvenli aktarım yöntemleri üzerinden tek yönlü veri aktarımı yapılmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.6.1	Ağ Topolojisi	Gözden Geçirme	Kurum ağlarına ait topolojiler tutulmakta mıdır? Kurum ağlarının fiziksel ve mantıksal topolojileri dokümante edilmekte midir? Mevcut donanım ve yazılım envanteri ile ağ topolojileri eşleşmekte midir?
3.1.6.2	Ağ Cihazlarının Güvenli Konfigürasyonu	Mülakat, Güvenlik Denetimi, Sızma Testi	Ağ cihazları endüstri standartları, en iyi uygulamalar ve üretici tavsiyelerine uygun olarak yapılandırılmakta mıdır? Varsayılan parola ve kullanıcı adları kullanılmakta mıdır? Ağ altyapısındaki cihazların tamamı ağ üzerinden yönetilebilmekte midir? Komut satırı ve konsol erişimi nasıl sağlanmaktadır? Cihazların yönetimi nasıl yapılmaktadır? Cihazlara nasıl erişim sağlanmaktadır?
3.1.6.3	Ağ Cihazlarında Güvenlik Güncellemelerinin Yapılması	Mülakat, Güvenlik Denetimi	Ağ cihazları üzerinde üretici tarafından yayımlanmış kararlı ve güncel sürümlerin kullanıldığına dair kontroller nasıl yapılmaktadır?
3.1.6.4	Kara Liste veya Beyaz Liste Kullanımı	Mülakat, Güvenlik Denetimi	IP/MAC adresleri ve/veya TCP/UDP portları için beyaz liste/kara liste yapısı kullanılmakta mıdır?
3.1.6.5	İzin Verilmeyen Trafiğin Engellenmesi	Mülakat, Güvenlik Denetimi	Kurum ağ sınırlarından akan trafiğin erişim denetimi nasıl sağlanmaktadır?
3.1.6.6	Ağların İzole Edilmesi	Mülakat, Güvenlik Denetimi	Kurum ağları, bilgi güvenliği gereksinimleri doğrultusunda katmanlara ayrılmakta mıdır? Kurum ağlarına yönelik erişim denetimi nasıl yapılmaktadır? Sunucuların bulunduğu ağlar ile istemcilerin bulunduğu ağlar birbirinden ayrılmakta mıdır? Yönetimsel işlemler için ayrı yönetim ağları kullanılmakta mıdır?
3.1.6.7	DoS/DDoS Koruması	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Kurumun internete açık hizmetleri için olası DoS/DDoS saldırılarını engellemek amacıyla hangi önlemler alınmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.6.8	İnternet Ortamından Kurum İçi Kaynaklara Erişim	Mülakat, Güvenlik Denetimi	İnternet ortamından kurum içi kaynaklara erişilmekte midir? İnternet ortamından kurum içi kaynaklara erişim için VPN teknolojileri kullanılmakta mıdır?
3.1.6.9	Kablosuz Erişim Noktalarının Envanterinin Tutulması	Mülakat, Gözden Geçirme	Kurum ağına bağlı yetkili kablosuz erişim noktalarının envanteri tutulmakta mıdır? Envanter içeriğinde hangi bilgiler yer almaktadır?
3.1.6.10	Misafir Ağı Yönetimi	Mülakat, Güvenlik Denetimi	Kurum ağı ile fiziksel ve/veya mantıksal olarak izole edilmiş bir misafir ağı oluşturulmuş mudur? Misafirlerin, misafir ağına bağlanmaları öncesinde kimlik bilgilerini doğrulayan mekanizmalar devreye alınmış mıdır?
3.1.6.11	Yerel Güvenlik Duvarı Ayarlarının Yapılması	Mülakat, Güvenlik Denetimi	Kurum sunucu ve istemcilerinde güvenlik duvarı kullanılmakta mıdır? İzin verilenler dışındaki tüm bağlantılar varsayılan olarak reddedilmekte midir?
3.1.6.12	IP Telefon Kullanımı	Mülakat, Güvenlik Denetimi	Sistem güvenlik duvarlarıyla korunmakta mıdır? Erişim kısıtlaması yapılmış mıdır?
3.1.6.13	IP Telefon Sistemlerine Ait İz Kayıtlarının Tutulması	Mülakat, Güvenlik Denetimi	IP telefon sistemlerine ait iz kayıtları tutulmakta mıdır? İlgili kayıtlar düzenli aralıklarla yedeklenmekte midir? Alınan iz kayıtları hangi bilgileri içermektedir?
3.1.6.14	IP Telefon Kullanımında Parola Politikası	Mülakat, Güvenlik Denetimi	IP telefon sisteminde kullanılacak parolalar için nasıl bir politika tanımlanmıştır? Parolalar periyodik olarak yenilenmekte midir?
3.1.6.15	Ağ Erişim Denetimleri	Mülakat, Güvenlik Denetimi	Bk. Denetim No: 3.1.1.7
3.1.6.16	Ağ Cihazlarına Ait Yapılandırmaların Dokümante Edilmesi	Mülakat	Kurum ağ cihazlarına ait güvenlik yapılandırmaları hangi bilgileri içerecek şekilde dokümante edilmektedir? Kurum ağ cihazlarına ait yapılandırmalar için güncellik kontrolü nasıl yapılmaktadır?
3.1.6.17	Ağ Paketlerinin Kaydedilmesi	Mülakat	Kurum tarafından gerekli görülen durumlarda, belirlenen kaynak(lar) ve hedef(ler) arasındaki ağ trafiğinin izlenebilmesi için kayıt mekanizmaları oluşturulmuş mudur?
3.1.6.18	Ağ Sınır Cihazlarında Kayıt Tutulması	Mülakat	Kurum bünyesinde yer alan ağ sınır cihazlarına ait hangi bilgiler kayıt altına alınmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.6.19	Ağ Tabanlı Saldırı Tespit/Engelleme Sistemi Kullanımı	Mülakat, Güvenlik Denetimi	Ağ tabanlı saldırı tespit ve engelleme sistemleri kullanılmakta mıdır?
3.1.6.20	Uygulama Katmanında Filtreleme Yapılması	Mülakat, Güvenlik Denetimi	İnternetten gelen veya internete giden tüm ağ trafiği, yetkisiz bağlantıları engellemek amacıyla uygulama katmanında filtreleme ve kimlik doğrulaması yapılarak iletilmekte midir?
3.1.6.21	Ağ Tabanlı URL Filtreleri Kullanımı	Mülakat, Sızma Testi	Kurumda tüm sistemler için ağ tabanlı URL filtreleme yapılmakta mıdır?
3.1.6.22	URL Kategori Hizmeti Kullanımı	Mülakat, Sızma Testi	Kurumda URL sınıflandırma servisi kullanılmakta mıdır? Bu servislerden alınan listeler periyodik olarak güncellenmekte midir? Kategorilendirilmemiş siteler varsayılan olarak engellenmekte midir?
3.1.6.23	URL'lerin Kayıt Altına Alınması	Mülakat, Güvenlik Denetimi	Kurumdaki sistemlerden gelen tüm isteklere ait URL'ler kayıt altına alınmakta mıdır?
3.1.6.24	Kurum Ağına Bağlı Kablosuz Erişim Noktalarının Tespiti	Mülakat, Güvenlik Denetimi	Kurum ağına bağlı yetkisiz kablosuz erişim noktalarını tespit etmek için hangi kontroller uygulanmaktadır?
3.1.6.25	İstemcilerin Kablosuz Ağ Erişimlerinin Sınırlandırılması	Mülakat, Güvenlik Denetimi	İstemcilerin yetkisiz kablosuz ağ noktalarına erişimi nasıl kontrol edilmektedir?
3.1.6.26	Eşler Arası Kablosuz Ağ Erişiminin Engellenmesi	Mülakat, Güvenlik Denetimi	Eşler arası (Peer to Peer) kablosuz ağ erişimi nasıl engellenmektedir?
3.1.6.27	Kablosuz Çevre Birimleri Aracılığı ile Yapılan Erişimin Engellenmesi	Mülakat, Güvenlik Denetimi	Cihazların, kablosuz çevre birimleri aracılığı ile yapacakları yetkisiz erişimler nasıl engellenmektedir?
3.1.6.28	Uygulama Seviyesi Saldırıların Engellenmesi	Mülakat, Güvenlik Denetimi	Kurum uygulamalarının uygulama seviyesi saldırılara karşı korunması için hangi önlemler alınmaktadır? Alınan önlemler kapsamında bir servis sağlayıcıdan destek alınmakta ise, ilgili tedarik şartname ve sözleşmelerinde bilgi güvenliğine yönelik hangi hususlar ele alınmaktadır?
3.1.6.29	IP Telefon Erişim Kontrol Listeleri	Mülakat, Güvenlik Denetimi	IP telefon sistemlerinde kimlik sahteciliği saldırılarına karşı hangi önlemler alınmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.6.30	Ağ Cihazlarının Yapılandırma Yönetimi	Mülakat, Güvenlik Denetimi	Ağ cihazlarına yönelik yapılandırma işlemleri nasıl takip edilmektedir? Ağ cihazları mevcut yapılandırmaları periyodik olarak kontrol edilmekte midir? Ağ cihazı mevcut yapılandırmalarının, onaylanmış ve olması gereken güvenlik yapılandırma içerikleri ile değişkenlik göstermesi durumunda alarm üreten mekanizmalar devreye alınmakta mıdır?
3.1.6.31	Ağ Cihazlarının Yönetimi	Mülakat, Güvenlik Denetimi	Ağ cihazlarının yönetimi kapsamında çok faktörlü kimlik doğrulama mekanizmaları kullanılmakta mıdır? Ağ cihazlarının yönetiminde güvenli iletişim protokolleri kullanılmakta mıdır? Ağ cihazlarını yönetmek için kullandığınız internete erişimi bulunmayan ayrı bir bilgisayar mevcut mudur? Bu bilgisayarlar ağ yönetimi dışında farklı amaçlar için de kullanılmakta mıdır?
3.1.6.32	Kuruma Uzaktan Bağlanan Cihazların Yönetimi	Mülakat, Güvenlik Denetimi	Kuruma uzaktan bağlanacak cihazların uymaları gereken güvenlik politikaları tanımlanmakta mıdır? Kuruma uzaktan bağlanacak cihazların kurum politikalarına uygunluğu cihaz bağlanmadan önce kontrol edilmekte midir? Kurum politikalarına uymayan cihazlara bağlantı izni verilmekte midir?
3.1.6.33	Kripto Ağ Cihazlarının Kullanımı	Mülakat, Güvenlik Denetimi	Kritik ağ ortamları arasındaki iletişim için kripto ağ cihazları kullanılmakta mıdır?
3.1.6.34	Kablosuz İletişim Güvenliği	Mülakat, Güvenlik Denetimi	Kritik veri kablosuz ağ üzerinde taşınırken hangi kimlik doğrulama protokolleri kullanılmaktadır?
3.1.6.35	Kablosuz Çevre Birimleri Kullanımının Engellenmesi	Mülakat, Güvenlik Denetimi	Kritik veri işleyen kapalı ağlarda, kablosuz fare ve klavye gibi çevre birimlerinin kullanılması engellenmekte midir?
3.1.6.36	Veri Transferi	Mülakat, Güvenlik Denetimi, Sızma Testi	Kritik seviyeli ağlarda veri aktarımı hangi yöntemler ile gerçekleştirilmektedir?

3.1.7. Veri Sızıntısı Önleme

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.7.1	1	Veri Sınıflandırma Politikasının Oluşturulması	Kurum verilerinin sistematik olarak kategorilere ayrılması ve sınıflandırılması için politikalar oluşturulmalıdır.
3.1.7.2	1	Servis Sağlayıcıdan Alınan Hizmetlerde Veri Güvenliği Hususları	Bulut servisleri kullanımı durumunda veri erişimi, muhafazası, kullanımı kapsamındaki güvenlik hususları servis şartname ve sözleşmelerinde belirtilmelidir.
3.1.7.3	1	Kritik Verinin Envanteri Yönetimi	Kurum bünyesinde veya dışında, kurumun teknoloji sistemleri tarafından depolanan, işlenen veya iletilen tüm kritik verinin envanteri tutulmalıdır.
3.1.7.4	1	Düzenli Olarak Erişilmeyen Kritik Verinin ve Sistemlerin Kaldırılması	Kurum tarafından düzenli olarak erişilmeyen kritik veri veya sistemler ağdan çıkarılmalıdır. Bu sistemler ihtiyaç duyulmadığı durumlarda ağ bağlantısı kesilmiş olarak tutulmalıdır.
3.1.7.5	1	Bulut Servislerinin Kullanımı	Bulut depolama ve bulut e-posta servisi kullanımında Bölüm 4.3'te ifade edilen hususlar uygulanmalıdır. Bk. Bölüm 4.3
3.1.7.6	1	Taşınabilir Ortam Yönetimi	İş ihtiyaçları gereği taşınabilir ortamların kullanılması gerektiği durumlarda, yalnızca kurum tarafından yetkilendirilmiş ve kurum envanterine kayıt edilmiş taşınabilir ortamların kullanılmasına izin verecek şekilde gerekli önlemler alınmalıdır. Bk. Tedbir Başlık No: 3.3.3
3.1.7.7	1	Ağda Kritik Veri Taşınması	Ağda kritik verinin taşınmasında güvenli protokoller kullanılmalı (VPN teknolojileri, SSL/TLS vb.) ve kritik veri şifreli olarak taşınmalıdır.
3.1.7.8	2	Ağ İçerisinde Veri Sızıntısı Önleme	Ağ içerisinde veri akışını kontrol etmek, izlemek ve izinsiz ağ trafiğini takip etmek amacıyla ağ tabanlı veri sızıntısı önleme sistemi kullanılmalıdır.
3.1.7.9	3	Durağan Veri Güvenliğinin Sağlanması	Durağan veri ortamlarında yer alan kritik veri, şifrelenerek muhafaza edilmelidir. Depolanan kritik veri kimlik doğrulama mekanizması gerektiren ikincil bir araç kullanarak şifrelenmelidir. Kritik veriyi görüntülemek veya kritik veride değişiklik yapmak için gerçekleştirilen tüm işlemler kayıt altına alınmalıdır.
3.1.7.10	3	Taşınabilir Ortam Engelleme	Kritik sistemler taşınabilir depolama birimlerini desteklemeyecek şekilde yapılandırılmalıdır. Taşınabilir depolama birimleri takıldığında uyarı üretecek mekanizmalar aktif edilmelidir. Bu uyarılar izlenmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.7.1	Veri Sınıflandırma Politikasının Oluşturulması	Mülakat, Gözden Geçirme	Kurum verilerinin sistematik olarak kategorilere ayrılması ve sınıflandırılması için politikalar mevcut mudur?
3.1.7.2	Servis Sağlayıcıdan Alınan Hizmetlerde Veri Güvenliği Hususları	Mülakat, Gözden Geçirme	Servis sağlayıcının veri erişim, muhafaza ve kullanımındaki hizmet koşulları ve veri güvenliği hususları sözleşme ve tedarik şartnamelerinde nasıl ele alınmıştır?
3.1.7.3	Kritik Verinin Envanteri Yönetimi	Mülakat, Gözden Geçirme	Kuruma ait kritik verinin envanteri tutulmakta mıdır? Güncelliği nasıl kontrol altına alınmaktadır?
3.1.7.4	Düzenli Olarak Erişilmeyen Kritik Verinin ve Sistemlerin Kaldırılması	Mülakat, Güvenlik Denetimi	Kurum tarafından düzenli olarak erişilmeyen kritik veri veya sistemler kullanılmadıkları durumda ağa bağlı tutulmakta mıdır? Bu veri veya sistemler ihtiyaç duyulana kadar izole bir ağda tutulmakta mıdır?
3.1.7.5	Bulut Servislerinin Kullanımı	Mülakat, Güvenlik Denetimi	Bk. Bölüm 4.3
3.1.7.6	Taşınabilir Ortam Yönetimi	Mülakat, Güvenlik Denetimi	Kurum bünyesinde sadece kurum tarafından yetkilendirilmiş taşınabilir ortamların kullanımı nasıl kontrol altına alınmaktadır? Kurum tarafından yetkilendirilmiş taşınabilir ortamların envanteri tutulmakta mıdır?
3.1.7.7	Ağda Kritik Veri Taşınması	Mülakat, Güvenlik Denetimi	Ağda kritik veri nasıl taşınmaktadır?
3.1.7.8	Ağ İçerisinde Veri Sızıntısı Önleme	Mülakat, Güvenlik Denetimi	Ağ içerisinde veri akışını kontrol etmek ve izlemek maksadıyla ağ tabanlı veri sızıntısı önleme sistemi kullanılmakta mıdır? Kritik verinin güvenlik politikalarına uyumsuz şekilde taşındığının tespiti halinde nasıl bir aksiyon alınmaktadır?
3.1.7.9	Durağan Veri Güvenliğinin Sağlanması	Mülakat, Güvenlik Denetimi	Durağan veri ortamlarında yer alan kritik veri nasıl muhafaza edilmektedir? Kritik veriyi görüntülemek ve bu veri üzerinde değişiklik yapmak için gerçekleştirilen işlemlere ait kayıtlar tutulmakta mıdır?
3.1.7.10	Taşınabilir Ortam Engelleme	Mülakat, Güvenlik Denetimi	Kritik sistemler taşınabilir ortamları desteklemeyecek şekilde yapılandırılmakta mıdır? Kritik sistemler kapsamında taşınabilir ortamların engellenmesine yönelik uyarı mekanizmaları devreye alınmakta mıdır?

3.1.8. İz ve Denetim Kayıtlarının Tutulması ve İzlenmesi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.8.1	1	İz ve Denetim Kayıtlarının Tutulması	Tüm sistemlerde ve ağ cihazlarında kayıt mekanizması etkin olmalıdır. Kayıtlar, bilgi güvenliği gereksinimleri ve ilgili mevzuat gereği kabul edilebilir süre boyunca cihaz üzerinde veya harici sistemlerde tutulmalı, yetkisiz erişime ve değişime karşı korunmalıdır. Kayıtlar, muhafazaları için tanımlanan kabul edilebilir sürenin sona ermesi ile birlikte güvenli bir şekilde yok edilmelidir.
3.1.8.2	1	Denetim Kayıtlarının Yönetimi	Sistem yöneticisi, operatörler ve kullanıcıların faaliyetleri kayıt altına alınmalı, kayıtlar korunmalı ve düzenli olarak gözden geçirilmelidir.
3.1.8.3	1	Zaman Sunucusu Kullanımı	Kayıtlarda zaman damgalarının tutarlı olması için ağa bağlı tüm sistemlerin (sunucular, iş istasyonları, güvenlik ürünleri, ağ aygıtları vb.) düzenli olarak zaman bilgisinin alındığı; yedekli yapıda ve senkronize zaman sunucusu kullanılmalıdır. Bk. Tedbir No: 5.1.1.11
3.1.8.4	1	Detaylı Kayıt Tutulması	Sistem iz kayıtları; olay açıklaması, olay kaynağı, olay zamanı, kullanıcı/sistem bilgisi, kaynak adresleri, hedef adresleri ve işlem detayları bilgilerini içerecek şekilde tutulmalı ve bütünlüğü zaman damgası ile korunmalıdır.
3.1.8.5	1	Kayıtlar için Yeterli Depolama Alanı Tahsisi	Kayıt tutan sistemlerde yeterli depolama alanı tahsis edilmelidir. Depolama alanı doluluk oranı düzenli olarak kontrol edilmelidir.
3.1.8.6	2	Merkezi Kayıt Yönetimi	Analiz ve inceleme amacıyla kayıtlar merkezi bir kayıt yönetim sisteminde toplanmalı ve düzenli olarak yetkili personel tarafından gözden geçirilmelidir. Kayıt tutma veya gönderme işlemi sırasında hata oluştuğunda uyarı mekanizmaları aktif edilmeli ve izlenmelidir.
3.1.8.7	2	Kayıt Analizi Araçları Kullanımı	Siber olayların korelasyon kuralları doğrultusunda tespiti ve detaylı analizi için siber tehdit ve olay yönetim sistemleri veya kayıt analizi araçları kullanılmalıdır.
3.1.8.8	2	Siber Tehdit ve Olay Yönetim Sistemlerinin Düzenli Yapılandırılması	Aksiyon alınabilecek olayların daha iyi tanımlanabilmesi ve gereksiz olayların elenebilmesi amacıyla siber tehdit ve olay yönetim sistemlerinin yapılandırması düzenli olarak gözden geçirilmelidir. Kayıtlar düzenli olarak izlenmelidir. Bk. Tedbir Başlık No: 3.1.10

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.8.1	İz ve Denetim Kayıtlarının Tutulması	Mülakat, Güvenlik Denetimi	Kurumun sistem ve ağ cihazlarının yüzde kaçında kayıt tutulmaktadır? Kayıtlar nasıl saklanmaktadır? Kayıtlar için saklama süreleri tanımlanmış mıdır? Saklama süresi sona eren kayıtlar güvenli şekilde imha edilmekte midir? Saklama süreleri ilgili varlığın tabi olduğu yasal mevzuata uygun mudur?
3.1.8.2	Denetim Kayıtlarının Yönetimi	Mülakat, Gözden Geçirme	Sistem yöneticisi, operatörler ve kullanıcıların faaliyetlerine yönelik denetim kayıtları tutulmakta mıdır? Tutulan kayıtlar düzenli olarak gözden geçirilmekte midir? Denetim kayıtları üzerinde değişiklik yapılması engellenmekte midir?
3.1.8.3	Zaman Sunucusu Kullanımı	Mülakat, Güvenlik Denetimi	Kurumda senkronize ve yedekli zaman sunucusu kullanılmakta mıdır?
3.1.8.4	Detaylı Kayıt Tutulması	Mülakat, Güvenlik Denetimi	Kayıtlar en az; olay açıklaması, olay kaynağı, olay zamanı, kullanıcı/sistem bilgisi, kaynak adresleri, hedef adresleri ve işlem detayları bilgilerini içerecek şekilde tutulmakta mıdır? Tutulan kayıtların bütünlüğü nasıl sağlanmaktadır?
3.1.8.5	Kayıtlar için Yeterli Depolama Alanı Tahsisi	Mülakat, Güvenlik Denetimi	Kayıtlar için yeterli depolama alanı sağlanmakta mıdır? Depolama alanı doluluk oranı düzenli olarak takip edilmekte midir?
3.1.8.6	Merkezi Kayıt Yönetimi	Mülakat, Güvenlik Denetimi	Kayıtlar merkezi bir kayıt yönetim sistemi üzerinde toplanmakta mıdır? Kayıtlar yetkili personel tarafından düzenli olarak gözden geçirilmekte midir? Kayıt tutma ve gönderme işlemi sırasında oluşan hataları takip etmek amacıyla uyarı mekanizması kullanılmakta mıdır?
3.1.8.7	Kayıt Analizi Araçları Kullanımı	Mülakat, Güvenlik Denetimi	Kurumda hangi siber tehdit ve olay yönetim sistemleri veya kayıt analiz araçları kullanılmaktadır?
3.1.8.8	Siber Tehdit ve Olay Yönetim Sistemlerinin Düzenli Yapılandırılması	Mülakat, Güvenlik Denetimi	Siber tehdit ve olay yönetim sistemlerine ait yapılandırmalar hangi aralıklarla gözden geçirilmektedir?

3.1.9. Sanallaştırma Güvenliği

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.9.1	1	Güncel Sürümlerin Kullanılması	Sanallaştırma ürünlerinin üretici tarafından desteği devam eden ve kararlı sürümleri kullanılmalıdır. Bu ürünlerin güvenliği ile ilgili duyurular takip edilmelidir.
3.1.9.2	1	Kapasite Planlaması	Gelecekteki ihtiyaçlar, yasal yükümlülükler ve olası güvenlik riskleri göz önünde bulundurularak sistem kaynaklarının planlaması yapılmalı ve kaynaklar sürekli izlenmelidir. Kapasite artırımı için kurumsal eşik değerleri tanımlanmalıdır.
3.1.9.3	1	Sanal Makinelerin Yönetilmesi	Sanallaştırma ortamında kullanılmayan sanal makineler kapatılmalı, ağdan izole edilmeli ve sanal makine görev ömrünü tamamlayınca üzerinde yer alan veriler güvenli silme yöntemleri ile imha edilmelidir.
3.1.9.4	1	İşletim Sistemi Sıkılaştırmalarının ve Güvenlik Kontrollerinin Yapılması	Kullanılmakta olan işletim sistemleri, iş gereksinimlerini karşılamak için ihtiyaç duyulan bağlantı noktaları, protokoller ve servisleri sağlayacak şekilde sıkılaştırılmalıdır. Zararlı yazılımdan korunma uygulamaları kullanılmalı, dosya bütünlüğünü izleyecek ve kayıt tutacak mekanizmalar devreye alınmalıdır. Bk. Bölüm 5.1
3.1.9.5	1	Tedarik Edilen Sanallaştırma Hizmeti Ortam Güvenliğinin Sağlanması	Sanallaştırma hizmetinin üçüncü taraflar aracılığıyla sunulması durumunda, sanallaştırma ortamının güvenliği garanti altına alınmalıdır. Bk. Tedbir No: 3.5.3.3 Bk. Bölüm 4.3
3.1.9.6	2	İmaj Bütünlüğünün Denetlenmesi ve İzlenmesi	Tüm sanal makine imajlarının bütünlüğünü denetleyecek ve izleyecek mekanizmalar devreye alınmalıdır.
3.1.9.7	2	Sanal Ağ Güvenliği	Ağ ortamları ve sanal makineler, kurum tarafından belirlenen kriterlere göre güvenilir ve güvenilmeyen bağlantılar arasındaki trafik kısıtlanacak şekilde yapılandırılmalıdır. Bu yapılandırmalar düzenli olarak gözden geçirilmeli; izin verilen tüm servisler, protokoller, portlar dokümante edilmeli ve kullanım gerekçesi gösterilmelidir. Bk. Tedbir No: 3.1.6.6
3.1.9.8	2	Operasyon ve Test Ortamlarının İzolasyonu	Operasyon ve test ortamları güvenlik duvarları, alan/bölge bazlı kimlik doğrulama vb. yöntemler kullanılarak birbirinden ayrılmalı ve bu ortamların yöneticileri için görevler ayrılığı prensibi uygulanmalıdır.
3.1.9.9	2	Sanallaştırma Yönetim Ortamına Erişim	Sanallaştırma sistemleri yönetim arayüzlerine erişim, iş ihtiyaçları doğrultusunda tanımlanan yetki ile güvenli bir şekilde yapılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.9.10	2	Sanallaştırma Ortamı Sertifika Yönetimi	Sanallaştırma ortamında kendinden imzalı sertifikalar yerine kuruma ait ve yetkili otoriteden alınmış sertifikalar kullanılmalıdır.
3.1.9.11	2	Sanal Makineler Arası Trafiğin Kontrol Edilmesi	Sanal makineler arasındaki trafik güvenlik kontrollerinden geçirilmeli, olası zararlı trafiğin ağdaki diğer sanal ve fiziksel makinelere ulaşmaması için gerekli önlemler alınmalıdır.
3.1.9.12	2	Depolama Ortamları ile İletişim Güvenliğinin Sağlanması	Sanallaştırma ortamları ile birlikte kullanılacak veya kurum bünyesinde müstakil olarak kullanılacak depolama ortamları ile iletişimin güvenliğinin sağlanmasında aşağıdaki hususlar dikkate alınmalıdır. • Ağ dosya paylaşım servisleri, ayrılmış depolama ağlarında veya yönlendirilemeyen ağlarda hizmet vermelidir. • Ağ dosya paylaşım servislerinde, eğer destekleniyorsa trafik şifreli olmalı, uygun kimlik doğrulama protokolleri kullanılarak erişim denetimi yapılmalı ve kayıtlar tutulmalıdır.
3.1.9.13	2	Fiziksel Kaynakların İzole Edilmesi	Farklı güvenlik seviyesinde yer alan ağlarda kullanılan sanal sistemlere ait kaynaklar fiziksel olarak izole edilmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.9.1	Güncel Sürümlerin Kullanılması	Mülakat, Güvenlik Denetimi	Sanallaştırma ürünlerinin üretici tarafından desteği devam eden ve kararlı sürümleri kullanılmakta mıdır? Bu ürünlere yönelik sürüm değişiklikleri nasıl takip edilmektedir?
3.1.9.2	Kapasite Planlaması	Mülakat, Gözden Geçirme	Kaynaklara yönelik kapasite planlaması hangi kriterler göz önüne alınarak yapılmaktadır? Kapasite planları ne kadar sürede bir gözden geçirilmektedir?
3.1.9.3	Sanal Makinelerin Yönetilmesi	Mülakat, Güvenlik Denetimi	Sanallaştırma ortamında sanal makinelerin yaşam döngüsü nasıl yönetilmektedir? Kullanılmayan sanal makineler kapatılmakta mıdır? Sanal makine görev ömrünü tamamlayınca üzerindeki veriler ile ilgili nasıl aksiyon alınmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.9.4	İşletim Sistemi Sıkılaştırmalarının ve Güvenlik Kontrollerinin Yapılması	Mülakat, Güvenlik Denetimi	İşletim sistemleri için güvenlik sıkılaştırmaları hangi sıklıkta kontrol edilmektedir? Zararlı yazılımdan korunma uygulamaları kullanılmakta mıdır? İşletim sistemleri dosya bütünlüğü kontrolü yapmakta mıdır? İşletim sistemleri seviyesinde gerçekleşen olayların kayıtları tutulmakta mıdır?
3.1.9.5	Tedarik Edilen Sanallaştırma Hizmeti Ortam Güvenliğinin Sağlanması	Mülakat, Güvenlik Denetimi	Servis sağlayıcıdan hizmet koşulları ile ilgili taahhüt alınmış mıdır? Sözleşmelerde ve tedarik şartnamelerinde sanallaştırma güvenliği hususları nasıl ele alınmaktadır?
3.1.9.6	İmaj Bütünlüğünün Denetlenmesi ve İzlenmesi	Mülakat, Güvenlik Denetimi	Kurumda sanal makine imajlarının bütünlüğü kontrol edilmekte midir?
3.1.9.7	Sanal Ağ Güvenliği	Mülakat, Güvenlik Denetimi	Kurumda kullanılan servisler, protokoller ve port numaraları dokümante edilmekte midir? Dokümante edilen bilgiler hangi hususları içermektedir? Bu yapılandırmalar düzenli olarak gözden geçirilmekte midir?
3.1.9.8	Operasyon ve Test Ortamlarının İzolasyonu	Mülakat, Güvenlik Denetimi	Operasyon ve test ortamları birbirlerinden izole edilmiş midir? Bu ortamların yönetimleri görevlerin ayrılığı prensibi göz önünde bulundurularak yapılmakta mıdır?
3.1.9.9	Sanallaştırma Yönetim Ortamına Erişim	Mülakat, Sızma Testi	Sanallaştırma sistemlerinin yönetimi kapsamında hangi erişim kontrolleri uygulanmaktadır?
3.1.9.10	Sanallaştırma Ortamı Sertifika Yönetimi	Mülakat, Güvenlik Denetimi	Sanallaştırma ortamında kuruma ait ve yetkili otoriteden alınmış sertifikalar kullanılmakta mıdır?
3.1.9.11	Sanal Makineler Arası Trafiğin Kontrol Edilmesi	Mülakat, Güvenlik Denetimi	Sanal makineler arasındaki trafik kontrol edilmekte midir?
3.1.9.12	Depolama Ortamları ile İletişim Güvenliğinin Sağlanması	Mülakat, Güvenlik Denetimi	Depolama ortamları kullanılmakta mıdır? Sanallaştırma ortamı ile depolama ortamları iletişim güvenliği nasıl sağlanmaktadır? Ağ dosya paylaşım servisleri hangi ağlarda konumlandırılmıştır? Ağ dosya paylaşım trafiği kritik veri içermekte midir? Ağ üzerindeki trafik şifrelenmekte midir? Erişim kayıtları tutulmakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.9.13	Fiziksel Kaynakların İzole Edilmesi	Mülakat, Güvenlik Denetimi	Farklı güvenlik seviyesinde yer alan ağlarda kullanılan sanal sistemlere ait kaynaklar fiziksel olarak izole edilmekte midir?

3.1.10. Siber Güvenlik Olay Yönetimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.10.1	1	Siber Olaylara Müdahale Planlarının Hazırlanması	Siber olaylara müdahale planları; uygulanması gereken akış, rol ve sorumlulukları içerecek şekilde dokümante edilmelidir. Kurumsal SOME Kurulum ve Yönetim Rehberi'ne uygun olarak çalışmalar yürütülmelidir.
3.1.10.2	1	Siber Olay Yönetimi Kapsamında Görev Alacak Personelin Belirlenmesi	Siber olayların yönetimi aşamalarında görev alacak personelin rol ve sorumlulukları tanımlanmalı, olay müdahale için gerekli teknik alt yapı personele sağlanmalı ve belirlenen personel ilgili taraflara bildirilmelidir. Siber olay yönetimi kapsamında görev alacak personel Kurumsal SOME Kurulum ve Yönetim Rehberi kriterlerine uygun olmalıdır.
3.1.10.3	1	İletişim Bilgileri Dokümanının Hazırlanması	Siber olay bildirimi yapılacak resmi kurumlara ilişkin iletişim bilgileri dokümanı oluşturulmalı ve periyodik olarak gözden geçirilmelidir. İletişim bilgileri dokümanı, iletişim kurulacak konu kapsamında iletişim kurulacak kişileri tanımlamalıdır.
3.1.10.4	1	Siber Tehdit Bildirimlerinin Yönetilmesi	Kurumlar siber olayların tespiti için gerekli altyapıları kurmalı, USOM ve olası diğer siber tehdit istihbarat kaynaklarından alınan bildirimler doğrultusunda gerekli önlemleri almalıdır.
3.1.10.5	1	Siber Olayların Raporlarının Standardize Edilmesi ve Yayınlanması	Siber olaylar ile ilgili bildirim süresi ve rapora yansıtılacak bilgiler USOM tarafından belirlenen kriterler göz önünde bulundurularak belirlenmeli ve standart hale getirilmelidir. Yaşanan siber olaya ilişkin iş ve işlemlerin detaylı bir şekilde anlatıldığı siber olay müdahale raporu, kurum standartlarına göre hazırlanmalı, üst yönetim, USOM ve varsa bağlı olduğu Sektörel SOME'ye iletilmelidir.
3.1.10.6	1	Üçüncü Taraflardan Alınan Siber Olay Yönetim Hizmetleri	Kurumların siber olay yönetimi kapsamındaki hizmetleri üçüncü taraflardan alması durumunda hizmetin güvenliği garanti altına alınmalıdır. Bk. Tedbir No: 3.5.3.3 Bk. Bölüm 4.3

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.10.7	2	SOME Personeli için Periyodik Siber Olay Tatbikatlarının Yapılması	SOME personelinin, gerçek dünyadaki tehditlere cevap verme konusundaki yeteneklerini arttırmak için rutin tatbikatlar planlanmalı ve uygulanmalıdır. Tatbikatlar iletişim kanallarını, karar mekanizmasını ve olaylara müdahale ekibinin teknik yeteneklerini test etmelidir. Tatbikat sonrasında tatbikat sonuçları ve öğrenilmiş dersler değerlendirilmeli ve kayıt altına alınmalıdır.
3.1.10.8	3	Siber Olay Yönetimi Puanlama ve Önceliklendirme	Olaylar, kuruma potansiyel etkileri göz önünde bulundurularak puanlanmalı ve olayların giderilmesi için hazırlanan aksiyon planında önceliklendirme için risk temelli bir model kullanılmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.10.1	Siber Olaylara Müdahale Planlarının Hazırlanması	Mülakat, Gözden Geçirme	Siber olaylara müdahale planları; uygulanması gereken akış, rol ve sorumlulukları içerecek şekilde dokümante edilmekte midir?
3.1.10.2	Siber Olay Yönetimi Kapsamında Görev Alacak Personelin Belirlenmesi	Mülakat, Gözden Geçirme	Siber olayların yönetimi aşamalarında görev alacak personel, rol ve sorumlulukları ile birlikte tanımlanmakta mıdır? Personele olay müdahale için gerekli teknik alt yapı sağlanmakta mıdır? Siber olay yönetimi kapsamında görev alacak personel Kurumsal SOME Kurulum ve Yönetim Rehberi kriterlerine uygun olarak belirlenmekte midir? Görev alacak personel listesi periyodik olarak gözden geçirilmekte midir?
3.1.10.3	İletişim Bilgileri Dokümanının Hazırlanması	Mülakat, Gözden Geçirme	Siber olay bildirimi yapılacak resmi kurumlara ilişkin iletişim bilgileri dokümanı mevcut mudur? İletişim bilgileri dokümanı periyodik olarak gözden geçirilmekte midir?
3.1.10.4	Siber Tehdit Bildirimlerinin Yönetilmesi	Mülakat	Siber tehdit bildirimlerinin takibi için hangi istihbarat kaynaklarından yararlanılmaktadır?
3.1.10.5	Siber Olayların Raporlarının Standardize Edilmesi ve Yayınlanması	Mülakat, Gözden Geçirme	Siber olay bildirim süresi ve bildirimde verilecek bilgiler kurum içinde standart mıdır? Siber olaylara müdahale adımları detaylı bir şekilde raporlanmakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.10.6	Üçüncü Taraflardan Alınan Siber Olay Yönetim Hizmetleri	Mülakat, Güvenlik Denetimi	Siber olay yönetim hizmetlerinin tamamı kurum tarafından mı karşılanmaktadır? Üçüncü taraflardan alınan siber olay yönetim fonksiyonları hangileridir? Üçüncü tarafın söz konusu hizmetleri rehberin yönlendirdiği şekliyle sağladığı denetlenmekte midir? Sözleşme, teknik şartname vb. hizmet alım dokümanlarında bu hususlar mevcut mudur? Denetim kayıtları var mıdır?
3.1.10.7	SOME Personeli için Periyodik Siber Olay Tatbikatlarının Yapılması	Mülakat, Gözden Geçirme	Kurumda periyodik olarak siber olay tatbikatları yapılmakta mıdır? Tatbikat senaryoları dokümante edilmekte midir? Tatbikat ile hangi yeterlilikler test edilmektedir? Tatbikat sonrasında tatbikat sonuçları ve öğrenilmiş dersler değerlendirilmekte ve kayıt altına alınmakta mıdır?
3.1.10.8	Siber Olay Yönetimi Puanlama ve Önceliklendirme	Mülakat	Siber olaylar, kuruma potansiyel etkileri göz önünde bulundurularak puanlanmakta ve olayların giderilmesi için hazırlanan aksiyon planında önceliklendirme risk temelli bir model kullanılarak yapılmakta mıdır?

3.1.11. Sızma Testleri ve Güvenlik Denetimleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.11.1	1	Sızma Testleri ve Güvenlik Denetimlerinin Gerçekleştirilmesi	Kurum sistemlerinin güvenlik açıklarını ve saldırı yüzeyini belirlemek için düzenli aralıklarla harici ve dâhili sızma testleri ve güvenlik denetimleri gerçekleştirilmelidir. Sızma testleri ve güvenlik denetimleri gerçekleştirilmeden önce testi gerçekleştirecek taraftan, test süresince elde edilen hiçbir verinin yetkisiz kişilere verilmemesi, aktarılmaması ve ifşa edilmemesine yönelik taahhüt alınmalıdır. Sızma testi ve güvenlik denetimi kapsamı tanımlanmalı ve dokümante edilmelidir. Sosyal mühendislik testleri de sızma testi kapsamına dâhil edilmelidir.
3.1.11.2	1	Sızma Testlerinin Kullanıcı Profillerine Göre Gerçekleştirilmesi	Sağlıklı ve gerçek hayata uygun bir sızma testi için testler sırasında anonim kullanıcılar, misafir kullanıcılar, çalışanlar, kurumdan hizmet alan kullanıcılar ve kuruma destek veren kullanıcılar gibi farklı yetki seviyesindeki kullanıcı profilleri kullanılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.11.3	1	Sızma Testi Gerçekleştirilemeyen Bileşenlerin Yönetimi	Operasyonel ortamda olup sızma testi yapılması mümkün olmayan veya yüksek risk içeren sistemler için güvenlik denetimleri ve güvenlik sıkılaştırmaları düzenli olarak yapılmalıdır.
3.1.11.4	1	Sızma Testi için Oluşturulan Hesapların Yönetimi	Sızma testini gerçekleştirmek için kullanılan herhangi bir kullanıcı veya sistem hesabı, yalnızca meşru amaçlar için kullanıldığından emin olmak için kontrol edilmeli, izlenmeli, kayıt altına alınmalı ve test bittikten sonra pasif hale getirilmelidir.
3.1.11.5	1	Doğrulama Testlerinin Yaptırılması	Kapatılan güvenlik açıklarına yönelik doğrulama testleri görevlerin ayrılığı ilkesi doğrultusunda yapılmalıdır.
3.1.11.6	1	Sızma Testi ve Güvenlik Denetimi Bulgularının Seviyelendirilmesi	Sızma testi ve güvenlik denetimi bulguları karşılaştırılabilir bir puanlama yöntemi dikkate alınarak raporlanmalıdır.
3.1.11.7	2	Test Ortamlarının Hazırlanması	Canlı ortamda olup sızma testi yapılması mümkün olmayan ve/veya yüksek risk içeren sistemler için gerçeğine benzer test ortamları oluşturulmalıdır. Test ortamının oluşturulması mümkün olmayan her bir bileşen için 3.1.11.3 numaralı tedbir maddesi uygulanmalıdır.
3.1.11.8	2	Sızma Testleri ve Güvenlik Denetimlerinin Periyodu	Sızma testleri ve güvenlik denetimleri yılda en az 1 defa yapılmalıdır.
3.1.11.9	3	Düzenli Kırmızı Takım Tatbikatlarının Yapılması	Siber saldırılara karşı kurumsal hazırlığı test etmek adına düzenli kırmızı takım tatbikatları yapılmalı veya yaptırılmalıdır. Tatbikat sonuçları kurum içi dokümante edilerek raporlanmalıdır. Rapor sonuçlarına göre kurumda gerekli iyileştirmeler sağlanmalıdır.
3.1.11.10	3	Kurum Ağına Eklenen Yazılımın ve Donanımın Kontrolü	Kurum ağına eklenecek donanıma veya yazılıma, ağa dâhil edilmeden önce zafiyet taraması ve güvenlik denetimi yapılmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.11.1	Sızma Testleri ve Güvenlik Denetimlerinin Gerçekleştirilmesi	Mülakat, Gözden Geçirme	Kurum bünyesinde sızma testleri ve güvenlik denetimleri düzenli olarak yapılmakta mıdır? Sızma testi ve güvenlik denetimleri öncesinde testi gerçekleştirecek taraftan test süresince elde edilen verilerin yetkisiz kişilere verilmemesi, aktarılmaması ve ifşa edilmemesine yönelik taahhüt alınmakta mıdır? Sızma testi ve güvenlik denetimleri kapsamı tanımlanmakta ve dokümante edilmekte midir? Kurumda sızma testi yapılmadan önce tüm sistemler için zafiyet taramaları yapılmakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.11.2	Sızma Testlerinin Kullanıcı Profillerine Göre Gerçekleştirilmesi	Mülakat	Sızma testleri, farklı yetki seviyesindeki bütün kullanıcı profillerini içerecek şekilde gerçekleştirilmekte midir?
3.1.11.3	Sızma Testi Gerçekleştirilemeyen Bileşenlerin Yönetimi	Mülakat	Operasyonel ortamda olup sızma testi yapılması mümkün olmayan ve/veya yüksek risk içeren sistemler için güvenlik denetimleri ve güvenlik sıkılaştırmaları düzenli olarak yapılmakta mıdır?
3.1.11.4	Sızma Testi için Oluşturulan Hesapların Yönetimi	Mülakat, Güvenlik Denetimi	Kurumda sızma testi için kullanılan hesaplar kontrol edilmekte midir? Bu hesaplar test sonrasında pasif hale getirilmekte midir?
3.1.11.5	Doğrulama Testlerinin Yaptırılması	Mülakat, Sızma Testi	Kapatılan güvenlik açıklarının doğrulama testleri yapılmakta mıdır?
3.1.11.6	Sızma Testi ve Güvenlik Denetimi Bulgularının Seviyelendirilmesi	Mülakat, Gözden Geçirme	Sızma testi ve güvenlik denetimi bulguları standart bir şekilde raporlanmakta mıdır?
3.1.11.7	Test Ortamlarının Hazırlanması	Mülakat, Gözden Geçirme	Canlı ortamda olup test edilmesi sakıncalı sistemler için benzer test ortamları oluşturulmakta mıdır? Test ortamının oluşturulması mümkün olmayan bileşenler için nasıl bir yol izlenmektedir?
3.1.11.8	Sızma Testleri ve Güvenlik Denetimlerinin Periyodu	Mülakat, Gözden Geçirme	Sızma testleri ve güvenlik denetimleri ne kadar sürede bir gerçekleştirilmektedir?
3.1.11.9	Düzenli Kırmızı Takım Tatbikatlarının Yapılması	Mülakat, Gözden Geçirme	Kurumda düzenli aralıklarla kırmızı takım tatbikatları yapılmakta mıdır? Tatbikat sonuçları kayıt altına alınmakta ve dokümante edilmekte midir?
3.1.11.10	Kurum Ağına Eklenen Yazılımın ve Donanımın Kontrolü	Mülakat, Gözden Geçirme	Yazılım ve donanımlar kurum ağına dâhil edilmeden önce zafiyet taraması ve güvenlik denetiminden geçmekte midir?

3.1.12. Kimlik Doğrulama ve Erişim Yönetimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.12.1	1	Erişim Kontrol Politikasının Oluşturulması ve Uygulanması	Erişim kontrol politikaları oluşturulmalı, uygulamaya alınmalı ve güncelliği periyodik olarak kontrol edilmelidir. Kullanıcı (sistem yöneticisi ve sisteme işlem amacıyla erişen kullanıcılar) hesap işlemleri (açma, kapama, değişiklik) ve erişim talepleri tanımlı bir süreç ile takip edilmeli ve kayıt altına alınmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.12.2	1	Kullanıcı Hesaplarının Yönetimi	Her kullanıcı için kendine ait ve kendisini benzersiz olarak tanımlayan bir kullanıcı hesabı tanımlanmalı, tüm kullanıcı hesaplarına ait bir parola ataması yapılmalıdır. Kullanıcı hesaplarına ait parolalar belirlenirken dikkat edilmesi gereken kurallar tanımlanmalı ve uygulanmalıdır.
3.1.12.3	1	Başarısız Oturum Açma Denemelerinin Yönetimi	Oturum açma mekanizmasına yapılacak saldırıları engellemek amacıyla uygun güvenlik önlemleri (istek sınırlandırma, IP bloklama, CAPTCHA vb.) alınmalıdır. Başarısız oturum açma denemeleri kayıt altına alınmalıdır.
3.1.12.4	1	Varsayılan Kullanıcıların ve Parolaların Değiştirilmesi	Kurum bilgi sistemindeki herhangi bir varlıkta varsayılan kullanıcı adı ve parolalar kullanılmamalıdır. Test ortamlarında kullanımda olan tüm varsayılan kullanıcılar ve parolalar, canlıya alınmadan önce silinmeli veya değiştirilmelidir.
3.1.12.5	1	Yönetici Hesaplarının Kullanımı	Sistem yöneticilerinin yüksek haklar gerektiren işlemleri yapmak için ayrı bir hesapları olmalıdır. Yönetici hesaplarıyla yapılan işlemler için denetim kayıtları oluşturulmalıdır.
3.1.12.6	1	İşlem Yapılmayan Oturumların Sonlandırılması	İşlem yapılmayan oturumlar belirli bir süre sonra sonlandırılmalıdır.
3.1.12.7	1	Kimlik Doğrulama	Kurum kaynaklarına erişimlerde kimlik doğrulama mekanizmaları kullanılmalıdır.
3.1.12.8	1	Kullanıcı Yetkilerinin Güncellenmesi	Sistem yöneticilerinin ve kullanıcılarının yetkileri düzenli olarak gözden geçirilmeli, görev değişikliklerinde erişim yetkileri güncellenmelidir. Bir personelin veya yüklenicinin sorumluluklarının değişmesinden hemen sonra hesapları devre dışı bırakmak ve sistem erişimini iptal etmek için süreç oluşturulmalı ve uygulanmalıdır. Bu hesaplar devre dışı bırakılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.12.9	1	Kurum Dışı Paydaşların Uzaktan Erişimi	Kurum dışı paydaşların kurum kaynaklarına uzaktan erişimine, ilgili kurum personelinin onayı dışında izin verilmemelidir. Uzaktan erişimin gerçekleştiği durumlarda ise aşağıdaki kurallar uygulanmalıdır: • Erişim yetkisi sınırlı ve belirli bir süreyle tanımlanmalıdır. Oturum zaman aşımı süresi belirlenmeli ve süre sonunda kullanıcı kimlik doğrulamaya zorlanmalıdır. • Çok faktörlü kimlik doğrulama metotları aktif edilmelidir. • Erişimin gerçekleştiği hedefler ile erişimin yapıldığı kaynaklar için kısıtlama yapılmalıdır. • Erişimlere ilişkin iz kayıtları tutulmalıdır. Bk. Tedbir No: 3.1.8.1 • Herhangi bir anomali ve ihlal durumuna karşın gerekli izleme ve alarm mekanizmaları aktifleştirilmelidir. • Gerektiği durumlarda video kayıt ve personel gözetimi metotları işletilmelidir. • Erişim yolu şifreli ve güvenli olmalıdır.
3.1.12.10	2	Kullanılmayan Hesapların Devre Dışı Bırakılması	Belirli bir süre kullanılmayan, bir iş süreci veya kurum personeli ile ilişkilendirilemeyen tüm hesaplar otomatik olarak devre dışı bırakılmalıdır.
3.1.12.11	2	Yönetici Hesaplarının İşletimi	Etki alanı ve yerel hesaplar dâhil tüm yönetim hesaplarını yönetmek için otomatik araçlar kullanılmalıdır. Kurumdaki sistemler bir yönetici hesabı oluşturulduğunda veya silindiğinde kayıt tutacak ve alarm oluşturacak şekilde yapılandırılmalıdır. Tüm yönetici hesap erişimleri için çok faktörlü kimlik doğrulama ve şifreli kanallar kullanılmalıdır. Kurumdaki sistemler bir yönetici hesabından giriş denemesi yapıldığında kayıt tutmalı ve giriş denemesi yapılması durumunda alarm oluşturacak şekilde yapılandırılmalıdır.
3.1.12.12	2	Betik Dillerinin Kullanımına Yönelik Erişimin Sınırlandırılması	Betik dosyası oluşturma araçlarına (PowerShell ve Python gibi) erişim, yalnızca iş amaçları doğrultusunda bu özelliklere erişmesi gereken hesaplar ile sınırlandırılmalıdır.
3.1.12.13	2	Kimlik Yönetim ve Doğrulama Sistemlerinin Envanterinin Tutulması	Yerel veya uzak servis sağlayıcılarında bulunanlar da dâhil olmak üzere, kurumun tüm kimlik doğrulama sistemlerinin ve bu sistemlerle entegre uygulamaların envanteri tutulmalıdır.
3.1.12.14	2	Merkezi Kimlik Doğrulama	Kimlik doğrulama merkezi olarak yapılmalıdır. Merkezi kimlik yönetim ve doğrulama sisteminin kullanılamadığı durumlarda, risk analizi çalışması doğrultusunda telafi edici önlemler alınmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.12.15	2	Çok Faktörlü Kimlik Doğrulama Yapılması	Kurum ağına dışarıdan yapılan erişimler çok faktörlü kimlik doğrulaması ile sağlanmalıdır.
3.1.12.16	2	Kimlik Doğrulama Bilgilerinin Güvenli Olarak Saklanması	Tüm kimlik doğrulama bilgileri güçlü kriptografik algoritmalar kullanılarak saklanmalı ve şifreli kanallar kullanılarak iletilmelidir.
3.1.12.17	2	Servis Hesaplarının Yönetimi	Servis hesapları en az yetki prensibi göz önünde bulundurularak oluşturulmalıdır. Kullanıcı veya yetkili hesaplar servis hesabı olarak kullanılmamalıdır. Servis hesaplarının kurum içerisinde bir sahibi olmalı ve periyodik olarak gözden geçirilmelidir.
3.1.12.18	3	Hesap Giriş Davranışlarında Değişikliklerin Saptanması	Kullanıcı davranışları, kullanıcı rolü ve yetki seviyesi değişiklikleri güvenlik ihlal durumlarına karşı izlenmeli ve alarm mekanizmaları devreye alınmalıdır.
3.1.12.19	3	Oturum Kayıtlarının Tutulması	Gizlilik dereceli verilerin saklandığı/işlendiği sistemler üzerinde sistem yönetimi amacıyla açılan oturumlar sırasında gerçekleştirilen faaliyetler kayıt altına alınmalı ve alınan kayıtların doğrulaması yapılmalıdır.
3.1.12.20	3	Sistem Yöneticisi Görevlerinin Güvenliği	Tüm sistem yöneticisi görevleri belirli IP adresleri kullanılarak yapılmalıdır. Yönetim işlemlerini gerçekleştiren sistem yöneticileri, sadece yönetimsel haklar gerektiren işler için ilgili hesapları kullanmalıdır. Yetkilendirmelerin senede en az 1 kez olacak şekilde gözden geçirilmesi, gereksinimi kalmamış yetkilerin geri alınması sağlanmalıdır.
3.1.12.21	3	Veri ve Parola Güvenliğinin Sağlanması	Veri ve parolaların güvenliğinin sağlanması gerektiğinde otomatik parola yönetim aracı (password vault) kullanılmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.12.1	Erişim Kontrol Politikasının Oluşturulması ve Uygulanması	Mülakat, Gözden Geçirme	Erişim kontrol politikaları oluşturulmakta mıdır? Politika kapsamında kullanıcı hesap işlemleri ve erişim taleplerinin yönetilmesine ilişkin nasıl bir süreç tanımlanmaktadır?
3.1.12.2	Kullanıcı Hesaplarının Yönetimi	Mülakat, Güvenlik Denetimi	Kullanıcı hesaplarının yönetimine ilişkin hangi bilgi güvenliği kontrolleri uygulanmaktadır?
3.1.12.3	Başarısız Oturum Açma Denemelerinin Yönetimi	Mülakat, Sızma Testi	Oturum açma mekanizmasına yapılacak saldırıları engellemek amacıyla hangi güvenlik önlemleri alınmaktadır? Başarısız oturum açma denemeleri kayıt altına alınmakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.12.4	Varsayılan Kullanıcıların ve Parolaların Değiştirilmesi	Mülakat, Sızma Testi	Kurum bilgi sistemlerinde yer alan varlıkların varsayılan parolaları değiştirilmekte midir? Test çalışmalarında varsayılan parolalar değiştirilmekte midir? Kullanılmayan varsayılan hesaplar silinmekte midir?
3.1.12.5	Yönetici Hesaplarının Kullanımı	Mülakat, Sızma Testi	Kurumda sistem yöneticileri, yönetimsel işlemler için ayrı bir hesap kullanmakta mıdır? Yöneticiler hedef cihazlara nasıl erişim sağlamaktadırlar?
3.1.12.6	İşlem Yapılmayan Oturumların Sonlandırılması	Mülakat, Sızma Testi	İşlem yapılmayan oturumlar belirli bir süre sonra sonlandırılmakta mıdır?
3.1.12.7	Kimlik Doğrulama	Mülakat, Sızma Testi	Kurum kaynaklarına erişimlerde hangi kimlik doğrulama mekanizmaları kullanılmaktadır?
3.1.12.8	Kullanıcı Yetkilerinin Güncellenmesi	Mülakat, Gözden Geçirme	Sistem yöneticilerinin ve kullanıcılarının hakları düzenli aralıklarla gözden geçirilmekte midir? Kimlik doğrulama sistemi tarafından düzenlenen tüm hesapların envanteri tutulmakta mıdır? Görevi sona eren hesaplar devre dışı bırakılmakta mıdır? Bu işlem için otomatik bir süreç oluşturulmuş mudur? Devre dışı bırakılan hesaplara yapılan erişim denemeleri izlenip, kayıt altına alınmakta mıdır?
3.1.12.9	Kurum Dışı Paydaşların Uzaktan Erişimi	Mülakat, Güvenlik Denetimi	Kurum dışı paydaşların kurum sistemlerine uzaktan erişimi kapsamında hangi güvenlik kontrolleri uygulanmaktadır?
3.1.12.10	Kullanılmayan Hesapların Devre Dışı Bırakılması	Mülakat, Güvenlik Denetimi	Bir iş süreci veya kurum çalışanı ile ilişkilendirilemeyen tüm hesaplar devre dışı bırakılmakta mıdır?
3.1.12.11	Yönetici Hesaplarının İşletimi	Mülakat	Kurumda yönetim hesaplarının envanteri tutulmakta mıdır? Bu işlem otomatik araçlarla mı yapılmaktadır? Yönetici hesap erişimleri nasıl yapılmaktadır?
3.1.12.12	Betik Dillerinin Kullanımına Yönelik Erişimin Sınırlandırılması	Mülakat, Güvenlik Denetimi	Kurum bilgisayarlarında betik çalıştırma yetkisi hangi kullanıcılara verilmektedir?
3.1.12.13	Kimlik Yönetim ve Doğrulama Sistemlerinin Envanterinin Tutulması	Mülakat, Gözden Geçirme	Yerel veya uzak servis sağlayıcılarında bulunanlar da dâhil olmak üzere, kurumun tüm kimlik sağlayıcılarının envanteri tutulmakta mıdır?
3.1.12.14	Merkezi Kimlik Doğrulama	Mülakat, Güvenlik Denetimi, Sızma Testi	Kurum mümkün olan tüm durumlarda kimlik denetimini merkezi olarak yapmakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.12.15	Çok Faktörlü Kimlik Doğrulama Yapılması	Mülakat, Güvenlik Denetimi	Kurum tarafından yapılan kimlik denetimlerinde çok faktörlü kimlik doğrulama mekanizmasının uygulanmadığı yerler var mıdır?
3.1.12.16	Kimlik Doğrulama Bilgilerinin Güvenli Olarak Saklanması	Mülakat, Güvenlik Denetimi	Kimlik doğrulama bilgilerinin saklanmasına yönelik hangi güvenlik önlemleri alınmaktadır? Kurumun tüm kimlik doğrulama bilgileri şifreli kanallar üzerinden iletilmekte midir? Alınan önlemler yetkili kurumlarca test edilmiş midir?
3.1.12.17	Servis Hesaplarının Yönetimi	Mülakat, Güvenlik Denetimi	Servis hesapları erişim yetkileri nasıl tanımlanmaktadır? Servis hesaplarına yönelik gözden geçirme süreci nasıl işletilmektedir? Kullanıcı veya yetkili hesaplar servis hesabı olarak kullanılmakta mıdır?
3.1.12.18	Hesap Giriş Davranışlarında Değişikliklerin Saptanması	Mülakat	Kullanıcı hesap giriş davranışları düzenli olarak izlenmekte midir? Kullanıcı rolü ve yetki seviyesi değişiklikleri gibi durumlarda alarm oluşturulmakta mıdır?
3.1.12.19	Oturum Kayıtlarının Tutulması	Mülakat, Güvenlik Denetimi	Gizlilik dereceli verilerin saklandığı/işlendiği sistemler üzerinde açılan oturumlar sırasında gerçekleştirilen faaliyetler kayıt altına alınmakta mıdır? Alınan kayıtların doğrulaması nasıl yapılmaktadır?
3.1.12.20	Sistem Yöneticisi Görevlerinin Güvenliği	Mülakat, Güvenlik Denetimi	Tüm yönetimsel görevler yönetim dışı faaliyetler için kullanılmayan belirli bilgisayarlar üzerinden mi yapılmaktadır? Yetkilendirmeler periyodik olarak gözden geçirilmekte midir?
3.1.12.21	Veri ve Parola Güvenliğinin Sağlanması	Mülakat, Sızma Testi	Veri ve parolaların güvenliği için otomatik parola yönetim aracı (password vault) kullanılmakta mıdır?

3.1.13. Felaket Kurtarma ve İş Sürekliliği Yönetimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.13.1	1	Yedekleme Planının Oluşturulması	Kurum bünyesinde iş süreçlerinde kullanılan ve iş süreçlerini destekleyen tüm sistemler göz önünde bulundurularak yedekleme ihtiyacı olan sistemler tespit edilmeli ve dokümante edilmiş bir yedekleme planı üzerinden yedekleme yönetimi yapılmalıdır. Yedekleme planı en az aşağıdaki başlıkları içerecek şekilde oluşturulmalıdır: • Yedeği alınan sistemler • Yedekleme işleminin adı • Yedekleme işlemi başlangıç tarih ve saat bilgisi • Yedekleme tipi • Yedekleme periyodu • Yedekleme süreçlerinde versiyonlama
3.1.13.2	1	Yedekleme Planının Periyodik Olarak Gözden Geçirilmesi	Yedekleme planı, yedekleme ihtiyaçları göz önünde bulundurularak yılda en az bir kere gözden geçirilmelidir. Bu gözden geçirme kapsamında iş birimleri ile de görüşülerek yedekleme ihtiyacı ortadan kalkan sistemler tespit edilmeli, yedekleme işleminden çıkarılmalı ve yedekleme işleminde olmayan fakat dâhil edilmesi gereken sistemler tespit edilerek yedekleme işlemine dâhil edilmelidir.
3.1.13.3	1	Yedekleme İşlemleri için İz Kayıtlarının Oluşturulması	Yedekleme işlemlerine ilişkin iz kayıtları oluşturulmalı, bu kayıtlar bilgi güvenliği gereklilikleri ve ilgili mevzuat göz önünde bulundurularak tanımlanmış süre kadar tutulmalı ve zaman damgası ile korunmalıdır. Bk. Tedbir No: 3.1.8.1
3.1.13.4	1	Yedekten Geri Dönüş Testleri	Yedekleme ortamlarının çalıştığından ve geri dönülebilir olduğundan emin olmak adına; kapsamdaki sistemlerin, uygulamaların ve verinin yedekleri düzenli olarak geri dönüş testlerine tabi tutulmalı ve gerçekleştirilen geri dönüş testlerine yönelik kayıtlar oluşturulmalıdır. Bu kayıtlar en az aşağıdaki bilgileri içermelidir: • Testin gerçekleştirildiği gün ve saat bilgisi • Testi yapılan sistemler • Testin gerçekleştirildiğini kanıtlayan ekran görüntüleri • Testin başarılı sonuçlanıp sonuçlanmadığı • Test sırasında karşılaşılan sorunlar ve çıkarılan dersler.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.13.5	1	Yedekleme Medyalarının Saklanması, Güvenliği ve İmhası	Yedekleme medyalarının envanteri tutulmalı ve envanter periyodik olarak gözden geçirilmelidir. Yedekleme medyaları, fiziksel olarak güvenli ve yedek alınan bölgeden farklı bir konumda saklanmalıdır. Yedeklenen verinin; ana sistemlerin bulunduğu ortamla benzer riskleri içermeyen başka bir ortamda saklandığı teyit edilmelidir. Yedeklenen veri tesis/yerleşke dışına taşınırken güvenliğinin sağlandığı ve bulunduğu ortamın fiziksel ve mantıksal güvenliğinin sağlanmış olduğu teyit edilmelidir. Yedekler kullanım süresinin sona ermesi sonrasında ulusal/uluslararası standartlara uygun olarak güvenli bir şekilde imha edilmeli ve imha kayıtları tutulmalıdır.
3.1.13.6	2	İş Sürekliliği Kapsamının Tanımlanması	Kurumun faaliyet alanı ile yasal ya da sözleşmelerden doğan yükümlülükleri de göz önünde bulundurularak iş sürekliliği çalışmaları kapsamında ele alınması gereken hizmetler, birimler ve lokasyonlar tanımlanmalıdır.
3.1.13.7	2	İş Sürekliliği Planlarının Hazırlanması	Kapsam dâhilinde yer alan hizmetler, birimler ve lokasyonlar göz önünde bulundurularak iş sürekliliği planları hazırlanmalı ve belirli aralıklarla gözden geçirilmelidir.
3.1.13.8	2	İş Sürekliliği Kapsamında Rol ve Sorumlulukların Tanımlanması	İş sürekliliği kapsamında olan tüm paydaşların ve süreç içinde yer alacak personelin görev ve sorumlulukları dokümante edilmeli ve ilgili taraflara bildirilmelidir.
3.1.13.9	2	İş Sürekliliği Çalışmalarında Üçüncü Taraf Hizmetlerin Dikkate Alınması	İş sürekliliği planları kapsamında; hizmet alınan üçüncü tarafların rol ve sorumlulukları ile birlikte tedarik edilen hizmetlerin süreklilik kriterleri de dikkate alınmalıdır.
3.1.13.10	2	İş Sürekliliği Planlarının Test Edilmesi	Süreklilik yönetimi dâhilinde tüm planlar kurum tarafından belirlenen periyotlarda test edilmeli ve test sonuçları kayıt altına alınmalıdır.
3.1.13.11	2	İş Sürekliliği Planlarının Güvenli Muhafazası	Süreklilik yönetimi dâhilindeki planların, acil durum müdahale prosedürlerinin ve gerekli diğer dokümanların güncel versiyonlarının kurumun yerleşkesi içinde ve mümkünse kurum binası dışında belirlenecek bir yerde tutulması ve her türlü felaket senaryosu sırasında erişilebilir olması sağlanmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.13.12	2	Felaket Kurtarma Planlarının Hazırlanması	İş sürekliliği planları göz önünde bulundurularak kritik bilgi sistemleri bileşenlerine yönelik felaket kurtarma planları oluşturulmalıdır. Plan içerisinde aşağıdaki konular göz önünde bulundurulmalıdır: • Felaket kurtarma planı yapılan yerleşkenin felaket kurtarma merkezinde manuel olarak devreye alınması için gerekli minimum envanter gereksinimi • Felaket sonrası normale dönüş planı kapsamında uygulanacak adımlar • Felaket sonrası adı geçen servise ait verinin aktarma işlemi tamamlandığında kabul edilebilir kayıp veri miktarı ve niteliği, maksimum kesinti süresi ile yedekten geri dönüş süresi
3.1.13.13	2	Felaket Kurtarma Planları Kapsamında Rol ve Sorumlulukların Tanımlanması	Felaket kurtarma planlarının devreye alınması aşamasında yer alacak tüm paydaşların ve süreç içinde yer alacak personelin görev ve sorumlulukları dokümante edilmeli ve ilgili taraflara bildirilmelidir.
3.1.13.14	2	Felaket Kurtarma Çalışmalarında Üçüncü Taraf Hizmetlerin Dikkate Alınması	Felaket kurtarma planları kapsamında; hizmet alınan üçüncü tarafların rol ve sorumlulukları ile tedarik edilen hizmetlerin sürekliliği dikkate alınmalıdır.
3.1.13.15	2	Felaket Kurtarma Planlarının Test Edilmesi	Felaket kurtarma çalışmaları dâhilindeki tüm planlar yılda en az bir kez test edilmeli ve test sonuçları kayıt altına alınmalıdır.
3.1.13.16	2	Felaket Kurtarma Planlarının Güvenli Muhafazası	Felaket kurtarma çalışmaları dâhilindeki planların güncel versiyonları her türlü felaket senaryosu sırasında erişilebilir olmalıdır.
3.1.13.17	3	Kritik Sistem Sürekliliğinin Sağlanması	Kurum tarafından kritik olarak belirlenen sistem, servis, uygulama ve altyapının hizmet sürekliliğini sağlamak amacıyla gerekli yedeklilik yapıları oluşturulmalıdır. Hizmetler devreye alınırken yedeklilik testleri yapılmalıdır. Hizmet seviye taahhütleri oluşturulmalı, ölçülmeli ve raporlanmalıdır.
3.1.13.18	3	Felaket Kurtarma Merkezi Oluşturulması	Herhangi bir felaket anında bilgi sistemleri işlevlerinin sürdürülebilmesi için bir felaket kurtarma merkezi kurulmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.13.1	Yedekleme Planının Oluşturulması	Mülakat, Gözden Geçirme	Yedekleme ile ilgili nasıl bir süreç işletilmektedir? Yedeği alınacak sistemler nasıl belirlenmektedir? Yedekleme ihtiyaçlarının belirlenmesine yönelik hangi çalışmalar yapılmaktadır? Yedekleme planları oluşturulmakta mıdır? Yedeklemelerin hangi sıklıkta alınacağı nasıl belirlenmektedir?
3.1.13.2	Yedekleme Planının Periyodik Olarak Gözden Geçirilmesi	Mülakat, Gözden Geçirme	Yedekleme planları yılda en az bir kere gözden geçirilmekte midir? Yapılan gözden geçirmeler kayıt altına alınmakta mıdır? Planların gözden geçirilmesi çalışmaları için iş birimlerinden geri dönüş alınmakta mıdır?
3.1.13.3	Yedekleme İşlemleri için İz Kayıtlarının Oluşturulması	Mülakat, Gözden Geçirme	Yedekleme işlemlerine yönelik iz kayıtları tutulmakta mıdır? İz kayıtları yedekleme işlemlerine yönelik hangi bilgileri içermektedir? İz kayıtları ne kadar süre tutulmaktadır? İz kayıtları zaman damgası ile korunmakta mıdır?
3.1.13.4	Yedekten Geri Dönüş Testleri	Mülakat, Gözden Geçirme	Yedekten geri dönüş testleri yapılmakta mıdır? Geri dönüş testlerine yönelik bir zaman planı hazırlanmakta mıdır? Geri dönüş testlerinin kapsamı nasıl belirlenmektedir? Geri dönüş testlerine yönelik oluşturulmuş kayıtlar nelerdir?
3.1.13.5	Yedekleme Medyalarının Saklanması, Güvenliği ve İmhası	Mülakat, Gözden Geçirme	Yedekleme medyalarına ait envanter bulunmakta mıdır? Envanter belirli aralıklara gözden geçirilmekte midir? Yedekleme sistemi, yedekleme ile ilgili kasetler ve sunucu nerede bulunmaktadır? Kullanım ömrünü tamamlamış olan yedekler nasıl imha edilmektedir?
3.1.13.6	İş Sürekliliği Kapsamının Tanımlanması	Mülakat, Gözden Geçirme	Hangi sistemler iş sürekliliği planları kapsamında yer almaktadır? Kapsama alınacak sistemler nasıl belirlenmektedir?
3.1.13.7	İş Sürekliliği Planlarının Hazırlanması	Mülakat, Gözden Geçirme	İş sürekliliği ile ilgili planlar hazırlanmış ve belirli aralıklarla gözden geçirilmekte midir?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.13.8	İş Sürekliliği Kapsamında Rol ve Sorumlulukların Tanımlanması	Mülakat, Gözden Geçirme	İş sürekliliği planı hazırlanırken rol ve sorumluluklar tanımlanmakta mıdır? İş sürekliliği planlarında yer alan kilit personel kimlerdir? Bu personelin bulunmaması durumunda yedek personel tanımlaması yapılmış mıdır? Acil durumlar için kimlerin aranacağına ve kimlerle iletişim kurulacağına yönelik bir iletişim listesi var mıdır? Bu liste hangi sıklıkla gözden geçirilmektedir?
3.1.13.9	İş Sürekliliği Çalışmalarında Üçüncü Taraf Hizmetlerin Dikkate Alınması	Mülakat, Gözden Geçirme	İş sürekliliği planlarında, üçüncü taraflardan alınan hizmetler de değerlendirilmekte midir? Bu kapsamda üçüncü tarafların rol ve sorumlulukları tanımlanmakta mıdır?
3.1.13.10	İş Sürekliliği Planlarının Test Edilmesi	Mülakat, Gözden Geçirme	İş sürekliliği planlarına yönelik testler yapılmakta mıdır? Test kayıtları tutulmakta mıdır? Testler hangi aralıklarla gerçekleştirilmektedir?
3.1.13.11	İş Sürekliliği Planlarının Güvenli Muhafazası	Mülakat, Gözden Geçirme	İş sürekliliği planları nerede muhafaza edilmektedir?
3.1.13.12	Felaket Kurtarma Planlarının Hazırlanması	Mülakat, Gözden Geçirme	Felaket kurtarma planları yazılı hale getirilmekte midir? Felaket kurtarma planı içeriğinde hangi konular ele alınmaktadır?
3.1.13.13	Felaket Kurtarma Planları Kapsamında Rol ve Sorumlulukların Tanımlanması	Mülakat, Gözden Geçirme	Felaket kurtarma planları hazırlanırken rol ve sorumluluklar tanımlanmakta mıdır? Felaket kurtarma planlarında yer alan kilit personel ve bu personelin bulunmaması durumunda yedeği olacak personel belirlenmiş midir? Acil durumlar için kimlerin aranacağına ve kimlerle iletişim kurulacağına yönelik bir iletişim listesi var mıdır? Bu liste hangi aralıklarla güncellenmektedir?
3.1.13.14	Felaket Kurtarma Çalışmalarında Üçüncü Taraf Hizmetlerin Dikkate Alınması	Mülakat, Gözden Geçirme	Felaket kurtarma planlarında, üçüncü taraflardan alınan hizmetler değerlendirilmekte midir? Bu kapsamda üçüncü tarafların rol ve sorumlulukları tanımlanmakta mıdır?
3.1.13.15	Felaket Kurtarma Planlarının Test Edilmesi	Mülakat, Gözden Geçirme	Felaket kurtarma planları periyodik olarak test edilmekte midir? Test sonuçları kayıt altına alınmakta mıdır?
3.1.13.16	Felaket Kurtarma Planlarının Güvenli Muhafazası	Mülakat, Gözden Geçirme	Felaket kurtarma planları nerede muhafaza edilmektedir?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.13.17	Kritik Sistem Sürekliliğinin Sağlanması	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Üzerinde kritik veri bulunan, kritik servis sunulan, kurumlar tarafından kritik olarak belirlenen altyapı ve sistemlerin hizmet sürekliliği nasıl sağlanmaktadır? Cihaz, enerji, personel, ağ vb. yedekliliği nasıl kurgulanmaktadır? Hizmetler devreye alınırken yedeklilik testleri yapılmakta mıdır? Hizmet seviye taahhütleri var mıdır? Hizmet seviyesi nasıl ve hangi aralıklarla ölçülmekte ve raporlanmaktadır?
3.1.13.18	Felaket Kurtarma Merkezi Oluşturulması	Mülakat, Gözden Geçirme	Felaket kurtarma merkezi var mıdır? Felaket kurtarma merkezinin bilgi güvenliği kriterleri kurumun bilgi güvenliği gereksinimlerini karşılamakta mıdır? Felaket kurtarma merkezi, kurumun asıl sistemlerine göre nasıl konumlandırılmıştır?

3.1.14. Uzaktan Çalışma

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.14.1	1	Uzaktan Çalışma Politikasının Hazırlanması ve Uygulanması	Kurum tarafından uzaktan çalışma faaliyetlerinde uygulanması gereken şartları ve kısıtlamaları tanımlayan bir politika hazırlanmalı ve uygulanmalıdır. Hazırlanan politika asgari olarak aşağıdaki hususları içermelidir. • Önerilen uzaktan çalışma ortamı • Zararlı yazılımlardan korunma ve güvenlik duvarı gereksinimleri • Yetkisiz erişimin engellenmesi • Kablosuz ağ hizmetlerinin kullanımı • Yedekleme gereksinimleri • Fiziksel güvenlik • Kişilere ait teçhizatlar üzerinde geliştirilen işlere ait fikri mülkiyet hakları ile ilgili anlaşmazlıklar • Uzaktan çalışmanın sona ermesi durumunda; yetki ve erişim haklarının iptali ve kullanılan teçhizatın iadesi
3.1.14.2	1	Ekipman Güvenliğinin Sağlanması	Kurum personeli, uzaktan çalışma faaliyetlerinde yalnızca kurum tarafından sağlanan ve/veya yapılandırma ayarları kurumun bilgi güvenliği gereksinimlerine uygun olan cihazları kullanmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.14.3	1	Dosya Paylaşımı	Uzaktan çalışma faaliyetlerinde, çalışma dosyalarını paylaşmak için kurumsal kaynaklar kullanılmalıdır.
3.1.14.4	1	Farkındalık Eğitimlerinin Verilmesi	Uzaktan çalışan kurum personeline özellikle güçlü parola kullanımı, sosyal mühendislik ve kimlik avı/oltalama saldırıları gibi konularda farkındalık eğitimleri verilmelidir. Bk. Tedbir No: 3.5.2.1
3.1.14.5	1	Zararlı Yazılımdan Korunma Uygulamaları	Uzaktan çalışma kapsamında kurum bilgilerinin işleneceği cihazlarda zararlı yazılımdan korunma uygulaması kullanılmalı ve zararlı yazılımdan korunma uygulamalarında en güncel yama dosyalarının bulunması ve imza veri tabanının güncel olması sağlanmalıdır. Bk. Tedbir No: 3.1.5.1 Bk. Tedbir No: 3.1.5.4
3.1.14.6	1	Güncel İşletim Sistemi ve Uygulamaların Kullanılması	Uzaktan çalışma kapsamında kurum bilgilerinin işleneceği cihazların işletim sistemlerinin ve kullanılan uygulamaların güncel olması sağlanmalı, güvenlik yamaları yüklü olmalıdır. Bk. Bölüm 5.1
3.1.14.7	1	Kurum Kaynaklarına Uzaktan Erişim	Uzaktan çalışma kapsamında kurum kaynaklarına erişim VPN teknolojileri ve çok faktörlü kimlik doğrulama ile sağlanmalıdır. Erişimler kurum politikalarına göre en az yetki prensibine göre sınırlandırılmalıdır. Bk. Tedbir No: 3.1.6.8
3.1.14.8	1	Video Konferans Uygulamalarının Kullanımı	Video konferans uygulamaları kurum içerisinde barındırılmalıdır. Kurum içerisinde barındırılmayan üçüncü taraf bir uygulama kullanılacak ise uygulama açık kaynak kodlu olmalıdır.
3.1.14.9	1	Güçlü Parola Kullanımı	Uzaktan çalışma kapsamında kurumun politikalarına uygun güçlü parolaların kullanılması sağlanmalıdır.
3.1.14.10	1	Güncel Video Konferans Uygulamalarının Kullanılması	Video konferans uygulamasının güncel olması ve uygulamada en güncel yamaların yüklü olması sağlanmalıdır.
3.1.14.11	1	Video Konferans Görüşmelerine Yetkisiz Katılım	Video konferans görüşmelerine sadece toplantı bağlantı adresi kullanılarak yapılabilecek yetkisiz erişimler engellenmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.14.12	1	Video Konferans Paylaşım İşlemleri ve Sohbet Özelliği	Video konferans uygulaması üzerinden toplantı sırasında toplantı moderatörü/yardımcı moderatör onayı ile; • İstenilen kullanıcının ekran paylaşımı durdurulabilmeli, • Sohbet (chat) özelliği devre dışı bırakılabilmeli, • Dosya paylaşımı özelliği devre dışı bırakılabilmelidir. Video konferans uygulaması üzerinden yapılacak dosya paylaşımlarında dosya kontrolü yapılmalıdır. Dosya kontrolü yapılamıyorsa video konferans uygulaması üzerinden dosya paylaşımı yapılması engellenmelidir. Bk. Tedbir No: 3.2.4.5 Video konferans uygulaması üzerinden yapılan görüşmeler (dosya paylaşımı, ses, video, chat) uçtan uca şifreli olmalıdır.
3.1.14.13	1	Video Konferans Katılımcı Yönetimi	Video konferans uygulaması üzerinden toplantıya erişimin toplantı moderatöründen önce sağlanması engellenmelidir.
3.1.14.14	1	Video Konferans Toplantı Odası İsimlendirmeleri	Video konferans uygulaması üzerinde yapılan toplantılarda, toplantı odası isimlendirmeleri karmaşık olarak oluşturulmalıdır.
3.1.14.15	1	Kullanıcı Bilgisayarında Güvenlik Duvarının Aktif Olması	Uzaktan çalışan kullanıcı bilgisayarlarında güvenlik duvarı yazılımları aktif durumda olmalıdır. Bk. Tedbir No: 3.1.6.11
3.1.14.16	2	Bekleme Odası Özelliğinin Bulunması	Video konferans uygulaması bekleme odası özelliği içermelidir. Katılımcılar, konferansı organize eden kişinin manuel onayı ile katılım sağlamalıdır.
3.1.14.17	3	Uç Nokta Seviyesinde Veri Sızıntısının Önlenmesi	Uzaktan çalışan kullanıcı bilgisayarlarında olası veri sızıntısını engellemek amaçlı uç nokta seviyesinde veri sızıntısını önlemeye yönelik güvenlik önlemleri alınmalıdır. Bk. Tedbir Başlık No: 3.1.7
3.1.14.18	3	Erişimin Kurum Bilgisayarları ile Sınırlandırılması	Uzaktan çalışma kapsamında sadece kurum cihazları üzerinden erişim sağlanmalıdır. VPN erişiminde kurum tarafından sağlanan cihazlar için oluşturulan sertifikaların kullanılması sağlanmalıdır.
3.1.14.19	3	Kuruma Uzaktan Bağlanan Cihazların Yönetimi	Bk. Tedbir No: 3.1.6.32

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.14.1	Uzaktan Çalışma Politikasının Hazırlanması ve Uygulanması	Mülakat, Gözden Geçirme	Kurum tarafından uzaktan çalışma faaliyetlerinde uygulanması gereken şartları ve kısıtlamaları tanımlayan bir politika tanımlanmış mıdır? İlgili politika uygulanmakta mıdır? Uzaktan çalışma politikası kapsamında hangi konular ele alınmaktadır?
3.1.14.2	Ekipman Güvenliğinin Sağlanması	Mülakat, Güvenlik Denetimi	Kurum personeli tarafından uzaktan çalışma faaliyetlerinde kullanılacak cihazlara yönelik tanımlanan bilgi güvenliği gereksinimleri nelerdir? Cihazlara yönelik tanımlanan bilgi güvenliği gereksinimlerine uyum nasıl kontrol edilmektedir?
3.1.14.3	Dosya Paylaşımı	Mülakat, Güvenlik Denetimi	Uzaktan çalışma faaliyetlerinde çalışma dosyalarını paylaşmak amacıyla hangi kaynaklar kullanılmaktadır?
3.1.14.4	Farkındalık Eğitimlerinin Verilmesi	Mülakat	Bilgi güvenliği farkındalık eğitimleri kapsamında uzaktan çalışma faaliyetleri ile ilgili hangi konular ele alınmaktadır?
3.1.14.5	Zararlı Yazılımdan Korunma Uygulamaları	Mülakat, Güvenlik Denetimi	Uzaktan çalışma kapsamında kullanılan cihazlarda hangi zararlı yazılımdan korunma programları kullanılmaktadır? Kullanımda olan zararlı yazılımdan korunma programları versiyonları nelerdir? Güncelleme durumu nasıl kontrol edilmektedir? Zararlı yazılımdan korunma politikaları nasıl yönetilmektedir?
3.1.14.6	Güncel İşletim Sistemi ve Uygulamaların Kullanılması	Mülakat, Güvenlik Denetimi	Uzaktan çalışma kapsamında kullanılan cihazlarda yer alan işletim sistemlerine ait versiyonlar nedir? Kullanılan uygulamalar güncel midir? Güncellik durumu nasıl takip edilmektedir?
3.1.14.7	Kurum Kaynaklarına Uzaktan Erişim	Mülakat, Güvenlik Denetimi	Uzaktan çalışma kapsamında kurum kaynaklarına erişim nasıl sağlanmaktadır? Kullanıcı kimlik doğrulama nasıl yapılmaktadır? Erişimler sınırlandırılmakta mıdır?
3.1.14.8	Video Konferans Uygulamalarının Kullanımı	Mülakat, Güvenlik Denetimi	Kurum hangi video konferans uygulamasını kullanmaktadır? Kurum içerisinde barındırılan video konferans uygulaması var mıdır?
3.1.14.9	Güçlü Parola Kullanımı	Mülakat, Güvenlik Denetimi	Uzaktan çalışma kapsamında dikkate alınması gereken bir parola politikası tanımlanmış mıdır? Parola politikası hangi kurallara uyumu zorunlu kılmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.14.10	Güncel Video Konferans Uygulamalarının Kullanılması	Mülakat, Güvenlik Denetimi	Video konferans uygulaması güncel midir? Kontrolü nasıl sağlanmaktadır?
3.1.14.11	Video Konferans Görüşmelerine Yetkisiz Katılım	Mülakat, Güvenlik Denetimi	Video konferans görüşmelerine yetkisiz katılımı engellemek için hangi kontroller uygulanmaktadır?
3.1.14.12	Video Konferans Paylaşım İşlemleri ve Sohbet Özelliği	Mülakat, Güvenlik Denetimi	Video konferans uygulaması üzerinden toplantı sırasında ekran paylaşımlarının yönetimine ilişkin hangi işlemler yapılabilmektedir? Video konferans uygulaması sohbet özelliği devre dışı bırakılabilmekte midir? Video konferans uygulaması üzerinden dosya paylaşımı özelliği devre dışı bırakılabilmekte midir? Video konferans uygulaması tarafından dosya paylaşım imkânının sunulması durumunda, dosya kontrolü nasıl yapılmaktadır? Video konferans uygulaması üzerinden yapılan görüşmeler uçtan uca şifreli olarak sağlanmakta mıdır?
3.1.14.13	Video Konferans Katılımcı Yönetimi	Mülakat, Güvenlik Denetimi	Video konferans uygulaması üzerinden katılımcıların toplantıya erişimleri, ancak toplantı moderatörünün erişimi sonrasında olacak şekilde ayarlanmakta mıdır?
3.1.14.14	Video Konferans Toplantı Odası İsimlendirmeleri	Mülakat, Güvenlik Denetimi	Video konferans uygulaması üzerinden oluşturulan toplantı odası isimlendirmeleri karmaşık olarak oluşturulmakta mıdır?
3.1.14.15	Kullanıcı Bilgisayarında Güvenlik Duvarının Aktif Olması	Mülakat, Güvenlik Denetimi	Uzaktan çalışan kullanıcı bilgisayarlarında güvenlik duvarı yazılım aktif olarak kullanılmakta mıdır?
3.1.14.16	Bekleme Odası Özelliğinin Bulunması	Mülakat, Güvenlik Denetimi	Video konferans başladıktan sonra sadece yetkili kullanıcıların katılımının sağlanabilmesi için hangi kontroller uygulanmaktadır?
3.1.14.17	Uç Nokta Seviyesinde Veri Sızıntısının Önlenmesi	Mülakat, Güvenlik Denetimi	Uzaktan çalışan kullanıcı bilgisayarlarında veri sızıntısı nasıl önlenmektedir?
3.1.14.18	Erişimin Kurum Bilgisayarları ile Sınırlandırılması	Mülakat, Güvenlik Denetimi	Uzaktan çalışma kapsamında kurum cihazları dışında bir erişim imkânı bulunmakta mıdır?
3.1.14.19	Kuruma Uzaktan Bağlanan Cihazların Yönetimi	Mülakat, Güvenlik Denetimi	Bk. Denetim No: 3.1.6.32

3.2. Uygulama ve Veri Güvenliği

Amaç

Bu güvenlik tedbiri ana başlığının amacı, uygulama ve veri güvenliği çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. "Uygulama ve Veri Güvenliği" ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Kimlik Doğrulama
- Oturum Yönetimi
- Yetkilendirme
- Dosyaların ve Kaynakların Güvenliği
- Güvenli Kurulum ve Yapılandırma
- Güvenli Yazılım Geliştirme
- Veri Tabanı ve Kayıt Yönetimi
- Hata Ele Alma ve Kayıt Yönetimi
- İletişim Güvenliği
- Kötücül İşlemleri Engelleme
- Dış Sistem Entegrasyonlarının Güvenliği

3.2.1. Kimlik Doğrulama

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.1.1	1	Kullanıcı Yönetiminin Yapılabilmesi	Uygulamalar kullanıcı hesaplarının yönetimini sağlayan arayüzlere sahip olmalı ve bu arayüzlere yalnızca yetkili kullanıcıların erişebilmesi sağlanmalıdır. Kullanıcı hesapları, geçici (belirli bir süre, koşul vb. boyunca) veya kalıcı (aksi belirtilmedikçe sürekli) olarak kilitlenebilmelidir. Kalıcı olarak kilitlenen hesap, üzerindeki geçici kilit kaldırılsa dahi kilitli kalmalıdır.
3.2.1.2	1	Ortak Hesap Kullanılmaması	Kullanıcı tanımlamaları, yapılan işlemlerin izlenebilirliğini sağlayacak ve tekil olarak kişi veya sistemi işaret edecek şekilde yapılmalıdır.
3.2.1.3	1	Kimlik Doğrulama İşlemleri için İz Kayıtlarının Oluşturulması	Tüm başarılı ve başarısız kimlik doğrulama girişimleri için özet veri içerecek şekilde iz kaydı oluşturulmalıdır. Bk. Tedbir No: 3.1.8.1

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.1.4	1	Kimlik Doğrulama Bilgilerinin Güvenliği	Tüm parola alanlarında kullanıcı giriş yaparken kullanıcının parolası varsayılan olarak maskelenmeli ve açık olarak görünmemelidir. Unutulan parola işlevi ve diğer kurtarma yolları geçerli parolayı açığa çıkarmamalı ve yeni parola kullanıcıya açık metin olarak gönderilmemelidir. Kimlik doğrulama bilgileri sadece güvenli kanallar üzerinden taşınmalıdır. Parola veya diğer kimlik doğrulama bilgileri açık metin olarak saklanmamalıdır. Bu bilgileri korumak için kaba kuvvet saldırılarına dayanıklı, güçlü kriptografik yöntemler (şifreleme, tuzlama, özet alma) kullanılmalıdır.
3.2.1.5	1	İlk Parolanın Belirlenmesi	İlk parola belirleme işlemi kullanıcı tarafından yapılmayacak ise, güvenli bir parola belirleme mekanizması ve üretilmiş bu parolaların güvenli olarak taşınması için iletme mekanizması oluşturulmalıdır. Ayrıca, bu parolalar ilk kullanımda değiştirilmeye zorlanmalıdır.
3.2.1.6	1	Varsayılan Kullanıcı Adı ve Parolaların Kullanılmaması	Tüm yazılım bileşenlerinde (veri tabanı, uygulama sunucu, paket program vb.) varsayılan veya tahmin edilebilir kullanıcı adı ve parolalar değiştirilmelidir. Bu gibi bilgilere sahip hesaplar kaldırılarak kullanılmaması sağlanmalıdır. Tahmin edilebilir bilgilere sahip veya varsayılan hesapların kullanılmasının zorunluluk olduğu durumlarda ilgili parolalar değiştirilerek kullanılmalı ve hesaplara ait her aktivite izlenmelidir. Bu hesapların parolaları periyodik olarak veya her kullanım sonrasında güncellenmelidir.
3.2.1.7	1	Kaynak Kodda Kimlik Doğrulama Bilgilerinin Bulunmaması	Kaynak kodda veya kaynak kod depolarında gizli bilgiler, API anahtarları ve parolalar yer almamalıdır. Kullanılan tüm kimlik doğrulama bilgileri şifrelenmeli ve korunan bir yerde depolanmalıdır. Açık anahtar altyapısı tabanlı kimlik doğrulama kullanılıyorsa özel anahtara sadece yetkili kullanıcının erişimine izin verecek mekanizmalar mevcut olmalıdır.
3.2.1.8	1	Parola Yönetimi	Parola giriş alanları uzun ve karmaşık bir parola girilmesini engellememeli, parola cümle (deyimsel parola) kullanımına izin vermeli ya da teşvik etmelidir. Kurumlar güvenlik gereksinimlerine göre parola politikası belirlemelidir. Ayrıca parolalar için bir en uzun geçerlilik süresi tanımlanmış olmalıdır. Değişen parola fonksiyonu eski parolayı, yeni parolayı ve bir parola onayını kapsamalıdır. Kimlik doğrulama için bilgi sorgulayan sorular (gizli sorular) kullanılmamalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.1.9	1	Kimlik Doğrulama Fonksiyonlarına Yapılacak Saldırılara Karşı Önlem Alınması	Oturum açma, parola sıfırlama ya da hesap unutma gibi işlevler sıralı denemelerle bilgi edinmeye olanak vermemelidir. Kaba kuvvet saldırılarını önlemek amacıyla (istek sınırlandırma, IP bloklama, CAPTCHA vb.) etkin güvenlik yöntemleri uygulanmalıdır. Kimlik doğrulama işlemlerinin başarılı olup olmadığı paket boyutu gibi değerler üzerinden anlaşılamamalıdır. Hesaplara erişim için yeniden oynatma (replay) saldırılarına dayanıklı bir kimlik doğrulama mekanizması kullanılmalıdır.
3.2.1.10	2	Güçlü Kimlik Doğrulama Yöntemlerinin Desteklenmesi	Unutulan parolanın sıfırlaması kullanıcı adının unutulması vb. durumlar için; kısa ileti, e-posta onayı, mobil onay, çevrimdışı onay vb. yöntemler kullanılmalıdır. İlgili yöntemler kullanılırken sahip olunan, bilinen ve biyometrik faktörlerin en az ikisinden yararlanılmalıdır. Hassas işlevler gerçekleştirilmeden önce, yeniden kimlik doğrulama, daha güçlü bir mekanizmayla kimlik doğrulama, çok faktörlü kimlik doğrulama veya işlem imzalama gibi yöntemler uygulanmalıdır. Uygulamanın ilgili yönetim arayüzlerine yalnızca yetkili kullanıcılar tarafından erişim sağlanmalıdır. Açık anahtar altyapısı tabanlı kimlik doğrulama kullanılıyorsa sertifika yolu doğrulanmalı ve kullanıcının sertifikası sistem üzerindeki geçerli kullanıcı veya grup bilgisi ile eşleştirilmelidir.
3.2.1.11	2	Hesap Kurtarma Seçeneklerinin Güvenliği	Hesaba yeniden erişebilecek tüm hesap kimlik doğrulama işlevleri (parola güncelleme, parolamı unuttum, devre dışı/kayıp simge (token), süresi dolmuş parolanın güncellenmesi, yardım masası vb.) en az ana kimlik doğrulama mekanizması kadar güvenli olmalıdır.
3.2.1.12	2	Kullanılmayan Hesapların Tespiti	Uygulama, belirli bir süre boyunca hiç kullanılmamış olan hesapları raporlayabilmelidir. Bu hesaplar pasif duruma getirilmeli veya silinmelidir.
3.2.1.13	3	Merkezi Kimlik Doğrulama Mekanizmalarının Kullanılması	Kurumsal merkezi kimlik yönetim ve doğrulama sistemleri kullanılmalı veya e-Devlet sistemi ile entegrasyon sağlanmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.1.1	Kullanıcı Yönetiminin Yapılabilmesi	Mülakat, Gözden Geçirme	Uygulamalarda kullanılan bir kimlik doğrulama mekanizması mevcut mu? Tasarım dokümanında kullanıcı yönetimi için süreç/işlev tanımlanmış mı? Uygulamalar, kullanıcı hesaplarını yönetmek için ilgili arayüzlere sahip mi? Kullanıcı hesapları geçici veya kalıcı olarak kilitlenebiliyor mu? Uygulamalar üzerinden geçici/kalıcı olarak kilitlenmiş hesaplar tespit edilebiliyor mu?
3.2.1.2	Ortak Hesap Kullanılmaması	Mülakat, Güvenlik Denetimi	Kullanıcıların yerine işlem yapan yazılımsal süreçler (web servisleri, kurumsal yazılımlar vb.) kullanıcı olarak tanımlanabiliyor mu? Kullanıcıların yerine işlem yapan yazılımsal süreçlerin (web servisleri, kurumsal yazılımlar vb.) gerçekleştirdiği işlemlerin kaydı oluşturuluyor mu? Aynı hesabın birden fazla kullanıcı tarafından kullanılmasını (ortak hesap) önlemek adına tekil kullanıcılar tanımlanmakta mıdır?
3.2.1.3	Kimlik Doğrulama İşlemleri için İz Kayıtlarının Oluşturulması	Mülakat, Gözden Geçirme	Kullanıcıların oturum açma istekleri ve ilgili isteklere verilen yanıtlar/işlem sonuçları kayıt altına alınıyor mu? Şüpheli kimlik doğrulama işlemleri kayıt altına alınıyor mu? İz ne kadar süre için saklanıyor?
3.2.1.4	Kimlik Doğrulama Bilgilerinin Güvenliği	Mülakat, Gözden Geçirme, Kaynak Kod Analizi	Kullanıcı parolaları oluşturulurken veya güncellenirken giriş yapılan parolalar nasıl görüntülenmektedir? Parola sıfırlama süreci tasarım dokümanında tanımlanmış mıdır? Parola sıfırlama işlemi kapsamında yeni parola nasıl oluşturulmaktadır? Parolalar veri tabanında hangi kriptografik yöntemler kullanılarak saklanmaktadır? Bu kriptografik yöntemler ulusal ve/veya uluslararası standartlar tarafından güvenli kabul ediliyor mu? Kritik bilgilerin taşınması esnasında ifşa olmaması için iletişimde ne gibi önlemler alınmaktadır?
3.2.1.5	İlk Parolanın Belirlenmesi	Mülakat, Gözden Geçirme, Sızma Testi	Parola belirleme süreci tasarım dokümanında tanımlanmış mıdır? Parola belirleme sürecinde ilk parolanın güvenli olarak oluşturulmasında ve iletiminde hangi yöntemler kullanılmaktadır? Kullanıcı, ilk parolasını kendisi oluşturmadığında ilgili parolayı ilk kullanımda değiştirmeye zorlanıyor mu?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.1.6	Varsayılan Kullanıcı Adı ve Parolaların Kullanılmaması	Mülakat, Güvenlik Denetimi	Uygulamaya erişim için varsayılan kullanıcılar tanımlanmış mıdır? Uygulamanın kullandığı veri tabanı ve uygulama sunucularında varsayılan kullanıcı bulunmakta mıdır? Varsayılan kullanıcıların aktiviteleri izlenmekte midir? Parola değişim periyodu politikada nasıl tanımlanmıştır?
3.2.1.7	Kaynak Kodda Kimlik Doğrulama Bilgilerinin Bulunmaması	Mülakat, Gözden Geçirme, Kaynak Kod Analizi	Uygulama kodlarında herhangi bir kullanıcıya ait bilgiler (kullanıcı adı, parola, anahtar vb.) yer almakta mıdır? Uygulamanın diğer hizmetlere erişmek için kullandığı kimlik doğrulama bilgileri nasıl depolanmakta ve kullanılmaktadır?
3.2.1.8	Parola Yönetimi	Mülakat, Gözden Geçirme, Sızma Testi	Uygulama hesaplarının parolalarında kullanmak üzere mevcut bir parola politikası tanımlanmış mıdır? Bu parola politikasının işletilmesini uygulama destekliyor mu? Uygulama, parola değiştirme işlemi esnasında kullanıcının mevcut parolası üzerinden doğrulama yapıyor mu? Uygulamada, parola değiştirme işlemi esnasında yeni parolanın tekrar girilmesi (parola onayı) istenerek istenmeyen/bilinmeyen bir değer ile parolanın değiştirilmesi engelleniyor mu?
3.2.1.9	Kimlik Doğrulama Fonksiyonlarına Yapılacak Saldırılara Karşı Önlem Alınması	Mülakat, Güvenlik Denetimi, Sızma Testi	Uygulama yaygın kimlik doğrulama saldırılarına karşı (sürekli istek gönderme, yeniden oynatma, şüpheli aktivitelere ait sürekli alarmlar ürettirme vb.) zafiyet içermekte midir? Araçlarla otomatik yapılan yaygın kimlik doğrulama saldırılarını önlemek için hangi önlemler alınmıştır? Bu saldırılara karşı neler yapılacağı dokümante edilmiş midir?
3.2.1.10	Güçlü Kimlik Doğrulama Yöntemlerinin Desteklenmesi	Mülakat, Güvenlik Denetimi, Sızma Testi	Uygulama kimlik doğrulamak için hangi ek güvenlik önlemlerini kullanıcılarına sunmaktadır? Kimlik doğrulama mekanizmalarında elektronik imza gibi güçlü yöntemlerin kullanılabilmesi için seçenek sağlanıyor mu? Uygulamanın yönetim arayüzlerine güvenilmeyen taraflarca erişilmesini engellemek için kimlik doğrulama, yetkilendirme vb. mekanizmalar tanımlanmış mı? Kimlik doğrulama mekanizmasında kullanılan açık anahtar altyapısının sertifika yolu doğrulanmakta mıdır? Unutulan parola ve diğer kurtarma işlemleri nasıl gerçekleştiriliyor?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.1.11	Hesap Kurtarma Seçeneklerinin Güvenliği	Mülakat, Güvenlik Denetimi, Sızma Testi	Profil güncelleme, parolamı unuttum, devre dışı/kayıp simge (token), süresi dolmuş parolanın güncellenmesi ve yardım masası ile hesap kurtarma yöntemlerinin güvenliği nasıl sağlanmıştır? Uygulama kullanıcı bilgilerinin değişmesi ile sonuçlanacak tüm durumlar için iz kaydı oluşturmakta mıdır?
3.2.1.12	Kullanılmayan Hesapların Tespiti	Mülakat, Güvenlik Denetimi	Uygulama, belirli bir süre boyunca hiç kullanılmamış olan hesapları raporlayabilmekte midir? Bu hesapların yönetimi için nasıl bir yol izlenmektedir?
3.2.1.13	Merkezi Kimlik Doğrulama Mekanizmalarının Kullanılması	Mülakat, Güvenlik Denetimi	Merkezi kimlik yönetim ve doğrulama sistemi kullanılıyor mu? Kimlik doğrulama için E-Devlet sistemi ile entegrasyon sağlanmış mıdır?

3.2.2. Oturum Yönetimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.2.1	1	Kimlik Doğrulama İşlemleri Sonrasında Yeni Bir Oturum ve Yeni Bir Oturum Kimliğinin Üretilmesi	Tüm kimlik doğrulama ve yeniden kimlik doğrulama işlemleri sonucunda yeni bir oturum ve yeni bir oturum kimliği üretilmelidir. Oturum kimlikleri yeterince uzun olmalı, rastgele olmalı ve etkin oturumlar içerisinde tekil olmalıdır. Oluşturulan oturum kimliği yalnızca bir kez kullanılmalıdır.
3.2.2.2	1	Oturum Kimliğinin Doğrulanması ve Güvenliğinin Sağlanması	Yalnızca uygulama tarafından üretilen oturum kimliklerinin uygulamada aktif oturum kimliği olarak kullanıldığı doğrulanmalıdır. Oturum kimliğinin URL, hata mesajları ve iz kayıtları içerisinde yer almaması sağlanmalıdır. URL içerisinde oturum kimliğinin yeniden yazılması engellenmelidir.
3.2.2.3	1	Kullanıcı Oturumlarının Sonlandırılması	Kimlik doğrulamayla erişilen tüm sayfalardan oturum kapatma işlevine erişilebilmelidir. Buna ek olarak, oluşturulan oturum kimliğinin geçerlilik süresi belirlenmelidir. İlgili süre sonunda, belirli süre etkinlik olmadığında veya kullanıcı oturumu kapattığında oturum geçersiz hale gelmelidir. İlgili sürelerin güncellenmesi sürecinde yetkilendirme mekanizmasından faydalanılmalıdır. Ayrıca oturumun geçersiz olmasına sebep olacak bilgilerin değişmesi durumunda (kullanıcı parolasının güncellenmesi, yetkilerin güncellenmesi vb.) etkin oturumların sonlandırılması sağlanmalıdır. Oturum sonlandığında istemci ve sunucuda oturum ile ilgili tüm geçici depolama alanları ve çerezler uygulama tarafından silinmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.2.4	1	Oturum Güvenlik Mekanizmalarının Kullanılması	Kullanılan çatının, programlama dilinin ve iletişim protokolünün sağladığı oturum güvenlik mekanizmaları kullanılmalıdır. Web uygulamalarının oturum çerezlerinde HTTPOnly, Secure, SameSite vb. bayraklar kullanılmalıdır. Tanımlama bilgilerinde depolanan oturum kimliklerinin yolları, uygulama için uygun kısıtlayıcı bir değere ayarlanmalıdır.
3.2.2.5	3	Kullanıcıların Aktif Oturumlarını Yönetebilmesi	Kullanıcılar uygulamadaki etkin oturumlarını görüntüleyebilmeli ve aktif oturumlarından istediğini sonlandırabilmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.2.1	Kimlik Doğrulama İşlemleri Sonrasında Yeni Bir Oturum ve Yeni Bir Oturum Kimliğinin Üretilmesi	Mülakat, Gözden Geçirme, Sızma Testi	Yeni oturum açıldığında yeni bir kimlik (oturum anahtar değeri) oluşturuluyor mu? Kullanılan çatı ve geliştirme platformu, yeni oturum açıldığında yeni kimlik (oturum anahtar değeri) oluşturulmasını destekliyor mu? Kimlik doğrulama yapmak amacıyla kullanılan bileşenler üzerinde her oturum açıldığında farklı bir kimliğin oluşturulduğunu kontrol için sızma testi gerçekleştirildi mi?
3.2.2.2	Oturum Kimliğinin Doğrulanması ve Güvenliğinin Sağlanması	Mülakat, Gözden Geçirme, Kaynak Kod Analizi	Uygulama tarafından üretilmemiş ancak farklı yöntemlerle/farklı uygulamalarla oluşturulmuş oturum kimliklerinin sistemde kullanılamadığı test edildi mi? Uygulama, farklı yöntemlerle/farklı uygulamalarla oluşturulmuş oturum kimliklerinin kullanıldığı durumda nasıl davranmaktadır? Oturum kimliğinin güvenliğinin sağlanması için uygulama içerisinde güvenlik önlemi tanımlanmış mıdır? Hata mesajlarının ve iz kayıtlarının hangi bilgileri içereceği / içeremeyeceği tasarım dokümanında tanımlanmış mıdır?
3.2.2.3	Kullanıcı Oturumlarının Sonlandırılması	Mülakat, Gözden Geçirme, Sızma Testi	Kullanıcı oturumu kapattığında oturumun sonlandığı test edilmiş midir? İşlem yapılmadan beklenecek süre ve/veya oturum kimliğinin geçerlilik süresi yetkisiz güncellenebiliyor mu? Oluşturulan oturum kimliğinin geçerlilik süresi belirlenmiş midir? İşlem yapılmadan beklenen geçerlilik süresi sonunda oturum sonlandırılıyor mu? Kullanıcı, oturumun geçersiz olmasına sebep olacak bilgilerini değiştirdikten sonra etkin olan tüm oturumlarını sonlandırabiliyor mu? Oturum sonlandığında oturum ile ilgili tüm geçici depolama alanları ve çerezler uygulama tarafından siliniyor mu?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.2.4	Oturum Güvenlik Mekanizmalarının Kullanılması	Mülakat, Gözden Geçirme, Sızma Testi	Uygulamanın geliştirme platformunun hangi güvenlik mekanizmaları kullanılmaktadır? Veri taşıma için hangi protokoller (HTTP, FTP vb.) kullanılmaktadır? Bu protokollerin güvenliği için hangi önlemler alınmaktadır?
3.2.2.5	Kullanıcıların Aktif Oturumlarını Yönetebilmesi	Mülakat, Güvenlik Denetimi	Uygulama arayüzleri kullanılarak etkin olan oturumlar listelenebiliyor mu? Uygulama arayüzleri kullanılarak etkin olan oturumlar sonlandırılabiliyor mu?

3.2.3. Yetkilendirme

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.3.1	1	Yetki Denetimi	Kullanıcıların uygulamaya erişimlerini tanımlayan yetki matrisi oluşturulmalı ve belirli aralıklarla güncellenmelidir. Kullanıcı sadece yetkilendirildiği uygulama bileşenlerine ve kaynaklara erişebilmeli ve bunları kullanabilmelidir. Uygulamaya yapılan her istek için yetki denetimi kontrolü uygulanmalıdır.
3.2.3.2	1	Kritik Veriye ve Kaynaklara Erişimlerin Kayıt Altına Alınması	Uygulama, yönettiği veriye ve kaynaklara erişimleri kayıt altına alabilmek için denetim kayıtları üretebilmelidir. Bk. Tedbir No: 3.1.8.1
3.2.3.3	1	En Az Yetki Prensibinin Uygulanması	Kullanıcılara verilecek yetkiler, yürütülen görevler ve ihtiyaçlar doğrultusunda belirlenmelidir. En az yetki prensibine göre kullanıcının gerçekleştirebileceği ilgili işlemler için gereken asgari yetkilerin haricinde bir ayrıcalık tanımlanmamalıdır.
3.2.3.4	3	İçerik Duyarlı ve Gelişmiş Erişim Denetimi	Uygulama içerik duyarlı (zaman, konum, IP adresi gibi öznitelikler) erişim denetimi yapabilmelidir. Uygulama; fonksiyonlara, kaynaklara, veriye erişim sürelerini, kullanım oranlarını veya kullanım sıklığını sınırlandırabilmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.3.1	Yetki Denetimi	Mülakat, Gözden Geçirme, Sızma Testi	Uygulamalara erişimi tanımlayan yetki matrisi oluşturulmuş ve belirli aralıklara güncellenmekte midir? Uygulamada kullanıcının yalnızca ilgili olduğu uygulama bileşenlerine ve kaynaklara erişebilmesini sağlayacak bir yetkilendirme mekanizması tanımlanmış mı? Uygulamada kullanıcıların diğer kullanıcılara ait kritik bilgilere erişmesini engellemek için nasıl bir yetkilendirme mekanizması tanımlanmıştır? Uygulamaya gelen her istek için yetki denetimi kontrolü yapılmakta mıdır?
3.2.3.2	Kritik Veriye ve Kaynaklara Erişimlerin Kayıt Altına Alınması	Mülakat, Gözden Geçirme, Sızma Testi	Veri akışı ve kaynaklara erişim için iz ve denetim kayıtları oluşturuluyor mu? Kayıtlar hangi bilgileri içeriyor? Kayıtlar kullanıcı arayüzünden sorgulanabiliyor mu? Kayıtlar silinebiliyor veya değiştirilebiliyor mu? Kayıtlar ne kadar süre ile saklanıyor?
3.2.3.3	En Az Yetki Prensibinin Uygulanması	Mülakat, Güvenlik Denetimi	Kullanıcılara verilen yetkiler, yürütülen görevler ve ihtiyaçlar doğrultusunda mı belirlenmektedir?
3.2.3.4	İçerik Duyarlı ve Gelişmiş Erişim Denetimi	Mülakat, Güvenlik Denetimi, Sızma Testi	Uygulamada yetkilendirmeler zaman, konum, kullanılan ağ, IP adresi gibi özelliklere göre sınırlandırılabiliyor mu? Uygulama yetkilendirme ile erişimleri erişim süresi, kullanım sıklığı gibi parametrelere göre sınırlandırabiliyor mu? Uygulama erişim denetleme mekanizmasında içeriğe duyarlı kontroller ve yetkilendirmeler tanımlanabiliyor mu?

3.2.4. Dosyaların ve Kaynakların Güvenliği

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.4.1	1	Yapılandırma Dosyaları, Denetim Kayıtları, İz Kayıtları vb. Bilgilerin Kullanıcı Verisiyle Aynı Konumda Depolanmaması	Uygulamanın sahip olduğu sistem ve yapılandırma dosyaları ile denetim kayıtları ve iz kayıtları gibi bilgiler kullanıcı verisiyle aynı konumda (dizin, sistem bölümü vb.) depolanmamalıdır. Bk. Tedbir No: 3.1.8.1

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.4.2	1	Uygulama Bileşenlerine Dış Kaynaklardan Erişimin Kısıtlanması	Uygulamanın bileşenlerinin çalıştığı sunuculardan (web sunucusu, uygulama sunucusu vb.), kendi sınırları dışında bulunan / kendi kontrolünde bulunmayan veya ilişkili olmayan kaynak ve sistemlere uzak bağlantı ve erişim varsayılan olarak engellenmelidir. Aynı şekilde uygulama bileşenlerinin bulunduğu sunuculara uzaktan erişim izni kontrollü sağlanmalıdır.
3.2.4.3	1	İstemci Ön Bellekleme İşlevinin Kritik Veri için Kapatılması	Tüm formlarda istemci tarafında yapılan ön bellekleme işlevselliği kritik veri için kapatılmalıdır.
3.2.4.4	1	Uygulamanın Kullandığı Kaynakların Güvensiz Ortamlarda Saklanmaması	Uygulama kullandığı veya ürettiği kayıtları (resimler, ofis dosyaları, iz kayıtları vb.) güvensiz ortamlarda (ortak dizin, USB disk vb.) saklamamalıdır.
3.2.4.5	1	Güvenilmeyen Kaynaklardan Alınan Dosyaların Denetlenmesi	Güvenilmeyen kaynaklardan alınan dosyaların öncelikle türü ve içeriği doğrulanmalı, güvenlik açığına sebep olabilecek bir içeriğe sahip olup olmadığı kontrol edilmelidir. Bu dosyalar kısıtlı izinlerle uygulama ana dizini dışında depolanmalıdır. Bu dosyaların çalıştırılmasına ve çalıştırılan koda dâhil edilmesine (parametre, eklenti vb. olarak) izin verilmemelidir.
3.2.4.6	1	Kaynaklara Erişimin Kısıtlanması	Kökler arası kaynak paylaşımında (CORS) güvenilmeyen kaynakların uygulamanın verilerine erişmesi engellenmelidir. URL yeniden yönlendirmelerinin sadece bilinen beyaz liste adreslerine yapılması, bilinmeyen adreslere yönlendirme gerekiyorsa kullanıcının uyarılarak onayının alınması sağlanmalıdır.
3.2.4.7	2	Açık Kaynak Kod Tabanının Kurum Bünyesinde Tutulması	Açık kaynak kod tabanın zafiyete neden olacak şekilde değiştirilmesini engellemek için kod tabanı kurum bünyesinde barındırılmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.4.1	Yapılandırma Dosyaları, Denetim Kayıtları, İz Kayıtları vb. Bilgilerin Kullanıcı Verisiyle Aynı Konumda Depolanmaması	Mülakat, Güvenlik Denetimi	Uygulamanın yapılandırmasını ve ayarlarını içeren bilgiler nerede saklanmaktadır? Uygulamanın ürettiği denetim kayıtları ve iz kayıtları nerede saklanmaktadır? Uygulamanın sahip olduğu yapılandırma dosyaları, denetim kayıtları ve iz kayıtları gibi bilgiler kullanıcı verileri ile ayrı yerde mi saklanıyor? Uygulamanın yönettiği veri nerede saklanmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.4.2	Uygulama Bileşenlerine Dış Kaynaklardan Erişimin Kısıtlanması	Gözden Geçirme, Sızma Testi	Uygulamanın çalıştığı sunuculardan veri tabanına/dış kaynaklara uzaktan bağlantı ve erişim sağlanabilmekte midir? Uygulamanın çalıştığı sunuculardan uygulama ile ilişkili olmayan kaynak ve sistemlere uzaktan bağlantı ve erişim engelleniyor mu? Uygulama sunucularına her yerden uzak masaüstü ile erişilebilmekte midir?
3.2.4.3	İstemci Ön Bellekleme İşlevinin Kritik Veri için Kapatılması	Mülakat, Gözden Geçirme, Sızma Testi	İstemci tarafında önbellekte kritik bilgiler tutuluyor mu?
3.2.4.4	Uygulamanın Kullandığı Kaynakların Güvensiz Ortamlarda Saklanmaması	Mülakat, Gözden Geçirme, Sızma Testi	Uygulamanın kullandığı kayıtların hangi ortamlarda saklanabileceği tasarım dokümanında tanımlanmış mı?
3.2.4.5	Güvenilmeyen Kaynaklardan Alınan Dosyaların Denetlenmesi	Mülakat, Gözden Geçirme, Sızma Testi	Kullanıcıdan ve güvenilmeyen kaynaklardan alınan dosyalar nerede depolanmaktadır? Bu dosyalar depolanmadan önce dosya türü nasıl doğrulanmaktadır ve zararlı içeriğe sahip olup olmadığı nasıl kontrol edilmektedir? Çalıştırılacak komutlara girdi olarak verilen dosyalar ile çalıştırılan komutların ürettiği dosyaların içeriği saldırılara maruz kalmamak için kullanılmadan önce denetleniyor mu? Denetim yapılan ortamın güvenliği nasıl sağlanıyor?
3.2.4.6	Kaynaklara Erişimin Kısıtlanması	Gözden Geçirme, Sızma Testi	URL yeniden yönlendirme işleminden önce hangi kontroller yapılıyor? Yönlendirilebilir güvenilir URL adresleri listesi tutuluyor mu? Listede olmayan adreslerle karşılaştığında uygulama nasıl karşılık vermektedir? Uygulamada kökler arası kaynak paylaşımında (CORS) güvenlik önlemleri tanımlanmış mıdır?
3.2.4.7	Açık Kaynak Kod Tabanının Kurum Bünyesinde Tutulması	Mülakat, Gözden Geçirme	Açık kaynaklı kod kullanarak yazılım geliştirilirken kod tabanı geliştirme yapan kurum bünyesinde tutuluyor mu?

3.2.5. Güvenli Kurulum ve Yapılandırma

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.5.1	1	Uygulamada Güvenlik Güncellemeleri ve Yamaları Yüklenmiş Bileşenlerin Kullanılması	Uygulama, güvenlik güncellemeleri ve yamaları yapılmış bileşenlerden oluşmalıdır. Bk. Tedbir No: 5.3.1.1
3.2.5.2	1	Kaynak Paylaşım ve İçerik Güvenliği Sıkılaştırmaları	Uygulamanın güvenliğini artırmak ve istemci tarafında yer alan kaynakların güvenliğini sağlamak amacıyla güvenli HTTP başlıkları (X-Frame-Options, Content-Security-Policy vb.) kullanılmalıdır. Uygulamanın diğer sistemler, uygulamalar veya kişiler ile paylaştığı dosya, veri veya kaynaklar için erişim kontrolleri yapılmalıdır. Bk. Tedbir No: 5.3.1.17
3.2.5.3	1	Kurulumların Korumalı ve Ayrıştırılmış Şekilde Yapılması	Uygulama kurulumları, korumalı ve ayrıştırılmış şekilde yapılmalıdır. Bu kapsamda yöneticiler için hazırlanmış kullanıcı kılavuzları ürünlerin güvenli kurulumları ve yapılandırılmaları ile ilgili talimatlar içermelidir. Uygulama çok katmanlı mimari (multitier architecture) kullanılarak tasarlanmalı ve her katman için güvenlik mekanizmaları oluşturulmalıdır. Uygulamanın kullandığı veri tabanları ve kayıtlar, internetten doğrudan erişilemeyecek şekilde yapılandırılmalıdır. İnternete açık olarak çalışan sunucular (uygulama sunucusu, web sunucu, e-posta sunucuları vb.) DMZ (DeMilitarized Zone) gibi ayrı bir bölgede tutulmalıdır.
3.2.5.4	1	Sunuculara ve Çalışma Ortamlarına Sadece Uygulamanın ve Yetkili Kullanıcıların Erişebilmesi	Sunuculara ve çalışma ortamlarına (veri tabanı, dosya sistemi, servisler vb.) sadece uygulamanın ve yetkili kullanıcıların erişebileceği şekilde gerekli güvenlik yapılandırmaları uygulanmalıdır.
3.2.5.5	1	Sunucular Arası İletişimde İhtiyaç Duyulan En Az Yetkiye Sahip Hesapların Kullanılması	Uygulama sunucuları ve veri tabanı sunucuları gibi bileşenlerin arasındaki iletişimde ihtiyaç duyulan en az yetkiye sahip hesaplar kullanılmalıdır. Bk. Tedbir No: 3.2.3.3
3.2.5.6	1	İşletimdeki Sistemler Üzerinde Uygulama Kurulumu	İşletimdeki sistemler üzerine derleyiciler ve diğer geliştirme araçları kurulmamalıdır.
3.2.5.7	2	Güvenli Derleme	Sistem seviyesinde erişimi olan diller ile geliştirilmiş uygulamalar, güvenlik bayrakları (ASLR, DEP, hata ayıklama kapalı vb.) etkin olacak şekilde derlenmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.5.8	2	Yapılandırma Değişikliklerinin İzlenmesi	Uygulama, yapılandırma değişiklikleri ile ilgili erişimleri kısıtlamalı ve yapılandırma değişiklikleri için iz kayıtları oluşturmalıdır. Çalışan uygulamanın kodlarının değiştirilmemesini sağlayacak önlemler (kaynak kodun özetinin saklanması, kaynak kodun konfigürasyon yönetim aracında bulunan sürüm numarasının (build number) saklanması vb.) alınmalıdır. Bk. Tedbir No: 3.1.8.1
3.2.5.9	2	Sistem Kaynaklarının Azalması Durumunda Uyarı Verilmesi	Sistem kaynakların azalması durumunda yöneticiye uyarı verilebilecek altyapı oluşturulmalıdır. Bu kapsamda ilgili altyapı, uyarı üretebilmeli veya üretilmiş uyarıları yöneticiye iletebilmelidir.
3.2.5.10	2	Anahtarlar ve Parolaların Değiştirilebilir Olması	Tüm anahtar ve parolalar değiştirilebilir olmalıdır ve kurulum esnasında oluşturulmalı veya değiştirilmelidir.
3.2.5.11	3	Sunucular Arası İletişimin Şifreli Olması	Uygulama sunucuları ile bağlantı kurduğu sunucular arasındaki iletişim şifreli olmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.5.1	Uygulamada Güvenlik Güncellemeleri ve Yamaları Yüklenmiş Bileşenlerin Kullanılması	Mülakat, Gözden Geçirme	Belirli aralıklarla mevcut uygulama bileşenlerinin güncelliği kontrol ediliyor mu? Mevcut uygulama bileşenlerinin eski versiyona sahip olduğu tespit edildiğinde ne gibi faaliyetler gerçekleştirilmektedir? Bu faaliyetler dokümanlarda tanımlanmış mıdır?
3.2.5.2	Kaynak Paylaşım ve İçerik Güvenliği Sıkılaştırmaları	Mülakat, Güvenlik Denetim, Sızma Testi	http güvenlik başlıkları kullanılıyor mu? CORS yapılandırması güvenli mi?
3.2.5.3	Kurulumların Korumalı ve Ayrıştırılmış Şekilde Yapılması	Mülakat, Gözden Geçirme	Kurulumun yapıldığı sunucu ve ağların ayrıştırılmış ve korunaklı olabilmesi için nasıl bir yöntem izlenmektedir? Bu yöntem için adımlar tanımlanmış ve dokümante edilmiş midir? Yöneticiler için hazırlanmış kullanıcı kılavuzları ürünlerin güvenli kurulumları ve yapılandırılmaları ile ilgili talimatlar içeriyor mu? İnternete açık olarak çalışan sunucuların çeşitli saldırılar sonucunda ele geçirilmesi durumunda kurum yerel ağının ve ilgili ağda bulunan diğer sunucuların güvenliğinin sağlanması için ne gibi önlemler alınıyor? Kurulum yapmaya yetkili kullanıcılar kimlerdir? Sadece yetkili kullanıcılar mı uygulama kurulumlarını yapıyor?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.5.4	Sunuculara ve Çalışma Ortamlarına Sadece Uygulamanın ve Yetkili Kullanıcıların Erişebilmesi	Mülakat, Gözden Geçirme	Yalnızca uygulamanın ve yetkili kullanıcıların sunuculara ve çalışma ortamlarına erişebileceği şekilde gerekli güvenlik yapılandırmaları uygulanmış mıdır?
3.2.5.5	Sunucular Arası İletişimde İhtiyaç Duyulan En Az Yetkiye Sahip Hesapların Kullanılması	Mülakat, Gözden Geçirme, Sızma Testi	Uygulama ana bileşenleri (sunucular, servisler vb.) arası iletişimde kullanılacak hesapların yetkileri ihtiyaç duyacağı en az yetkiye göre yapılandırılmış mıdır?
3.2.5.6	İşletimdeki Sistemler Üzerinde Uygulama Kurulumu	Mülakat, Gözden Geçirme, Güvenlik Denetimi	İşletimdeki sistemler üzerinde derleyici veya geliştirme araçları bulunmakta mıdır?
3.2.5.7	Güvenli Derleme	Gözden Geçirme, Sızma Testi, Kaynak Kod Analizi	Derleme aşamasında kullanılan güvenlik bayrakları nelerdir?
3.2.5.8	Yapılandırma Değişikliklerinin İzlenmesi	Mülakat, Gözden Geçirme	Uygulamada yapılan yapılandırma değişiklikleri için iz kaydı (işletim sistemi, ağ veya uygulama seviyesinde) tutuluyor mu? Yapılandırma değişikliklerini yapabilecek kullanıcıların yetkilendirmesine yönelik bir süreç tanımlanmış ve uygulanmakta mıdır? Bu yetkilere sahip olan kullanıcıların listesi periyodik olarak gözden geçirilmekte midir?
3.2.5.9	Sistem Kaynaklarının Azalması Durumunda Uyarı Verilmesi	Mülakat, Gözden Geçirme	Uygulamanın kullandığı mevcut sistem kaynakları takip edilebiliyor mu? Uygulamanın kullandığı mevcut sistem kaynaklarının belirli bir sınır altına düşmesi durumunda yönetici/ilgili personel uygulama tarafından otomatik olarak bilgilendiriliyor mu?
3.2.5.10	Anahtarlar ve Parolaların Değiştirilebilir Olması	Mülakat, Gözden Geçirme	Uygulamada kullanılan tüm parola, şifre ve anahtarlar uygulamanın tekrar derlenmesi, kurulması vb. işlemlere ihtiyaç duyulmadan değiştirilebiliyor mu?
3.2.5.11	Sunucular Arası İletişimin Şifreli Olması	Mülakat, Gözden Geçirme, Sızma Testi	Uygulama sunucuları ve bağlantı kurduğu sunucular arasındaki iletişimin güvenliği nasıl sağlanmaktadır?

3.2.6. Güvenli Yazılım Geliştirme

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.6.1	1	Güvenlik Gereksinimleri ve Tasarımı	Yazılım geliştirme sürecinde güvenlik gereksinimleri tanımlanmalı ve bu gereksinimler göz önünde bulundurularak tasarım yapılmalıdır. Tedarik edilen veya hizmet alımı ile geliştirilen uygulamaların teknik şartnamelerinde güvenlik gereksinimlerine yer verilmelidir.
3.2.6.2	1	Test ve Geliştirme Ortamında Gerçek Veri Kullanılmaması	Geliştirme ve/veya test ortamında kullanılacak veriler gerçek veri olmamalıdır. Bu kapsamda, ilgili ortamlarda kullanılması için amaca uygun veriler üretilmelidir.
3.2.6.3	1	Tedarik Edilen Uygulamalarda Kullanım Amacına Uygun Olmayan Özellik/Arka Kapı Bulunmaması	Tedarik edilen veya hizmet alımı ile geliştirilen uygulamalar için yazılımın kullanım amacına uygun olmayan bir özellik ve arka kapı (kullanıcıların bilgisi/izni olmaksızın sistemlere erişim imkânı sağlayan güvenlik zafiyeti) içermediğine/içermeyeceğine dair üretici ve/veya tedarikçilerden imkânlar ölçüsünde taahhütname alınmalıdır. Bk. EK-C.6: Taahhütname Örneği
3.2.6.4	1	Arayüzün Türkçe Dil Desteğine Sahip Olması	Bk. Tedbir No: 4.6.1.4
3.2.6.5	1	Güncel İstemci ve Sunucu Teknolojilerinin Kullanılması	Üretici tarafından sunulan teknik desteği sona ermiş, güvenlik açığı barındıran veya teknolojisi zaman aşımına uğramış sunucu veya istemci teknolojileri kullanılmamalıdır.
3.2.6.6	1	Uygulama Güvenlik Testlerinin Yapılması	Devreye alınan veya güncellenen uygulamalarda sızma testleri ve uygulama güvenliği testleri yapılmalıdır. Tedarik edilen uygulamalar üzerinde sızma testleri gerçekleştirilmelidir. Bk. Tedbir Başlık No: 3.1.11
3.2.6.7	2	Kaynak Kod Güvenlik Analizlerinin Yapılması	Kurumun kaynak koduna sahip olduğu tüm uygulamalar devreye alım öncesinde kaynak kod analizinden geçirilmelidir.
3.2.6.8	2	Güvenli Yazılım Geliştirme Süreçlerinin Uygulanması	Güvenli yazılım geliştirme süreçleri ve olgunluk modellerinden faydalanılarak kurumsal yazılım geliştirme süreçleri güncellenmeli ve güvenli yazılım geliştirme yaşam döngüsü uygulanmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.6.1	Güvenlik Gereksinimleri ve Tasarımı	Mülakat, Gözden Geçirme	Tasarım, tanımlanmış yazılım güvenlik gereksinimlerine göre yapılmış mı? Yazılım güvenlik gereksinimleri, tedarik edilen veya hizmet alımı ile geliştirilen uygulamaların teknik şartnamelerinde yer alıyor mu?
3.2.6.2	Test ve Geliştirme Ortamında Gerçek Veri Kullanılmaması	Mülakat	Geliştirme ve/veya test ortamlarında kullanılan veriler hangi yöntem ile / nasıl oluşturuldu? Yazılım için geliştirme ve test süreçlerinde hangi veriler kullanılıyor?
3.2.6.3	Tedarik Edilen Uygulamalarda Kullanım Amacına Uygun Olmayan Özellik/Arka Kapı Bulunmaması	Mülakat, Gözden Geçirme	Tedarik edilen veya hizmet alımı ile geliştirilen uygulamaların; yazılımın kullanım amacına uygun olmayan bir özellik ve arka kapı içermediğine/içermeyeceğine dair üretici ve/veya tedarikçilerden imkânlar ölçüsünde taahhütname alınıyor mu?
3.2.6.4	Arayüzün Türkçe Dil Desteğine Sahip Olması	Mülakat	Bk. Denetim No: 4.6.1.4
3.2.6.5	Güncel İstemci ve Sunucu Teknolojilerinin Kullanılması	Mülakat, Gözden Geçirme	Belirli aralıklarla kullanılan istemci ve sunucu teknolojilerinin mevcut sürümlerinin bilinen zafiyet içerip içermediği kontrol ediliyor mu? Mevcut istemci ve sunucu teknolojilerinin eski versiyona sahip olduğu ya da kullanılan teknolojilerin bilinen zafiyet içerdiği tespit edildiğinde ne gibi önlemler alınmaktadır?
3.2.6.6	Uygulama Güvenlik Testlerinin Yapılması	Mülakat, Gözden Geçirme	Devreye alınan, güncellenen veya kaynak kodları ile tedarik edilen uygulamalar için sızma testleri gerçekleştiriliyor mu? İlgili testler neticesinde elde edilmiş sonuçlara göre düzeltici/önleyici tedbirler alınıyor mu?
3.2.6.7	Kaynak Kod Güvenlik Analizlerinin Yapılması	Mülakat, Gözden Geçirme	Kurumun kaynak koduna sahip olduğu tüm uygulamalar devreye alım öncesinde kaynak kod analizinden geçirilmekte midir?
3.2.6.8	Güvenli Yazılım Geliştirme Süreçlerinin Uygulanması	Mülakat, Gözden Geçirme	Güvenli yazılım geliştirme süreçleri ve/veya olgunluk modelleri uygulanıyor mu? Kurumsal yazılım geliştirme süreçleri güvenli yazılım geliştirme yaşam döngüsü süreçleri ve modellerinden faydalanılarak güncelleniyor mu?

3.2.7. Veri Tabanı ve Kayıt Yönetimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.7.1	1	Ortak Hesap Kullanılmaması ve En Az Yetki Prensibinin Uygulanması	Her veri tabanı kullanıcısı (kullanıcı, yönetici, uygulama vb.) için ayrı hesaplar tanımlanarak ortak hesap kullanılmamalıdır. En az ayrıcalık ilkesi kapsamında, kullanıcılara veri tabanı üzerinde gerçekleştirebilecekleri işlemler için gereken minimum yetkilerin haricinde bir ayrıcalık tanımlanmamalıdır. Bk. Tedbir No: 5.2.1.7
3.2.7.2	1	Bulut Depolama Hizmetlerinde Kurumsal Verilerin Bulundurulmaması	Kurumların kendi özel sistemleri veya yurt içinde yerleşik kurum kontrolündeki hizmet sağlayıcılar hariç olmak üzere kurumsal kritik verilerin saklanması/depolanması amacıyla bulut depolama hizmetleri kullanılmamalıdır. Bk. Tedbir No: 4.3.1.1
3.2.7.3	1	Veri Tabanlarına ve Verinin Saklandığı Ortamlara Yalnızca Yetkili Kullanıcıların Erişebilmesi	Veri tabanlarına ve verinin saklandığı ortamlara erişimin sadece yetkili kullanıcılar tarafından gerçekleştirilebilmesi için ilgili kaynaklar (güvenlik duvarı, işletim sistemi vb.) üzerinde yetkilendirme ve ayarlar yapılmalıdır.
3.2.7.4	1	Veri Tabanının Dışarıya Aktarımının Yetkili Kullanıcı Tarafından Yapılması	Veri tabanının dışarıya aktarımı (dosya olarak kaydetme, yerel veya uzak uygulamalara transfer etme vb.) sadece yetkili olan hesaplarla yapılmalıdır.
3.2.7.5	1	Veri Tabanlarında Varsayılan Kullanıcı ve Parolaların Kullanılmaması	Bk. Tedbir No: 5.2.1.3
3.2.7.6	1	Veri Tabanı Kullanıcıları için Parola Politikalarının Oluşturulması	Bk. Tedbir No: 5.2.1.4
3.2.7.7	1	Test ve Geliştirme Ortamında Kullanılan Veri Tabanı Üzerinde Gerçek Veri Bulundurulmaması	Gerçek veri, test verisi olarak kullanılmamalıdır. Bu kapsamda geliştirme ve/veya test ortamlarında bulunan veri tabanı, gerçek veri barındırmamalıdır. Bunun yerine ilgili işlemler için özel üretilmiş veriler kullanılmalıdır. Bk. Tedbir No: 3.2.6.2
3.2.7.8	1	Kullanıcıların Denetim Kayıtları Üzerinde Değişiklik Yapmasının Engellenmesi	Kullanıcıların denetim kayıtları üzerinde değişiklik yapması engellenmelidir. Bunun için kullanıcıların ilgili kaynaklar (tablo, dosya vb.) üzerindeki yetkilerinin sınırlandırılması, kayıtların güvenli olarak farklı bir lokasyona kopyalanması vb. yöntemler kullanılabilir.
3.2.7.9	1	Veri Tabanı Versiyonunun Güncel ve Güvenlik Yamalarının Yüklü Olması	Bk. Tedbir No: 5.2.1.1
3.2.7.10	1	Veri Tabanı Üzerinde Özel Nitelikli Kişisel Verinin Açık Metin Olarak Tutulmaması	Veri tabanı üzerinde yer alan özel nitelikli kişisel veriler açık metin olarak tutulmamalıdır. İlgili bilgiler, ulusal ve/veya uluslararası standartlar tarafından kabul görmüş kriptografik yöntemlerden faydalanılarak saklanmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.7.11	1	Veri Tabanına Yapılan Uzak Bağlantıların Güvenliğinin Sağlanması	Bk. Tedbir No: 5.2.1.5
3.2.7.12	1	Ayrıcalıkların Roller ve/veya Profiller Üzerinden Verilmesi	Tüm ayrıcalıklar veri tabanının sunduğu imkânlar dâhilinde en az yetki prensibine uyularak kullanıcılar yerine rollere ve/veya profillere tanımlanmalıdır. Kullanıcılar için mümkün olduğunca varsayılan roller ve profiller tercih edilmemeli, en uygun rol ve/veya profil ilgili kullanıcıya atanmalıdır. Bk. Tedbir No: 5.2.1.8
3.2.7.13	1	Veri Kurtarma Prosedürünün Hazırlanması	Verilerin yanlışlıkla silinmesine karşı verinin geri döndürülebilmesi için veri tabanı yönetim sisteminin sağladığı yedekleme ve kurtarma mekanizmaları önceden kurulmalıdır. Düzenli veri tabanı yedeği alınmalıdır.
3.2.7.14	1	Yedeklerin Güvenliğinin Sağlanması	Bk. Tedbir No: 5.2.1.11
3.2.7.15	1	Varsayılan Yapılandırmaların Kullanılmaması	Veri tabanlarında varsayılan güvensiz yapılandırmalar (iletişim protokolü, ihtiyaç duyulmayan veri tabanı özellikleri, varsayılan olarak güvensiz yapılandırılmış parametreler vb.) kullanılmamalıdır. Bk. Tedbir No: 5.2.1.2
3.2.7.16	2	Yetkili Kullanıcı İşlemlerinin Kaydedilmesi	Veri tabanı üzerinde yetkili kullanıcılar tarafından gerçekleştirilen işlemler için denetim kayıtları oluşturulmalıdır. Bu kapsamda ilgili denetim politikaları/prosedürleri kurum ihtiyaçları doğrultusunda belirlenerek veri tabanı üzerinde uygulanmalıdır.
3.2.7.17	2	Kritik Tablolar ve Görüntüler Üzerindeki Yetkilerin Denetlenmesi	Kritik veri tabanı tabloları ve görüntüleri (view) üzerindeki yetkiler periyodik olarak gözden geçirilmeli ve denetlenmelidir.
3.2.7.18	3	Tüm Kullanıcı İşlemlerinin Kaydedilmesi	Veri tabanı üzerinde bulunan tüm kullanıcılar tarafından gerçekleştirilen işlemler için denetim kayıtları oluşturulmalıdır. Bu kapsamda ilgili denetim politikaları/prosedürleri kurum ihtiyaçları doğrultusunda belirlenerek veri tabanı üzerinde uygulanmalıdır.
3.2.7.19	3	Saklama Gereksinimi Sona Eren Kritik Verinin Güvenli Silinmesi	Saklama gereksinimi sona eren kritik veri geri getirilemeyecek şekilde silinmelidir.
3.2.7.20	3	İşlenmesi Asıl Amaç Olmayan Verilerin Veri Tabanı Sunucusundan Maskelenerek Sunulması	İşlenmesi asıl amaç olmadığı durumlarda maskelenmesine ihtiyaç duyulan veriler dokümante edilerek belirlenmelidir. Bu kapsamda dokümante edilmiş ilgili veriler, işlenmesi asıl amaç olmadığında kullanıcının yetkisi doğrultusunda veri tabanı sunucusundan maskelenerek sunulmalıdır.
3.2.7.21	3	Veri Tabanına Gönderilen Sorguların Kontrol Edilmesi	Veri tabanına gönderilen tüm sorgular içerik ve yazım açısından denetlenmeli, olası enjeksiyon saldırıları engellenmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.7.22	3	Kritik Veri İçeren Veri Tabanı Sunucularında Durağan Verinin Güvenliğinin Sağlanması	Bk. Tedbir No: 5.2.1.20

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.7.1	Ortak Hesap Kullanılmaması ve En Az Yetki Prensibinin Uygulanması	Mülakat, Sızma Testi	Her veri tabanı kullanıcısı için ayrı hesap tanımlanıyor mu? Kullanıcılar üzerinde, veri tabanında gerçekleştirebilecekleri işlemler için gereken minimum yetkilerin haricinde bir ayrıcalık mevcut mu?
3.2.7.2	Bulut Depolama Hizmetlerinde Kurumsal Verilerin Bulundurulmaması	Mülakat, Gözden Geçirme	Kurumların kendi özel sistemleri üzerinde veya yurt içinde yerleşik hizmet sağlayıcılar hariç olmak üzere bulut depolama hizmetlerinde veriler saklanmakta veya depolanmakta mıdır?
3.2.7.3	Veri Tabanlarına ve Verinin Saklandığı Ortamlara Yalnızca Yetkili Kullanıcıların Erişebilmesi	Mülakat, Güvenlik Denetimi	Veri tabanlarına ve verinin saklandığı ortamlara erişimde yetkilendirme mekanizması kullanılıyor mu?
3.2.7.4	Veri Tabanının Dışarıya Aktarımının Yetkili Kullanıcı Tarafından Yapılması	Mülakat, Güvenlik Denetimi	Hangi kullanıcılar veri tabanının dışarıya aktarımında kullanılabilir? Veri tabanının dışarıya aktarımında yetkilendirilmiş olan hesapların hangileri olduğu periyodik denetleniyor mu?
3.2.7.5	Veri Tabanlarında Varsayılan Kullanıcı ve Parolaların Kullanılmaması	Mülakat, Güvenlik Denetimi	Veri tabanında varsayılan hesaplar ve/veya varsayılan parolalar kullanılıyor mu?
3.2.7.6	Veri Tabanı Kullanıcıları için Parola Politikalarının Oluşturulması	Mülakat, Güvenlik Denetimi	Veri tabanı kullanıcıları için parola politikaları tanımlanmış mı?
3.2.7.7	Test ve Geliştirme Ortamında Kullanılan Veri Tabanı Üzerinde Gerçek Veri Bulundurulmaması	Mülakat, Güvenlik Denetimi	Geliştirme ve/veya test ortamlarında bulunan veri tabanı, gerçek veri barındırıyor mu? İlgili ortamlarda kullanılan/kullanılacak veriler nasıl oluşturulmaktadır?
3.2.7.8	Kullanıcıların Denetim Kayıtları Üzerinde Değişiklik Yapmasının Engellenmesi	Mülakat, Güvenlik Denetimi	Kullanıcıların denetim kayıtları üzerinde değişiklik yapabilmesinin önüne geçmek adına hangi önlemler alınmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.7.9	Veri Tabanı Versiyonunun Güncel ve Güvenlik Yamalarının Yüklü Olması	Mülakat, Sızma Testi	Veri tabanı için güncelleştirmeler ve güvenlik yamaları belirli periyotlar ile kontrol edilerek uygulanıyor mu?
3.2.7.10	Veri Tabanı Üzerinde Özel Nitelikli Kişisel Verinin Açık Metin Olarak Tutulmaması	Mülakat, Gözden Geçirme	Veri tabanı üzerinde yer alan özel nitelikli kişisel veriler kriptografik yöntemler kullanılarak saklanmakta mıdır?
3.2.7.11	Veri Tabanına Yapılan Uzak Bağlantıların Güvenliğinin Sağlanması	Mülakat, Güvenlik Denetimi	Veri tabanı sunucularına yapılan uzak bağlantıların güvenliği nasıl sağlanıyor?
3.2.7.12	Ayrıcalıkların Roller ve/veya Profiller Üzerinden Verilmesi	Mülakat, Güvenlik Denetimi	Kullanıcılara ayrıcalıklar doğrudan atanıyor mu? Varsayılan roller ve profiller kullanılıyor mu?
3.2.7.13	Veri Kurtarma Prosedürünün Hazırlanması	Mülakat, Gözden Geçirme	Olası veri kayıplarına karşı nasıl bir önlem alınmıştır? Düzenli olarak yedek alınmakta mıdır? Yedekler nerede ve nasıl muhafaza edilmektedir?
3.2.7.14	Yedeklerin Güvenliğinin Sağlanması	Mülakat, Gözden Geçirme, Sızma Testi	Yedek dosyalarına yetkisiz erişimleri engellemek adına hangi önlemler alınmaktadır?
3.2.7.15	Varsayılan Yapılandırmaların Kullanılmaması	Mülakat, Güvenlik Denetimi	Veri tabanında, varsayılan güvensiz yapılandırmalar (iletişim protokolü, ihtiyaç duyulmayan veri tabanı özellikleri, varsayılan olarak güvensiz yapılandırılmış parametreler vb.) bilinen güvenli değerler/yöntemler ile değiştirilerek oluşabilecek zafiyetlere karşı önlemler alınıyor mu?
3.2.7.16	Yetkili Kullanıcı İşlemlerinin Kaydedilmesi	Mülakat, Güvenlik Denetimi	Veri tabanı denetleme mekanizması aktif mi? Veri tabanı denetim kayıtları, hangi denetim politikaları/prosedürleri göz önünde bulundurularak oluşturulmaktadır? Veri tabanında yetkili kullanıcıların yaptığı işlemler kayıt altına alınıyor mu?
3.2.7.17	Kritik Tablolar ve Görüntüler Üzerindeki Yetkilerin Denetlenmesi	Mülakat, Güvenlik Denetimi	Periyodik olarak kritik veri tabanı tabloları ve görüntüleri (view) üzerinde yetkilere sahip olan kullanıcılar/roller analiz ediliyor mu?
3.2.7.18	Tüm Kullanıcı İşlemlerinin Kaydedilmesi	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Veri tabanı denetleme mekanizması aktif mi? Veri tabanı denetim kayıtları, hangi denetim politikaları/prosedürleri göz önünde bulundurularak oluşturulmaktadır? Veri tabanında tüm kullanıcıların yaptığı işlemler kayıt altına alınıyor mu?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.7.19	Saklama Gereksinimi Sona Eren Kritik Verinin Güvenli Silinmesi	Mülakat, Gözden Geçirme	Kritik verinin kullanımları tamamlandığında üzerlerinde ne gibi işlemlerin uygulanacağı tanımlanmış mıdır? Tanımlanmış faaliyetler nasıl uygulanmaktadır?
3.2.7.20	İşlenmesi Asıl Amaç Olmayan Verilerin Veri Tabanı Sunucusundan Maskelenerek Sunulması	Mülakat, Sızma Testi	Hangi verilerin maskelenerek kullanılacağı dokümante edilmiş midir? Veri tabanı üzerinde bulunan ilgili veriler, işlenmesi asıl amaç olmadığında kullanıcı yetkisi doğrultusunda maskelenerek sunulmakta mıdır?
3.2.7.21	Veri Tabanına Gönderilen Sorguların Kontrol Edilmesi	Mülakat, Güvenlik Denetimi, Sızma Testi	Veri tabanına gönderilen tüm sorgular için uygulamadan bağımsız olarak içerik ve yazım denetimi yapılmakta mıdır?
3.2.7.22	Kritik Veri İçeren Veri Tabanı Sunucularında Durağan Verinin Güvenliğinin Sağlanması	Mülakat, Güvenlik Denetimi	Kritik veri içeren veri tabanı sunucularında bulunan durağan verinin güvenliğinin sağlanmasında hangi yöntemler kullanılmaktadır?

3.2.8. Hata Ele Alma ve Kayıt Yönetimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.8.1	1	Hataların Yakalanması ve Varsayılan Olarak Güvenli Duruma Geçmesi	Uygulamalar, tüm oluşabilecek hataları yakalayabilecek ve hata durumlarında varsayılan olarak güvenli durumlara geçecek şekilde tasarlanmış olmalıdır. Örneğin, yetkilendirme esnasında hata oluşması durumunda uygulama ilgili işlemi durdurmalı ve kullanıcı yetkilendirilmemelidir. Kimlik doğrulama işlemi sırasında hata ile karşılaşıldığında ise kullanıcının uygulamaya girişi engellenmelidir. Hata durumu ile ilgili detaylar kullanıcıya gösterilmemelidir.
3.2.8.2	1	Hataların ve Tanımlanan Olayların İz Kayıtlarının Oluşturulabilmesi	Uygulama, tanımlanan güvenlik olaylarının/işlemlerinin (yetki değişiklikleri, kullanıcı değişiklikleri, kimlik doğrulama işlemleri) başarılı ve başarısızlık durumları için iz kayıtları oluşturabilmelidir. İz kaydı minimum şu bilgileri içermelidir: • İşlemi yapan kullanıcı (gerçek kişi veya yazılımsal süreç için tanımlanmış kullanıcı) bilgisi • İşlem zamanı • Kaynak ve hedef sistem tanımlayıcı bilgileri (ip, sunucu adı vb.) • İşlem özeti (başarılı işlem, başarısız işlem vb.) Bk. Tedbir No: 3.1.8.1

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.8.3	1	Özel Nitelikli Kişisel Veri İçeren Hata Mesajının veya İz Kaydının Üretilmemesi	Uygulama, özel nitelikli kişisel veri içeren hata mesajı veya iz kaydı üretmemelidir.
3.2.8.4	1	İz Kayıtlarında Olayların Zaman Bilgisinin Yer Alması	İz kayıtlarında olayların zaman sıralamasına ilişkin araştırma yapılabilecek şekilde zaman bilgisi yer almalıdır. Bk. Tedbir No: 3.1.8.3
3.2.8.5	1	İz Kayıtlarının Güvenliğinin Sağlanması	Uygulama, uygulama sunucusu ele geçirildiğinde iz kayıtlarının güvenliğini sağlamak amacıyla değiştirilmesine veya silinmesine izin vermemelidir. Bk. Tedbir No: 3.1.8.1
3.2.8.6	1	İz Kayıtlarının Saldırı Vektörü Olarak Kullanımının Engellenmesi	Kayıtların doğruluğunu sağlamak ve bütünlüğünün bozulmasını (log forging) engellemek için iz kayıtları oluşturulurken kullanılan girdiler üzerinde girdi denetimi yapılmalıdır. Kayıtlar görüntülenirken oluşabilecek zafiyetlere (XSS vb.) karşı ise karakter kodlama ve filtreleme gibi tedbirler uygulanmalıdır. Bk. Tedbir No: 3.2.10.12

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.8.1	Hataların Yakalanması ve Varsayılan Olarak Güvenli Duruma Geçmesi	Mülakat, Sızma Testi	Uygulamalarda hata ile karşılaşılması durumunda takip edilecek adımlar/faaliyetler tanımlanmış mıdır?
3.2.8.2	Hataların ve Tanımlanan Olayların İz Kayıtlarının Oluşturulabilmesi	Mülakat, Gözden Geçirme	Uygulama için önceden tanımlanan güvenlik olayları için hem başarılı hem de başarısız işlemler kayıt altına alınabilmekte midir? Oluşturulan iz kayıtlarında hangi bilgiler yer almaktadır?
3.2.8.3	Özel Nitelikli Kişisel Veri İçeren Hata Mesajının veya İz Kaydının Üretilmemesi	Mülakat, Gözden Geçirme	Hata mesajlarının ve iz kayıtlarının hangi bilgileri içereceği dokümante ediliyor mu? Hata mesajlarının ve iz kayıtlarının içereceği bilgiler arasında önceden tanımlanmış olan özel nitelikli kişisel veri bulunmakta mıdır?
3.2.8.4	İz Kayıtlarında Olayların Zaman Bilgisinin Yer Alması	Mülakat, Gözden Geçirme	Oluşturulan iz kayıtlarında doğru zaman bilgisi mevcut mudur? Oluşturulan iz kayıtlarında kullanılan zaman bilgisi formatı/biçimi tanımlanmış mıdır?
3.2.8.5	İz Kayıtlarının Güvenliğinin Sağlanması	Mülakat, Gözden Geçirme	İz kayıtlarının güvenliğinin sağlanması için uygulanabilir adımlar/süreçler tasarım dokümanında tanımlanmış mı? İz kayıtları için mevcut bir yetkilendirme mekanizması kullanılıyor mu?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.8.6	İz Kayıtlarının Saldırı Vektörü Olarak Kullanımının Engellenmesi	Mülakat, Gözden Geçirme, Sızma Testi	İz kayıtlarının veri yapısı ve veri sınırlaması tanımlanmış mıdır? İz kayıtlarında saldırı için kullanılabilecek kullanıcı girdisi üzerinde girdi denetimi yapılmakta mıdır?

3.2.9. İletişim Güvenliği

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.9.1	1	SSL/TLS Protokolünün Güvenli Kullanılması	Kimlik doğrulaması yapılmış, kritik veri ya da işlevler içeren tüm bağlantılar SSL/TLS protokolünün bilinen zafiyet içermeyen güvenilir sürümü ile yapılmalıdır. Sertifikalarda ve sertifikanın tüm hiyerarşisinde ulusal ve/veya uluslararası otoriteler tarafından güvenli olarak kabul görmüş güçlü algoritmalar ve protokoller kullanılmalıdır.
3.2.9.2	1	Sertifika Denetimlerinin Yapılması	Güvenilen bir sertifika otoritesinden her Transport Layer Security (TLS) sunucu sertifikasına bir güven zinciri oluşturulabilmeli ve internet üzerinden erişilebilen her sunucu sertifikası geçerli olmalıdır. Uygulama, Çevrimiçi Sertifika Durum Protokolü Damgalama (OCSP stapling) gibi yöntemlerle sertifika iptal denetimi gerçekleştirebilecek şekilde yapılandırılmalıdır.
3.2.9.3	2	HSTS Kullanılması	Web sayfalarına gerçekleştirilecek bağlantıların ve kullanılacak kaynakların güvenliği için HSTS kullanılmalıdır.
3.2.9.4	3	Hatalı Sertifikaların Tespiti	Uygulama adına oluşturulabilecek hatalı sertifikalar için sertifika şeffaflığı logları (Certificate Transparency Logs) üzerinde düzenli olarak kontroller yapılmalıdır.
3.2.9.5	3	SSL/TLS Hata İz Kayıtları	SSL/TLS bağlantı hatası durumları için iz kaydı oluşturulmalıdır.
3.2.9.6	3	Kritik Verinin Şifrelenmesi	Ulusal düzeyde kritik veri işleyen uygulamalar tarafından oluşturulan trafikten kripto analiz yöntemleri ile bilginin ifşası için yapılabilecek saldırılar engellenmelidir. Bu veri şifreli trafik üzerinden ayrıca şifrelenerek taşınmalıdır.
3.2.9.7	3	Kurum Tarafından Onaylanmış Sertifikaların Kullanılması	Yazılımlarda kullanılmak üzere üretilmiş sertifikaların kaynağı kontrol edilmelidir. Yazılımlarda sadece kurum tarafından belirlenen kaynak/otorite tarafından üretilmiş sertifikaların kullanılması sağlanmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.9.1	SSL/TLS Protokolünün Güvenli Kullanılması	Mülakat, Gözden Geçirme, Sızma Testi	Şifreli iletişim için hangi protokol versiyonu kullanılıyor? Sertifikalarda kullanılabilecek algoritmalar ve protokoller tanımlanmış mı? Sertifikalarda kullanılan algoritmalar ve protokoller ulusal ve/veya uluslararası otoriteler tarafından güvenli/uygulanabilir olarak kabul ediliyor mu?
3.2.9.2	Sertifika Denetimlerinin Yapılması	Mülakat, Gözden Geçirme	Mevcut sunucuların sertifikalarının geçerliliği belirli zamanlarda kontrol ediliyor mu? Otomatik olarak sertifika iptal denetimi gerçekleştirilebiliyor mu?
3.2.9.3	HSTS Kullanılması	Mülakat, Güvenlik Denetimi, Sızma Testi	Gerçekleştirilecek bağlantıların ve kullanılacak kaynakların güvenliği için HSTS kullanılıyor mu?
3.2.9.4	Hatalı Sertifikaların Tespiti	Mülakat, Gözden Geçirme	Uygulama adına oluşturulabilecek hatalı sertifikalar için sertifika şeffaflığı logları (Certificate Transparency Logs) üzerinde düzenli olarak kontroller yapılıyor mu?
3.2.9.5	SSL/TLS Hata İz Kayıtları	Mülakat, Gözden Geçirme	SSL/TLS bağlantı hatası durumlarında iz kaydı oluşturuluyor mu?
3.2.9.6	Kritik Verinin Şifrelenmesi	Mülakat, Gözden Geçirme, Sızma Testi	Ulusal düzeyde kritik uygulama verisinin taşınmasında ne gibi güvenlik önlemleri alınıyor?
3.2.9.7	Kurum Tarafından Onaylanmış Sertifikaların Kullanılması	Mülakat, Gözden Geçirme	Kurum tarafından yetkilendirilmiş sertifika otoriteleri/üreticileri belirlenmiş ve dokümante edilmiş midir? Onaylı olmayan sertifikaların cihazlara ve yazılımı kurulumunu engellemek amacıyla hangi yöntemler kullanılmaktadır? Kurumda sertifika üretme/temin etme konusunda görevlendirilmiş personel bulunmakta mıdır?

3.2.10. Kötücül İşlemleri Engelleme

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.10.1	1	Sunucu Tarafında Girdi Doğrulama Denetiminin Yapılması	Uygulama sunucu tarafında, kabul edilen her bir veri tipi için girdi doğrulama denetimi yapmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.10.2	1	Girdi Doğrulama Hataları için İz Kaydının Oluşturulması	Sistemlerde (sunucu, uygulama vb.) yapılan girdi doğrulama işlemi sırasında oluşan hatalar için iz kayıtları oluşturulmalı ve ilgili istek reddedilmelidir. Bk. Tedbir No: 3.1.8.1
3.2.10.3	1	Uygulamanın Yetkisiz Olarak Program Çalıştırmasının Engellenmesi	Uygulamanın fonksiyonel gereksinimlerini karşılamak amacıyla ihtiyaç duyduğu programlar haricinde program/uygulama çalıştırması engellenmelidir.
3.2.10.4	1	Kritik Bilgilerin Formlarda Bulunan Gizli Alanlarda Saklanmaması	Form yapısını kullanan uygulamalar, kritik bilgileri formlarda bulunan gizli alanlarda saklamamalıdır.
3.2.10.5	1	CSRF Saldırılarına Karşı Önlem Alınması	Siteler arası istek sahteciliği (CSRF) zafiyetine karşı gerekli güvenlik önlemleri (CSRF token, SameSite bayrağı vb.) alınmalıdır.
3.2.10.6	1	Veri Tabanına Erişimde Kullanılan Dile Karşı Enjeksiyon Saldırılarının Önlenmesi	Bütün veri tabanı sorguları, parametrik olarak yapılmalı ve veri tabanına erişimde kullanılan dile karşı (SQL, NoSQL vb.) enjeksiyon saldırılarını engelleyebilecek güvenlik önlemleri alınmalıdır.
3.2.10.7	1	İşletim Sistemi Komut Enjeksiyonu Açıklarının Önlenmesi	İşletim sistemi komut enjeksiyonu açıklarına karşı güvenlik önlemleri alınmalıdır.
3.2.10.8	1	Bellek Taşması Saldırılarının Önlenmesi	Uygulama ve uygulamanın çalışma ortamında bellek taşması saldırılarına karşı önlem alınmalıdır.
3.2.10.9	1	Dosya İçerme Açıklarının Önlenmesi	Uygulama, dosya yolunu girdi olarak alıyor ise uzak ya da yerel dosya içerme açıklarını önleyici güvenlik denetimlerini yapmalıdır.
3.2.10.10	1	XML Tabanlı Saldırıların Önlenmesi	Uygulama, XML açıklarını (XPath sorgu saldırıları, XML harici öğe saldırıları, XML enjeksiyonu vb.) önleyici güvenlik denetimlerini yapmalıdır.
3.2.10.11	1	Yapısal Olmayan Veri için Karakterlerin Denetlenmesi	Yapısal olmayan veriler (belirli bir formata/biçime sahip olmayan) için izin verilen karakterler ve uzunluklar belirlenerek verinin içeriğinde olabilecek olası zararlı karakterlere karşı girdi kontrolü yapılmalıdır.
3.2.10.12	1	Girdi Denetimi Yapılması	HTML form alanlarının veri girdileri, REST çağrıları, HTTP üst başlıkları, çerezler, toplu işlem dosyaları gibi veri girdileri için doğrulama denetimi yapılmalıdır.
3.2.10.13	1	Yüklenen Dosyaların Denetlenmesi	Bk. Tedbir No: 3.2.4.5
3.2.10.14	2	İsteklerin Öngörülmeyen Büyüklükte Olup Olmadığının Kontrol Edilebilmesi	Uygulama sunucusuna gelen isteklerin öngörülmeyen bir sayıda ya da büyüklükte olup olmadığı kontrol edilebilmelidir. Bk. Tedbir No: 5.3.1.8

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.10.15	3	TS ISO/IEC 19790-24759 Onaylı Kriptografik Modüllerin ve Rastgele Sayı Üreteçlerinin Kullanılması	Uygulamada şifreleme, anahtar değişimi, dijital imzalama veya özet alma gibi fonksiyonlar bulunuyorsa TS ISO/IEC 19790-24759 onaylı kriptografik modüller ve rastgele sayı üreteçleri kullanılmalıdır.
3.2.10.16	3	Karakter Kodlamasının Tespiti	Girdi-çıktı denetimi yapılmadan önce veri üzerinde karakter kodlaması (character encoding) yapılıp yapılmadığı tespit edilmelidir. Tespit edilen kodlamaya göre denetimler gerçekleştirilmelidir.
3.2.10.17	3	Uygulama Seviyesi Servis Dışı Bırakma Saldırılarının Engellenmesi	Uygulamalara servis dışı bırakma saldırılarını önlemek için güvenlik mekanizmaları (tasarım seviyesinde önlem, uygulama seviyesi DoS çözümleri, web uygulama güvenlik duvarı kullanımı vb.) hayata geçirilmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.10.1	Sunucu Tarafında Girdi Doğrulama Denetiminin Yapılması	Mülakat, Gözden Geçirme, Sızma Testi	Uygulamada kullanılan mevcut bir girdi doğrulama mekanizması var mı? Girdi doğrulama mekanizması her veri tipi için kullanılıyor mu?
3.2.10.2	Girdi Doğrulama Hataları İçin İz Kaydının Oluşturulması	Mülakat, Gözden Geçirme, Sızma Testi	Uygulamanın hata ile karşılaşması durumunda takip edeceği adımlar/faaliyetler tasarım dokümanında tanımlanmış mı? Girdi doğrulama işlemi esnasında karşılaşılan hatalar kayıt altına alınıyor mu?
3.2.10.3	Uygulamanın Yetkisiz Olarak Program Çalıştırmasının Engellenmesi	Mülakat, Gözden Geçirme, Sızma Testi	Uygulamanın fonksiyonel gereksinimlerini karşılamak amacıyla ihtiyaç duyduğu programlar haricinde program/uygulama çalıştırmaması engelleniyor mu? Program/uygulama çalıştırmaması amacıyla uygulanan yöntem/mekanizmalar nelerdir?
3.2.10.4	Kritik Bilgilerin Formlarda Bulunan Gizli Alanlarda Saklanmaması	Mülakat, Gözden Geçirme, Sızma Testi	Kritik bilgiler formlarda bulunan gizli alanlarda saklanıyor mu?
3.2.10.5	CSRF Saldırılarına Karşı Önlem Alınması	Mülakat, Gözden Geçirme, Sızma Testi	CSRF kaynaklı zafiyetleri önlemek için nelerin yapılacağı tasarım dokümanında tanımlanmış mı? CSRF kaynaklı zafiyetlere karşı açığın bulunup bulunmadığını tespit etmek için analiz yapıldı mı? Analizler sonucunda CSRF zafiyetlerine karşı açığı bulunan uygulama için hangi önlemler alındı?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.10.6	Veri Tabanına Erişimde Kullanılan Dile Karşı Enjeksiyon Saldırılarının Önlenmesi	Mülakat, Sızma Testi, Kaynak Kod Analizi	Veri tabanı işlemleri için parametrik sorgular mı kullanılıyor? Veri tabanına erişimde kullanılan dile karşı enjeksiyon saldırılarını önlemek için nelerin yapılacağı tasarım dokümanında tanımlanmış mı? Veri tabanına erişimde kullanılan dile karşı enjeksiyon saldırılarına karşı zafiyetin bulunup bulunmadığını tespit etmek için analiz yapıldı mı? Analizler sonucunda veri tabanına erişimde kullanılan dile karşı enjeksiyon saldırılarına karşı zafiyetli bulunan uygulama için hangi önlemler alındı?
3.2.10.7	İşletim Sistemi Komut Enjeksiyonu Açıklarının Önlenmesi	Mülakat, Sızma Testi, Kaynak Kod Analizi	Komut enjeksiyonu saldırılarını önlemek için nelerin yapılacağı tasarım dokümanında tanımlanmış mı? Komut enjeksiyonu saldırılarına karşı zafiyetin bulunup bulunmadığını tespit etmek için analiz yapıldı mı? Analizler sonucunda komut enjeksiyonu saldırılarına karşı zafiyetli bulunan uygulama için hangi önlemler alındı?
3.2.10.8	Bellek Taşması Saldırılarının Önlenmesi	Mülakat, Sızma Testi, Kaynak Kod Analizi	Bellek taşması saldırılarını önlemek için nelerin yapılacağı tasarım dokümanında tanımlanmış mı? Bellek taşması saldırılarına karşı zafiyetin bulunup bulunmadığını tespit etmek için analiz yapıldı mı? Analizler sonucunda bellek taşması saldırılarına karşı zafiyetli bulunan uygulama için hangi önlemler alındı?
3.2.10.9	Dosya İçerme Açıklarının Önlenmesi	Mülakat, Sızma Testi, Kaynak Kod Analizi	Uzak ya da yerel dosya içerme saldırılarını önlemek için nelerin yapılacağı tasarım dokümanında tanımlanmış mı? Uzak ya da yerel dosya içerme saldırılarına karşı zafiyetin bulunup bulunmadığını tespit etmek için analiz yapıldı mı? Analizler sonucunda uzak ya da yerel dosya içerme saldırılarına karşı zafiyetli bulunan uygulama için hangi önlemler alındı?
3.2.10.10	XML Tabanlı Saldırıların Önlenmesi	Mülakat, Sızma Testi, Kaynak Kod Analizi	XML açıklarını önlemek için nelerin yapılacağı tasarım dokümanında tanımlanmış mı? XML açıklarına karşı zafiyetin bulunup bulunmadığını tespit etmek için analiz yapıldı mı? Analizler sonucunda XML açıklarına karşı zafiyetli bulunan uygulama için hangi önlemler alındı?
3.2.10.11	Yapısal Olmayan Veri için Karakterlerin Denetlenmesi	Mülakat, Sızma Testi, Kaynak Kod Analizi	Uygulamada kullanılan mevcut bir girdi doğrulama mekanizması var mı? Mevcut girdi doğrulama mekanizması yapısal olmayan veri için kullanılabiliyor mu? Yapısal olmayan verinin girdi doğrulamasında hangi faaliyetler/yöntemler uygulanıyor?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.10.12	Girdi Denetimi Yapılması	Mülakat, Sızma Testi, Kaynak Kod Analizi	Uygulamada kullanılan mevcut bir girdi doğrulama mekanizması var mı? HTML girdilerinin işleme alınmadan önce kontrol edilmesi için girdi doğrulama mekanizması kullanılıyor mu?
3.2.10.13	Yüklenen Dosyaların Denetlenmesi	Mülakat, Gözden Geçirme, Sızma Testi	Bk. Denetim No: 3.2.4.5
3.2.10.14	İsteklerin Öngörülmeyen Büyüklükte Olup Olmadığının Kontrol Edilebilmesi	Gözden Geçirme, Sızma Testi	Uygulamaya gelen isteklerin ve yüklenecek dosyaların üst sınır büyüklükleri belirlenmiş midir? Bu sınırlar uygulama tarafından kontrol edilmekte midir?
3.2.10.15	TS ISO/IEC 19790-24759 Onaylı Kriptografik Modüllerin ve Rastgele Sayı Üreteçlerinin Kullanılması	Mülakat, Güvenlik Denetimi, Sızma Testi	Kullanılan kriptografik modüller/rastgele sayı üreteçleri TS ISO/IEC 19790-24759 onaylı mıdır?
3.2.10.16	Karakter Kodlamasının Tespiti	Mülakat, Sızma Testi, Kaynak Kod Analizi	Girdi-çıktı denetimi yapılmadan önce gerçekleştirilecek faaliyetler tasarım dokümanında tanımlanmakta mıdır? Girdi-çıktı denetimi yapılmadan önce karakter kodlaması doğrulaması yapılmakta mıdır?
3.2.10.17	Uygulama Seviyesi Servis Dışı Bırakma Saldırılarının Engellenmesi	Mülakat, Güvenlik Denetimi, Sızma Testi	Uygulama seviyesinde oluşabilecek servis dışı bırakma saldırılarını önlemek için hangi güvenlik mekanizmaları kullanılmaktadır?

3.2.11. Dış Sistem Entegrasyonlarının Güvenliği

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.11.1	1	Web Servislerinin Güvenli Protokol Üzerinden Sunulması	Dışarıya açılan web servisleri; iyi yapılandırılmış, bilinen zafiyet içermeyen, güncel SSL/TLS versiyonlarını destekleyen bir protokol ile sunacak şekilde tasarlanmalıdır. Bk. Tedbir No: 3.2.9.1
3.2.11.2	1	Web Servisi Yapılandırmalarının Yetkili Kullanıcılar Tarafından Yapılması ve Yönetilmesi	Web Servisi yapılandırmaları (konumlandırma, açılacak servis portlarının tahsisi, ağ yapılandırması vb.) yetkili kullanıcılar tarafından yapılmalı ve yönetilmelidir. Varsayılan olarak yapılandırmalar güvenliği en üst düzeyde sağlayacak şekilde belirlenmelidir.
3.2.11.3	1	Web Servis Çağrılarında Kimlik Doğrulama ve Yetkilendirme Kontrolü	Her servis çağrısı için kimlik doğrulama ve yetkilendirme kontrolü yapılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.11.4	1	Sunulan Web Servislerin Girdi-Çıktı Denetimlerinin Yapılması	Sunulan web servisleri, girdi-çıktı denetimlerinin eksikliğinden kaynaklı saldırı çeşitlerine (XSS, uzak kod çalıştırma vb.) karşı önlem alacak şekilde geliştirilmeli ve konumlandırılmalıdır. Web servisi geliştirme aşamasında bilinen zafiyet içeren bileşenler (çatı, kütüphane, yazılım modülleri vb.) kullanılmamalıdır. Bk. Tedbir Başlık No: 3.2.10
3.2.11.5	1	Web Servis Yapılandırma ve Yönetim İşlemleri	Uygulama, web servis yapılandırma ve yönetim işlevlerine sadece yetkili kullanıcıların erişebilmesini sağlamalıdır.
3.2.11.6	2	Entegre Olunan Sistemin Web Servislerinin Beklenen Şekilde Çalıştığının Doğrulanması	Mevcut sistemde entegre olunan sistemden kaynaklanan hataların tolere edilebilmesi için gerekli önlemler (eşik değerinin aşılması, veri uyuşmazlığının olması vb. durumda uyarı mekanizmalarının aktif edilmesi) alınmalıdır.
3.2.11.7	2	Uygulamanın Kararlılığının Sağlanması	Uygulamanın entegre olunan sisteme ulaşamaması veya sistemin hata dönmesi durumlarında, uygulama kararlı ve güvenli şekilde işlemlerini devam ettirebilecek şekilde tasarlanmalıdır. Uygulama bu durumlarda hizmet sürekliliğini sağlayacak fonksiyonlara sahip olmalıdır.
3.2.11.8	2	Web Servisi Çağrı Sayısının ve Kaynak Kullanımının Sınırlandırılması	Kullanıcıların belirli bir süre içinde yapabilecekleri çağrı sayısı ve maksimum kaynak kullanımı her bir kullanıcı için belirlenebilmelidir. Sınır aşımında çağrılara cevap verilmemeli veya çağrılar engellenmelidir.
3.2.11.9	3	Dış Sistemler / Uygulamalar Arası Çağrıların Kayıt Altına Alınması	Dış sistemler ve uygulamalar arasındaki çağrıların girdi parametreleri ve sonuçları çağrıyı yapan ve sunan uygulamalar tarafından kayıt altına alınmalıdır.
3.2.11.10	3	Kritik Altyapı Sistemleri ile Güvenli İletişimin Sağlanması	Kritik altyapı sistemleri ile entegrasyonda özel hatlar (kiralık hat, özel güvenli ağ vb.) kullanılmalı ve yedekliliği için altyapı hazırlanmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.11.1	Web Servislerinin Güvenli Protokol Üzerinden Sunulması	Mülakat, Gözden Geçirme, Sızma Testi	Güvenli iletişim için kullanılan mevcut SSL/TLS protokolü ilgili zafiyet ve saldırılara karşı analiz edildi mi? Güvenli iletişim için kullanılan mevcut SSL/TLS protokolü yapılandırması ulusal ve/veya uluslararası otoriteler tarafından güvenli/uygulanabilir olarak kabul ediliyor mu?
3.2.11.2	Web Servisi Yapılandırmalarının Yetkili Kullanıcılar Tarafından Yapılması ve Yönetilmesi	Mülakat, Gözden Geçirme	Web servis yapılandırma ve yönetim işlevleri için mevcut bir yetkilendirme mekanizması kullanılıyor mu?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.11.3	Web Servis Çağrılarında Kimlik Doğrulama ve Yetkilendirme Kontrolü	Gözden Geçirme, Sızma Testi	Web servislerinde her çağrı için kimlik doğrulama ve yetkilendirme kontrolü yapılıyor mu?
3.2.11.4	Sunulan Web Servislerin Girdi-Çıktı Denetimlerinin Yapılması	Mülakat, Gözden Geçirme, Sızma Testi	Uygulamada kullanılan mevcut bir girdi-çıktı denetim mekanizması var mı? Mevcut girdi-çıktı denetim mekanizması web servis girdileri/çıktıları için kullanılabiliyor mu? Web servis girdileri/çıktıları için yapılan girdi-çıktı denetimlerinde hangi faaliyetler/yöntemler uygulanıyor? Yazılımda kullanılan bileşenler (çatı, kütüphane, yazılım modülleri vb.) ve uygulanan yamalar bilinen zafiyet içeriyor mu?
3.2.11.5	Web Servis Yapılandırma ve Yönetim İşlemleri	Mülakat, Gözden Geçirme, Sızma Testi	Uygulama üzerinden sunulan web servis yapılandırma ve yönetim işlevleri için mevcut bir yetkilendirme mekanizması kullanılıyor mu?
3.2.11.6	Entegre Olunan Sistemin Web Servislerinin Beklenen Şekilde Çalıştığının Doğrulanması	Mülakat, Gözden Geçirme, Sızma Testi	Entegre olunan sistemin web servislerinin beklenen şekilde çalıştığının doğrulaması nasıl yapılıyor?
3.2.11.7	Uygulamanın Kararlılığının Sağlanması	Mülakat, Gözden Geçirme, Sızma Testi	Entegre olunan sistemin web servislerine ulaşılamaması veya web servislerinin hata sonucu dönmesi durumlarında uygulamanın kararlılığı nasıl sağlanıyor? İlgili durumda ne gibi faaliyetlerin/süreçlerin uygulanacağı tanımlanmış mı?
3.2.11.8	Web Servisi Çağrı Sayısının ve Kaynak Kullanımının Sınırlandırılması	Mülakat, Gözden Geçirme, Sızma Testi	Web servisi mevcut kaynaklarının kasıtlı olarak tüketilmesini engellemek için ne gibi önlemler alınıyor?
3.2.11.9	Dış Sistemler / Uygulamalar Arası Çağrıların Kayıt Altına Alınması	Mülakat, Gözden Geçirme	Dış sistemler / uygulamalar arası çağrılar kayıt altına alınıyor mu? İlgili çağrılar için tutulmuş kayıtlar üzerinde geçmişe dönük analizler/denetimler gerçekleştiriliyor mu?
3.2.11.10	Kritik Altyapı Sistemleri ile Güvenli İletişimin Sağlanması	Mülakat, Gözden Geçirme	Kritik altyapı sistemleri ile entegrasyonda hangi iletişim altyapıları kullanılıyor?

3.3. Taşınabilir Cihaz ve Ortam Güvenliği

Amaç

Bu güvenlik tedbiri ana başlığının amacı, taşınabilir cihaz ve ortam güvenliği çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. "Taşınabilir Cihaz ve Ortam Güvenliği" ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Akıllı Telefon ve Tablet Güvenliği
- Taşınabilir Bilgisayar Güvenliği
- Taşınabilir Ortam Güvenliği (CD/DVD, Taşınabilir Bellek Ortamları)

3.3.1. Akıllı Telefon ve Tablet Güvenliği

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.3.1.1	1	Akıllı Telefon ve Tabletlerin Kabul Edilebilir Kullanımı	Mobil cihazların kurum içinde kullanılabilmesi için taşınabilir cihazların kullanımı, uygunluğu ve uzaktan yönetimi ile ilgili aşağıdaki hususları içeren mobil cihaz kullanım politikası hazırlanmalı ve uygulanmalıdır. • Fiziksel koruma ile ilgili gereksinimler, • Parola tanımlama, • Yazılım kurulum kısıtları, • İşletim sistemi ve uygulama güncelleme politikası • Uzaktan devre dışı bırakma, silme ya da kilitleme • Yedekleme • Bulut servislerinin kullanımı • Kablosuz ağların kullanımı • El değiştirme ve imha Kurum, mobil cihaz üzerinden e-posta ve/veya VPN gibi kurumsal servislere erişim izni vermeden önce politikayı çalışana tebliğ etmelidir. Gizlilik dereceli veya kurumsal mahremiyet içeren veri, doküman ve belgeler kurumsal olarak yetkilendirilmemiş veya kişisel olarak kullanılan cihazlarda bulundurulmamalıdır.
3.3.1.2	1	Mobil Cihazlarda Jailbreak veya Rootlama İşleminin Yapılmaması	Kurum bünyesinde geliştirilen uygulamalar rootlanmış/jailbreak yapılmış cihazlarda çalışmayı reddetmelidir. Kurum tarafından sağlanan telefon ve tabletler üzerinde jailbreak veya rootlama işlemi yapılmamalıdır.
3.3.1.3	1	Kullanıcılara Uygulama İzinleri Hakkında Eğitim Verilmesi	Mobil cihaz kullanıcılarına uygulamaların istedikleri izinler ve bu izinlerin riskleri hakkında eğitim verilmelidir. Bk. Tedbir No: 3.5.2.1

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.3.1.4	1	Mobil Cihaz Envanterinin Tutulması	Kuruma ait mobil cihazların yazılım ve donanım envanteri tutulmalıdır. Bk. Tedbir No: 3.1.1.1 Bk. Tedbir No: 3.1.2.1
3.3.1.5	1	Halka Açık Şarj İstasyonlarının Kullanılmaması	Çalışanlar mobil cihazlarını halka açık şarj istasyonlarında şarj etmemeleri konusunda bilgilendirilmelidir.
3.3.1.6	2	Cihazın Uzaktan Fabrika Ayarlarına Döndürülmesi	Cihazı uzaktan fabrika ayarlarına döndürüp içindeki veriyi silebilecek bir mekanizma kullanılmalıdır.
3.3.1.7	2	Tamire Verilen Cihazlarda Bulunan Verinin Silinmesi	Onarım/tadilat için üçüncü kişilere (yetkisi servis vb.) verilecek cihazlar fabrika ayarlarına döndürülmeli ve içindeki kurumsal veriler silinmelidir. Cihaz içindeki veri silinemeyecek durumda ise cihaz imha edilmelidir.
3.3.1.8	3	Güvenlik Yazılımlarının Yüklenmesi	Zararlı yazılımları tespit eden ve önleyen güvenlik uygulamaları kullanılmalıdır.
3.3.1.9	3	Taşınabilir Cihaz Yönetimi	Kritik veriye erişen kişisel ve kurumsal cihazlar uzaktan yönetilebilmeli, cihazlara güvenlik politikaları uygulanabilmeli ve gerek duyulduğunda politikalar uzaktan güncellenebilmelidir.
3.3.1.10	3	Taşınabilir Cihazların Ayrı Sistemlerde Kullanılması	Kritik seviyeli ağlarda kullanılan taşınabilir cihazlar, internete bağlı veya kurum dışı sistemlerde kullanılmamalıdır.
3.3.1.11	3	Parola Politikaları	Taşınabilir cihazlar için parola politikaları belirlenmeli ve ekran kilitleri için bu politikanın uygulanması zorunlu tutulmalıdır.
3.3.1.12	3	Çok Sayıda Hatalı Giriş Denemesi Yapılması Halinde Cihaz İçindeki Verinin Silinmesi	Kaba kuvvet saldırılarından korunmak için, kurum tarafından belirlenecek sayıda hatalı giriş denemesi sonrası cihaz belleğinde bulunan veriler silinmelidir.
3.3.1.13	3	Desteklenen Cihaz Listesinin Oluşturulması	Kurum bünyesinde kullanılacak cihazların listesi çıkartılmalı ve bu liste dışında bulunan cihazların kurum sistemlerine erişimi engellenmelidir.
3.3.1.14	3	Güncel Olmayan Cihazların Sistemlere Erişiminin Engellenmesi	Güncelleme almayan veya bilinen zafiyete sahip olan işletim sistemi veya uygulama barındıran cihazların kurum sistemlerine erişimi engellenmelidir.
3.3.1.15	3	Seyahat Kullanım Politikasının Tanımlanması	Yurt dışı seyahatleri sırasında kullanılacak cihazlar için bir kullanım politikası hazırlanmalı, cihazlar seyahat sonrası bu politikaya göre kontrol edilmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.3.1.1	Akıllı Telefon ve Tabletlerin Kabul Edilebilir Kullanımı	Mülakat, Gözden Geçirme	Kurum verisine erişen kişisel cihazlar için tanımlanmış bir mobil cihaz kullanım politikası var mıdır? Politika içeriğinde aşağıdaki konular ele alınmakta mıdır? • İşletim sisteminin ve uygulamaların güncel tutulması gerektiği belirtilmiş midir? • Güncelleme almayan cihazalar için ne gibi önlemler tanımlanmıştır? • Hangi bulut servislerinin kullanılabileceği belirtilmiş midir? • Kullanımda olmayan kablosuz teknolojilerin (wifi, hotspot, airdrop vb.) kapalı tutulması gerektiği belirtilmiş midir? • Güvensiz kablosuz ağların (Otel, havalimanı vb.) kullanımına kısıtlama getirilmiş midir? • Cihazlarda ekran kilidi olması zorunlu tutulmuş mudur? • Root ve Jailbreak yapılması yasaklanmış mıdır? • Uygulamaların hangi kaynaklardan kurulması gerektiği belirtilmiş midir? • Uzaktan cihaz yönetimine izin veren fonksiyonların kullanımı ile ilgili maddeler var mıdır? Politika çalışanlara tebliğ edilmiş midir?
3.3.1.2	Mobil Cihazlarda Jailbreak veya Rootlama İşleminin Yapılmaması	Mülakat, Güvenlik Denetimi	Kurum için geliştirilen uygulamalar root veya jailbreak yapılmış cihazlarda çalışmayı reddetmekte midir? Mobil cihaz kullanım politikasında root veya jailbreak yapılmış cihazlar için hangi önlemler tanımlanmıştır?
3.3.1.3	Kullanıcılara Uygulama İzinleri Hakkında Eğitim Verilmesi	Mülakat	Kullanıcılara mobil cihaz güvenliği eğitimi verilmekte midir? Genel farkındalık eğitimleri içinde mobil cihaz güvenliğinden bahsedilmekte midir?
3.3.1.4	Mobil Cihaz Envanterinin Tutulması	Mülakat, Gözden Geçirme	Kurumun sahibi olduğu cihazların yazılım ve donanım envanteri tutulmakta mıdır?
3.3.1.5	Halka Açık Şarj İstasyonlarının Kullanılmaması	Mülakat, Güvenlik Denetimi	Mobil cihaz kullanım politikasında kullanıcılara halka açık şarj istasyonlarını kullanmamaları gerektiği bildirilmiş midir?
3.3.1.6	Cihazın Uzaktan Fabrika Ayarlarına Döndürülmesi	Mülakat	Mobil cihaz kullanım politikasında kurum çalışanlarının cihazlarını uzaktan fabrika ayarlarına döndürmelerini sağlayacak ayarları yapmaları istenmekte midir?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.3.1.7	Tamire Verilen Cihazlarda Bulunan Verinin Silinmesi	Mülakat	Kuruma ait mobil cihazlar tamire verilmeden önce fabrika ayarlarına döndürülmekte midir? Fabrika ayarlarına döndürülemeyen cihazlar için imha prosedürü tanımlanmış mıdır? Mobil cihaz kullanım politikasında kullanıcılara kendi cihazlarını fabrika ayarlarına döndürmeden üçüncü kişilere satmaması veya tamire vermemesi gerektiği belirtilmiş midir?
3.3.1.8	Güvenlik Yazılımlarının Yüklenmesi	Mülakat, Güvenlik Denetimi	Zararlı yazılımları tespit eden ve önleyen uygulamalar kullanılmakta mıdır?
3.3.1.9	Taşınabilir Cihaz Yönetimi	Mülakat, Güvenlik Denetimi	Kurum kritik veriye erişen cihazlarını merkezi olarak yönetebilmekte midir? Mobil cihaz kullanım politikasında listelenen tedbirleri kapsayan bir güvenlik politikası belirlenmiş midir? Güvenlik politikası kritik veriye erişen cihazlara yüklenmiş midir?
3.3.1.10	Taşınabilir Cihazların Ayrı Sistemlerde Kullanılması	Mülakat, Güvenlik Denetimi	Kritik seviyeli ağlarda kullanılan taşınabilir cihazlar kurum dışı veya internete bağlı ağlarda kullanılmakta mıdır?
3.3.1.11	Parola Politikaları	Mülakat, Güvenlik Denetimi	Kurumun güvenlik ihtiyaçlarına göre bir mobil cihaz parola politikası belirlenmiş midir? Politikanın kullanımı merkezi yönetim yazılımı ile zorunlu kılınmış mıdır?
3.3.1.12	Çok Sayıda Hatalı Giriş Denemesi Yapılması Halinde Cihaz İçindeki Verinin Silinmesi	Mülakat, Güvenlik Denetimi	Kilit ekranında çok sayıda hatalı giriş denemesi yapılan cihazların fabrika ayarlarına dönmesini sağlayan bir politika oluşturulmuş mudur? Politikanın kullanımı merkezi yönetim yazılımı ile zorunlu kılınmış mıdır? Mobil cihazlar kaç hatalı deneme sonrasında fabrika ayarlarına dönecek şekilde yapılandırılmıştır?
3.3.1.13	Desteklenen Cihaz Listesinin Oluşturulması	Mülakat, Güvenlik Denetimi	Kurumda kullanılmasına izin verilen cihazların listesi oluşturulmuş mudur? Cihaz seçiminde hangi kriterler kullanılmıştır?
3.3.1.14	Güncel Olmayan Cihazların Sistemlere Erişiminin Engellenmesi	Mülakat, Güvenlik Denetimi	Merkezi yönetim sistemi, güvenlik yamaları yüklenmemiş ya da üzerinde kara listeye alınmış uygulama/uygulama sürümü barındıran cihazların sisteme erişimini engelliyor mudur?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.3.1.15	Seyahat Kullanım Politikasının Tanımlanması	Mülakat	Yurt dışı seyahatleri sırasında kullanılacak cihazlar için bir kullanım politikası hazırlanmış mıdır? Yurt dışına giden personelin yurda dönüşte mobil cihazları incelemeye alınmakta mıdır? İncelemeye alınan cihazlar için hangi kontroller uygulanmaktadır?

3.3.2. Taşınabilir Bilgisayar Güvenliği

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.3.2.1	1	Taşınabilir Bilgisayarların Kabul Edilebilir Kullanımı	Taşınabilir bilgisayarların kurum bünyesinde kullanılabilmesi için taşınabilir bilgisayarların kullanımı, uygunluğu ve uzaktan yönetimi ile ilgili aşağıdaki hususları içeren kullanım politikası hazırlanmalı ve uygulanmalıdır. • Fiziksel koruma ile ilgili gereksinimler • Parola tanımlama • Yazılım kurulum kısıtları • İşletim sistemi ve uygulama güncelleme politikası • Yedekleme • Bulut servislerinin kullanımı • Kablosuz ağların kullanımı • El değiştirme ve imha Kurum, taşınabilir bilgisayarın temini öncesinde politikayı çalışana tebliğ etmelidir. Gizlilik dereceli veya kurumsal mahremiyet içeren veri, doküman ve belgeler kurumsal olarak yetkilendirilmemiş veya kişisel olarak kullanılan cihazlarda bulundurulmamalıdır.
3.3.2.2	1	Güvenlik Yazılımlarının Yüklenmesi	Zararlı yazılımları tespit eden ve önleyen güvenlik yazılımları kullanılmalıdır. Bk. Tedbir No: 3.1.5.1 Bk. Tedbir No: 3.1.5.4
3.3.2.3	1	Tamire Verilen Taşınabilir Bilgisayarlarda Bulunan Verinin Silinmesi	Onarım/tadilat için üçüncü kişilere (yetkisi servis vb.) verilecek taşınabilir bilgisayarlar fabrika ayarlarına döndürülmeli ve içindeki kurumsal veriler güvenli yöntemler kullanılarak silinmelidir.
3.3.2.4	2	Disk Şifreleme	Taşınabilir bilgisayarlara, çalınma ve kaybolma riskine karşı disk şifreleme uygulanmalıdır. Kullanıcıların disk şifreleme özelliğini devre dışı bırakmaları engellenmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.3.2.5	3	Harici Depolama Ortamlarına Erişimin Yönetimi	Taşınabilir bilgisayarlarda, harici depolama ortamlarına okuma ve yazma izinleri varsayılan olarak devre dışı bırakılmalıdır. İş gereksinimleri doğrultusunda gerekli onayların alınması durumunda okuma ve yazma izinleri devreye alınmalı, yapılan işlemler izlenmelidir.
3.3.2.6	3	Taşınabilir Bilgisayar Yönetimi	Taşınabilir bilgisayarlar uzaktan yönetilebilmeli, cihazlara güvenlik politikaları uygulanabilmeli ve gerek duyulduğunda politikalar uzaktan güncellenebilmelidir.
3.3.2.7	3	Güncel Olmayan Bilgisayarların Sistemlere Erişiminin Engellenmesi	Güncel olmayan işletim sistemi ve/veya güvenlik yazılımları barındıran bilgisayarların kurum sistemlerine erişimi engellenmelidir.
3.3.2.8	3	Seyahat Kullanım Politikasının Tanımlanması	Yurt dışı seyahatleri sırasında kullanılacak bilgisayarlar için bir kullanım politikası hazırlanmalı, bilgisayarlar seyahat sonrası bu politikaya göre kontrol edilmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.3.2.1	Taşınabilir Bilgisayarların Kabul Edilebilir Kullanımı	Mülakat	Kurum verisine erişen taşınabilir bilgisayarlar için tanımlanmış bir kullanım politikası var mıdır? Politika içeriğinde aşağıdaki konular ele alınmakta mıdır? • Fiziksel koruma ile ilgili gereksinimler • Parola tanımlama • Yazılım kurulum kısıtları • İşletim sistemi ve uygulama güncelleme politikası • Yedekleme • Bulut servislerinin kullanımı • Kablosuz ağların kullanımı • El değiştirme ve imha Politika çalışanlara tebliğ edilmiş midir?
3.3.2.2	Güvenlik Yazılımlarının Yüklenmesi	Mülakat, Güvenlik Denetimi	Taşınabilir bilgisayarlara hangi güvenlik yazılımları kurulmaktadır?
3.3.2.3	Tamire Verilen Taşınabilir Bilgisayarlarda Bulunan Verinin Silinmesi	Mülakat	Kuruma ait mobil cihazlar tamire verilmeden önce hangi güvenlik önlemleri uygulanmaktadır?
3.3.2.4	Disk Şifreleme	Mülakat, Güvenlik Denetimi	Taşınabilir bilgisayarlar için çalınma ve kaybolma riskine karşı ne gibi önlemler alınmaktadır?
3.3.2.5	Harici Depolama Ortamlarına Erişimin Yönetimi	Mülakat, Güvenlik Denetimi	Kritik veriye erişim imkânı olan taşınabilir bilgisayarlarda, harici depolama ortamlarını okuma ve yazma özellikleri devre dışı bırakılmış mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.3.2.6	Taşınabilir Bilgisayar Yönetimi	Mülakat, Güvenlik Denetimi	Kurum kritik veriye erişen cihazlarını merkezi olarak yönetebilmekte midir? Mobil cihaz kullanım politikasında listelenen tedbirleri kapsayan bir güvenlik politikası oluşturulmuş mudur? Güvenlik politikası kritik veriye erişen cihazlara yüklenmiş midir?
3.3.2.7	Güncel Olmayan Bilgisayarların Sistemlere Erişiminin Engellenmesi	Mülakat, Güvenlik Denetimi	Merkezi yönetim sistemi, güvenlik yamaları yüklenmemiş ya da üzerinde kara listeye alınmış uygulama/uygulama sürümü barındıran taşınabilir bilgisayarların sisteme erişimini engellemekte midir?
3.3.2.8	Seyahat Kullanım Politikasının Tanımlanması	Mülakat	Yurt dışı seyahatleri sırasında kullanılacak taşınabilir bilgisayarlar için bir kullanım politikası hazırlanmış mıdır? Yurt dışına giden personelin yurda dönüşte taşınabilir bilgisayarları incelemeye alınmakta mıdır? İncelemeye alınan bilgisayarlar için hangi kontroller uygulanmaktadır?

3.3.3. Taşınabilir Ortam Güvenliği (CD/DVD, Taşınabilir Bellek Ortamları)

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.3.3.1	1	Taşınabilir Ortamların Kabul Edilebilir Kullanımı	Taşınabilir ortam yönetimine ilişkin en az fiziksel koruma ve saklama ile ilgili gereksinimler, yedekleme, el değiştirme ve imha hususlarını içeren kullanım politikası hazırlanmalı ve uygulanmalıdır.
3.3.3.2	1	Taşınabilir Ortamların Saklama ve Kullanım Koşulları	Tüm taşınabilir ortamlar, olumsuz fiziksel etkilere karşı üretici tarafından tavsiye edilen saklama ve kullanım koşullarına uyumlu olarak kullanılmalıdır.
3.3.3.3	2	Taşınabilir Ortamların Barındırdığı Verilerin Güvenliği	Taşınabilir ortamlar üzerinde yer alan kritik bilgi/veri şifreli olarak saklanmalıdır.
3.3.3.4	2	Taşınabilir Ortamların Güvenli İmhası	Kullanım süresi dolmuş taşınabilir ortamlar veri sızıntılarını önlemek amacıyla güvenli olarak imha edilmelidir.
3.3.3.5	2	Taşınabilir Ortam Bilgisinin Yedeklenmesi	Taşınabilir ortam içindeki bilgi/veri saklanması gereken süre göz önünde bulundurularak güvenli şekilde yedeklenmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.3.3.1	Taşınabilir Ortamların Kabul Edilebilir Kullanımı	Mülakat	Kurum verisini barındıran taşınabilir ortamlar için tanımlanmış bir kullanım politikası var mıdır? Kabul edilebilir kullanım politikası içeriğinde hangi konular ele alınmaktadır? Politika çalışanlara tebliğ edilmiş midir?
3.3.3.2	Taşınabilir Ortamların Saklama ve Kullanım Koşulları	Mülakat	Taşınabilir ortamların güvenliğine yönelik hangi kontroller uygulanmaktadır?
3.3.3.3	Taşınabilir Ortamların Barındırdığı Verilerin Güvenliği	Mülakat, Güvenlik Denetimi	Taşınabilir ortamların barındırdığı verilerin güvenliği nasıl sağlanmaktadır?
3.3.3.4	Taşınabilir Ortamların Güvenli İmhası	Mülakat, Güvenlik Denetimi	Taşınabilir ortamların imhasına yönelik nasıl bir prosedür işletilmektedir?
3.3.3.5	Taşınabilir Ortam Bilgisinin Yedeklenmesi	Mülakat, Güvenlik Denetimi	Taşınabilir ortamların barındırdığı verilere yönelik yedekleme prosedürü nasıl işletilmektedir?

3.4. Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği

Amaç

Bu güvenlik tedbiri ana başlığının amacı, nesnelerin interneti cihazlarının güvenliği çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. “Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği” ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Ağ Servisleri ve İletişimi
- Dâhili Veri Depolama
- Kimlik Doğrulama ve Yetkilendirme
- API ve Bağlantı Güvenliği
- Diğer Güvenlik Tedbirleri

3.4.1. Ağ Servisleri ve İletişimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.4.1.1	1	Ağ Portlarının Kısıtlanması	Cihazlarda sadece ilgili fiziksel ve mantıksal portlar ile servisler açık bırakılmalıdır.
3.4.1.2	1	Ağ Servislerinin Güvenlik Kontrolleri	Gerekli tüm ağ servislerinin açıklara ve saldırılara karşı kontrolleri periyodik olarak yapılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.4.1.3	1	Güvenli Yapılandırma	Cihaza yönelik aşağıda yer alan işlemlerin yapılması ve işlemler sırasında gerekli tüm bilgilerin güvenli bir şekilde aktarılması sağlanmalıdır. • Cihaz kurulumu • Konfigürasyon güncellemeleri • Sistem yazılımı güncellemeleri • İşletim sistemi ve kütüphane güncellemeleri IoT cihazlarının kurulumu ve yapılandırılması, yeniden başlatma ve kurtarma işlemleri vb. operasyonel ve yönetsel faaliyetlere ilişkin işletim prosedürleri hazırlanmalıdır.
3.4.1.4	1	Cihazın Güvenli İmhası veya Tekrar Kullanımı	Cihazın depolama ortamı içeren tüm parçaları elden çıkarılmadan veya yeniden kullanılmadan önce, herhangi bir kritik veri ve/veya lisanslı yazılım varsa kaldırılmasını veya güvenli şekilde üzerine yazılmasını sağlamak için kontrol edilmelidir. Verinin ve veri içeren ortamların güvenli imhası için işletilecek yöntemler verinin kritikliği göz önünde bulundurularak sınıflandırılmalı, yazılı hale getirilmeli ve uygulamaya alınmalıdır.
3.4.1.5	1	Yetkisiz Cihazların Kurum Ağına Bağlanmasının Engellenmesi	IoT cihazlarının izin alınmadan ağa bağlanmalarını ve yer değiştirmelerini engellemek amacıyla gerekli önlemler alınmalıdır.
3.4.1.6	2	Cihaz Güvenlik Duvarının Aktifleştirilmesi	Cihazlarda varsa güvenlik duvarı aktifleştirilmeli ve IoT sistemlerini kritik BT sistemlerinden izole etmek için güvenlik duvarları kullanılmalıdır.
3.4.1.7	2	Kablosuz Erişim Noktalarına Güvenli Bağlantı	Cihazların kablosuz erişim noktalarına bağlantıları güvenli erişim protokolleri ile desteklenmelidir.
3.4.1.8	2	Cihazların Merkezi Yönetimi	Cihazlar, merkezi bir yazılım üzerinden yönetilmelidir.
3.4.1.9	3	Ağ Üzerinden Gönderilen Verinin Şifrelenmesi	Cihazın ağ üzerinden veri gönderimi sırasında, kritik veri cihazın desteklediği şifreleme algoritmalarıyla şifrelenmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.4.1.1	Ağ Portlarının Kısıtlanması	Güvenlik Denetimi, Sızma Testi	Cihazlarda gerektiğinden fazla port açık mıdır? Cihazın ağ portları ve servisleri internet üzerinden erişilebilir midir?
3.4.1.2	Ağ Servislerinin Güvenlik Kontrolleri	Mülakat, Gözden Geçirme	Ağ servisleri üzerinde zafiyet taramaları periyodik olarak yapılmakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.4.1.3	Güvenli Yapılandırma	Mülakat, Güvenlik Denetimi	Cihaz üzerine aktarılacak konfigürasyon verisinin güvenli bir şekilde iletildiği nasıl garanti altına alınmaktadır? IoT cihazlarının kurulumu ve yapılandırılması, yeniden başlatma ve kurtarma işlemleri vb. operasyonel ve yönetsel faaliyetlere ilişkin işletim prosedürleri hazırlanmakta mıdır?
3.4.1.4	Cihazın Güvenli İmhası veya Tekrar Kullanımı	Mülakat, Gözden Geçirme	Verinin ve veri içeren ortamların güvenli imhası veya tekrar kullanımı için işletilecek yöntemler yazılı hale getirilmiş ve uygulanmakta mıdır? İmha işleminde bilgilerin açığa çıkmaması ve başkalarının eline geçmemesi için ne gibi önlemler alınmaktadır?
3.4.1.5	Yetkisiz Cihazların Kurum Ağına Bağlanmasının Engellenmesi	Mülakat, Güvenlik Denetimi, Sızma Testi	Yetkisiz cihazların kurum ağına bağlanmasını engellemek üzere ne gibi önlemler alınmaktadır?
3.4.1.6	Cihaz Güvenlik Duvarının Aktifleştirilmesi	Güvenlik Denetimi	Güvenlik duvarı imkânı olan cihazlarda, güvenlik duvarı aktif olarak kullanılmakta mıdır? Güvenlik duvarının konfigürasyonu yapılmış mıdır?
3.4.1.7	Kablosuz Erişim Noktalarına Güvenli Bağlantı	Güvenlik Denetimi	Cihazların kablosuz erişim noktalarına erişimleri güvenli erişim protokolleri ile desteklenmekte midir?
3.4.1.8	Cihazların Merkezi Yönetimi	Güvenlik Denetimi	Cihazların yönetilmesi için merkezi bir yazılım kullanılmakta mıdır?
3.4.1.9	Ağ Üzerinden Gönderilen Verinin Şifrelenmesi	Mülakat, Güvenlik Denetimi	Cihazlardan gönderilen kritik veri şifreli gönderilmekte midir? Kullanılan şifreleme algoritmaları nelerdir?

3.4.2. Dâhili Veri Depolama

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.4.2.1	1	Veri Yedekleme	Cihaz üzerinde yer alan veri, bilgi güvenliği ve yedekleme ihtiyaçları doğrultusunda düzenli olarak yedeklenmelidir.
3.4.2.2	1	Verilere Yetkili Erişim	IoT sistemlerinde depolanan verilerin güvenliğinin sağlanması için yetkilendirme sağlanmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.4.2.3	3	Kullanılan Cihazlardan Kritik Verinin Temizlenmesi	Bilgi güvenliği gereksinimleri göz önünde bulundurularak, kullanımına ihtiyaç kalmayan veya farklı alanlarda kullanılacak cihazlar üzerindeki kritik veri geri döndürülemeyecek şekilde silinmelidir. Kritik verinin cihaz üzerinden güvenli silinmesinin mümkün olmadığı durumlarda cihaz ulusal/uluslararası kabul görmüş yöntemlere uygun şekilde imha edilmelidir. Bk. Tedbir No: 3.4.1.4

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.4.2.1	Veri Yedekleme	Mülakat, Gözden Geçirme	Cihaz üzerinde yer alan veri hangi aralıklarla yedeklenmektedir? Yedekleme periyotları kurumun bilgi güvenliği gereksinimleri ile uyumlu mudur?
3.4.2.2	Verilere Yetkili Erişim	Mülakat, Güvenlik Denetimi	IoT sistemlerinde depolanan verilerin güvenliğinin sağlanması için erişim yetkilendirme sağlanmakta mıdır?
3.4.2.3	Kullanılan Cihazlardan Kritik Verinin Temizlenmesi	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Kritik verilerin cihazlardan geri döndürülemeyecek şekilde silinmesi amacıyla bir prosedür belirlenmiş ve uygulanmakta mıdır? Cihaz üzerinden kritik verinin silinmesinin mümkün olmadığı durumlarda hangi yöntemler uygulanmaktadır? Cihazların imhasına yönelik tanımlanmış prosedür var mıdır? İmha sürecinde hangi yöntemlerden faydalanılmaktadır?

3.4.3. Kimlik Doğrulama ve Yetkilendirme

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.4.3.1	1	Oturum Sonlandırma İşlemlerinin Aktifleştirilmesi	Sistemde tanımlı ise oturum sonlandırma işlemleri aktifleştirilmelidir. Bilgi güvenliğini tehdit eden bir durumun ortaya çıkması halinde oturum sonlandırma ve cihazı pasife alma işlemleri uzaktan yapılabilmelidir.
3.4.3.2	1	Kimlik Doğrulama Politikası	Güçlü kimlik doğrulama politikası tanımlanmalı ve uygulanmalıdır. Cihazın içinde iletişim için kullanılan kimlik bilgileri güvenli bir şekilde tutulmalıdır.
3.4.3.3	1	Kullanıcı Yetki Sınırlaması	Kullanıcı hesapları tekil olacak şekilde oluşturulmalı, bilgi güvenliği gereksinimleri ve cihazın yetenekleri doğrultusunda erişim yetkileri asgari düzeyde tanımlanmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.4.3.4	1	Varsayılan Kimlik Doğrulama Bilgilerinin Değiştirilmesi	Ön tanımlı parolalar ve kullanıcı isimleri, kullanım öncesinde mutlaka değiştirilmeli ve kullanılan parolaların güvenli bir alanda muhafaza edilmesi sağlanmalıdır.
3.4.3.5	1	Sıfırlama Mekanizmaları	Cihaz üzerinde sıfırlama mekanizması bulunmalı ve bu mekanizmaya yetkisiz erişim engellenmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.4.3.1	Oturum Sonlandırma İşlemlerinin Aktifleştirilmesi	Güvenlik Denetimi	Giriş yapılan hesaplarda isteğe bağlı veya otomatik olarak oturum sonlandırılmakta mıdır? Bilgi güvenliğini tehdit eden bir durumun ortaya çıkması halinde oturum sonlandırma ve cihazı pasife alma işlemleri gerçekleştirilebilmekte midir?
3.4.3.2	Kimlik Doğrulama Politikası	Güvenlik Denetimi	Sistemde güçlü parola politikası aktif olarak kullanılmakta mıdır? Sistemde teknik olarak parola yenileme politikası mevcut ise aktif midir? Sistemde iki adımlı doğrulama mekanizması mevcut ise aktif midir?
3.4.3.3	Kullanıcı Yetki Sınırlaması	Güvenlik Denetimi	Sistemde kullanıcılar asgari düzeyde yetkiye sahip midir? Kullanıcıları sorumlu tutacak şekilde her kullanıcıya özel bir kullanıcı adı tanımlanmakta mıdır ve bu kullanıcı işlemlerinin kayıtları tutulmakta mıdır?
3.4.3.4	Varsayılan Kimlik Doğrulama Bilgilerinin Değiştirilmesi	Güvenlik Denetimi, Sızma Testi	Kurulum aşamasından sonra ön tanımlı parolalar değiştirilmekte midir? Parolalar nerede tutulmaktadır?
3.4.3.5	Sıfırlama Mekanizmaları	Güvenlik Denetimi	Cihaz üzerinde sıfırlama mekanizması bulunmakta mıdır? Bu mekanizmaya yetkisiz erişim nasıl engellenmektedir?

3.4.4. API ve Bağlantı Güvenliği

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.4.4.1	1	Varsayılan Kimlik Doğrulama Bilgilerinin Değiştirilmesi	Sistemde yerel veya bulut tabanlı web uygulamalarının varsayılan kimlik doğrulama bilgisi değiştirilmelidir. Bk. Tedbir No: 3.2.1.6
3.4.4.2	1	API ve Bağlantı Güvenliği	API ve bağlantılarda IP kısıtlaması yapılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.4.4.3	2	Web Uygulama Güvenlik Duvarı Kullanımı	Sistemde web uygulama güvenlik duvarı mevcut ise nesnelerin interneti cihazları için aktifleştirilmelidir.
3.4.4.4	2	Sistem API'lerinde Güvenli Haberleşme Protokolü Kullanımı	API'ler cihazın desteklediği bilinen zafiyet içermeyen güvenilir sürüme sahip bir haberleşme protokolü üzerinden haberleşmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.4.4.1	Varsayılan Kimlik Doğrulama Bilgilerinin Değiştirilmesi	Güvenlik Denetimi	Sistemde kullanılan yerel veya bulut tabanlı web uygulamalarına ait varsayılan kimlik doğrulama bilgileri değiştirilmekte midir?
3.4.4.2	API ve Bağlantı Güvenliği	Mülakat, Güvenlik Denetimi	API ve bağlantılarda IP kısıtlama yapılmakta mıdır?
3.4.4.3	Web Uygulama Güvenlik Duvarı Kullanımı	Mülakat, Güvenlik Denetimi	IoT sistemleri için web uygulama güvenlik duvarı kullanılmakta mıdır?
3.4.4.4	Sistem API'lerinde Güvenli Haberleşme Protokolü Kullanımı	Mülakat, Güvenlik Denetimi	Sistem API'leri cihazın desteklediği güvenli bir haberleşme protokolü kullanmakta mıdır? Kullanılan protokoller nelerdir?

3.4.5. Diğer Güvenlik Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.4.5.1	1	Güncellemelerin Kontrolü	Sistemde varsa yeni güncelleme alma özelliği aktifleştirilmeli ve güncellemeler güvenilir kaynaklardan periyodik olarak alınmalıdır.
3.4.5.2	1	Cihazlara Fiziksel Erişimin Kısıtlanması	Cihazlara sadece yetkili kişiler fiziksel erişim sağlamalıdır. Yetkisiz kişilerin fiziksel erişimini engelleyecek güvenlik tedbirleri alınmalıdır.
3.4.5.3	3	Gömülü İşletim Sistemi İçin Kod Analiz Raporu Alınması	Gömülü işletim sistemi için mümkünse onaylanmış kod analiz raporu alınmalıdır.
3.4.5.4	3	Elektromanyetik Sızıntılara Karşı Güvenlik Önlemlerinin Alınması	Cihaza yönelik elektromanyetik sızıntılara karşı gerekli güvenlik önlemleri alınmalıdır.
3.4.5.5	3	Tersine Mühendisliğe Karşı Koruma	Cihazın donanımı ve yazılımı tersine mühendisliği zorlaştıracak şekilde tasarlanmış olmalı ve tersine mühendisliğe karşı korunmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.4.5.6	3	Güvenli Önyükleme	Cihaz güvenli önyükleme (secure boot) özelliğine sahip olmalıdır.
3.4.5.7	3	Güncellemelerin Güvenilir Kanallar Üzerinden Yapılması	Dışarıdan cihaza gelen güncellemeler cihazın desteklediği ölçüde imza doğrulaması yapılarak kontrol edilmelidir. Eğer cihaz güncelleme kaynağının doğruluğunu kontrol edebilecek bir mekanizma desteklemiyorsa, güncellemeler sadece yetkili kişiler tarafından fiziksel olarak yapılmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.4.5.1	Güncellemelerin Kontrolü	Mülakat, Güvenlik Denetimi	Sistem üzerinde güncellemeler düzenli olarak alınmakta mıdır? Güncellemelere yönelik kontroller nasıl yapılmaktadır?
3.4.5.2	Cihazlara Fiziksel Erişimin Kısıtlanması	Mülakat, Güvenlik Denetimi	Cihazlara fiziksel erişim güvenliğini sağlamak için ne gibi önlemler alınmaktadır? Herhangi bir güvenlik ihlali durumunda işletilmesi planlanan eylem planı bulunmakta mıdır?
3.4.5.3	Gömülü İşletim Sistemi İçin Kod Analiz Raporu Alınması	Güvenlik Denetimi	Gömülü işletim sistemi için onaylanmış kod analiz raporu alınmakta mıdır?
3.4.5.4	Elektromanyetik Sızıntılara Karşı Güvenlik Önlemlerinin Alınması	Güvelik Analizi	Cihaza yönelik elektromanyetik sızıntılara karşı hangi güvenlik tedbirleri alınmaktadır?
3.4.5.5	Tersine Mühendisliğe Karşı Koruma	Güvenlik Denetimi	Cihazın tersine mühendisliğe karşı korumak amacıyla ne gibi önlemler alınmaktadır? Cihazın donanım ve yazılım bileşenleri tersine mühendisliği zorlaştıracak şekilde tasarlanmış mıdır?
3.4.5.6	Güvenli Önyükleme	Güvenlik Denetimi	Cihaz güvenli önyükleme (secure boot) özelliğine sahip midir?
3.4.5.7	Güncellemelerin Güvenilir Kanallar Üzerinden Yapılması	Mülakat, Güvenlik Denetimi	Cihaz güncellemeleri nasıl yapılmaktadır? Güncelleme yapılmadan önce güncellemenin geldiği kaynak kontrol edilmekte midir? Eğer güncelleme kaynağı kontrol edilemiyorsa, güncellemeler sadece fiziksel olarak yetkili kişiler tarafından mı yapılmaktadır?

3.5. Personel Güvenliği

Amaç

Bu güvenlik tedbiri ana başlığının amacı, personel güvenliği çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. “Personel Güvenliği” ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Genel Güvenlik Tedbirleri
- Eğitim ve Farkındalık Faaliyetleri
- Tedarikçi İlişkileri Güvenliği

3.5.1. Genel Güvenlik Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.5.1.1	1	Güvenlik Soruşturmalarının Yapılması	İşe alım aşamasında, yasal düzenlemeler ve iş gereksinimleri göz önünde bulundurularak tüm aday personel için akademik bilgilerin ve geçmiş iş tecrübelerinin doğruluğu, referanslar ve sahip olunan sertifikaların geçerliliği kontrol edilmeli, adli sicil kaydı sorgulaması yapılmalıdır.
3.5.1.2	1	Varlıkların Kabul Edilebilir Kullanım Kurallarının Tanımlanması	Kurum varlıklarının kabul edilebilir kullanım politikası belirlenerek kurum personelinin ve yüklenicilerin bu kurallara uyum sağlaması taahhüt altına alınmalıdır.
3.5.1.3	1	Temiz Masa Temiz Ekran Politikasının Tanımlanması	Fiziksel ortam, taşınabilir bilgi/veri depolama ortamları ve diğer bilgi işleme olanaklarını kapsayan temiz masa temiz ekran politikası tanımlanmalı ve uygulanmalıdır.
3.5.1.4	1	Sözleşmelerde Bilgi Güvenliği Hususlarının Yer Alması	Personel ve yüklenicilerin kurum varlıklarına erişimi sağlanmadan önce, kendileriyle yapılan sözleşmelerde bilgi güvenliği sorumlulukları belirtilmelidir.
3.5.1.5	1	Sosyal Medya Kullanım Politikasının Uygulanması	Sosyal medya kullanım politikası oluşturulmalı ve bu kapsamda personel tarafından sosyal medya üzerinden gizlilik dereceli veri paylaşımı ve haberleşme yapılmaması garanti altına alınmalıdır.
3.5.1.6	1	Bilgi Güvenliği İhlal Olayına Yönelik Disiplin Sürecinin Tanımlanması	Bilgi güvenliği ihlal olaylarını yönetmek amacıyla ilgili yasalar, iş sözleşmeleri vb. unsurlar göz önünde bulundurularak bir disiplin süreci tanımlanmalı ve uygulanmalıdır.
3.5.1.7	1	Rol, Sorumluluk ve Asgari Yetkinliklerin Tanımlanması	Kurum personeli tarafından gerçekleştirilen işin tanımı ve gereklilikleri göz önünde bulundurularak, ilgili personelin kurum bünyesindeki bilgi güvenliği rolü, sorumlulukları ve sahip olması gereken asgari yetkinlikler tanımlanmalı ve yazılı hale getirilmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.5.1.8	1	İstihdam Sorumluluklarının Sonlandırılması veya Değiştirilmesi	İstihdam sorumlulukları değişen personel/yükleniciye yeni bilgi güvenliği sorumlulukları ve görevleri; istihdamı sonlandırılan personel/yükleniciye ise istihdamın sona ermesinden sonra devam edecek bilgi güvenliği sorumlulukları bildirilmelidir.
3.5.1.9	1	Gizlilik ile İlgili Gereksinimlerin Personele Tebliğ Edilmesi	Kurumun bilgi güvenliği gereksinimleri göz önünde bulundurularak personel veya yüklenicilerin uyması gereken politika, prosedür, talimat gibi dokümanlar ilgili personel/yükleniciye tebliğ edilmelidir. İlgili dokümanların içeriği bilgi güvenliği gereksinimlerinde değişiklik olması durumunda güncellenmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.5.1.1	Güvenlik Soruşturmalarının Yapılması	Mülakat, Gözden Geçirme	İşe başvuru yapan personel tarafından beyan edilen akademik bilgilerin ve sertifikaların geçerliliği nasıl kontrol edilmektedir? Doğrulama kontrolleri kapsamında adli sicil kaydı, geçmiş iş tecrübeleri ve ilişkili referansların kontrolü yapılmakta mıdır? Doğrulama kontrollerine yönelik değerlendirme sonuçları nasıl ve nerede tutulmaktadır?
3.5.1.2	Varlıkların Kabul Edilebilir Kullanım Kurallarının Tanımlanması	Mülakat, Gözden Geçirme	Varlıkların kabul edilebilir kullanım politikası belirlenmiş midir? Varlıkların kabul edilebilir kullanım politikası kurum personeli ve yüklenicilere duyurulmuş mudur? Kurum personeli ve yüklenicilerin varlıkların kabul edilebilir kullanım politikasına uyum sağlamaları hususu taahhüt altına alınmış mıdır?
3.5.1.3	Temiz Masa Temiz Ekran Politikasının Tanımlanması	Mülakat, Gözden Geçirme	Fiziksel ortam, taşınabilir bilgi/veri depolama ortamları ve diğer bilgi işleme olanaklarını kapsayan temiz masa temiz ekran politikası tanımlanmış mıdır? Temiz masa temiz ekran politikası personel ve yüklenicilere nasıl bildirilmektedir? Temiz masa temiz ekran politikasının ihlal edilmesi durumunda işletilecek süreç tanımlanmış mıdır?
3.5.1.4	Sözleşmelerde Bilgi Güvenliği Hususlarının Yer Alması	Mülakat, Gözden Geçirme	İşe yeni başlayan personel ve yüklenicilerle yapılan sözleşme içeriklerinde bilgi güvenliği hususları yer almakta mıdır? Sözleşme içerikleri kapsamında bilgi güvenliği ile ilgili gerekliliklerin yeterli düzeyde ele alındığının kontrolü düzenli olarak yapılmakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.5.1.5	Sosyal Medya Kullanım Politikasının Uygulanması	Mülakat, Gözden Geçirme	Sosyal medya kullanım politikası oluşturulmuş mudur? Sosyal medya kullanım politikası içeriğinde hangi konular ele alınmıştır? Gizlilik dereceli verinin personel tarafından sosyal medya üzerinden paylaşılmaması hususu nasıl garanti altına alınmaktadır?
3.5.1.6	Bilgi Güvenliği İhlal Olayına Yönelik Disiplin Sürecinin Tanımlanması	Mülakat, Gözden Geçirme	Bilgi güvenliği ihlal olayını gerçekleştiren personel/yükleniciye yönelik ilgili yasalar, iş sözleşmeleri vb. unsurlar göz önünde bulundurularak oluşturulmuş bir disiplin süreci var mıdır?
3.5.1.7	Rol, Sorumluluk ve Asgari Yetkinliklerin Tanımlanması	Mülakat, Gözden Geçirme	Kurum personeli tarafından gerçekleştirilen işin tanımı ve gereklilikleri göz önünde bulundurularak, personelin kurum bünyesindeki bilgi güvenliği rolü, sorumlulukları ve sahip olması gereken asgari yetkinlikler tanımlanmakta mıdır?
3.5.1.8	İstihdam Sorumluluklarının Sonlandırılması veya Değiştirilmesi	Mülakat, Gözden Geçirme	Personel ve yüklenici sözleşmelerinde, istihdamın sona ermesinden sonra da geçerli olacak hükümlere yer verilmiş midir? İstihdamın sonlandırılmasından sonra veya istihdam koşullarının değiştirilmesinden sonra ilgili personele/yükleniciye, uymaları gereken bilgi güvenliği sorumlulukları nasıl bildirilmektedir?
3.5.1.9	Gizlilik ile İlgili Gereksinimlerin Personele Tebliğ Edilmesi	Mülakat, Gözden Geçirme	Personel veya yüklenicilerin uyması gereken bilgi güvenliği politikaları, prosedürleri, talimatları tanımlanarak tebliğ edilmiş midir? İlgili dokümanlar kurumun bilgi güvenliği gereksinimlerini karşılamakta mıdır? Bilgi güvenliği gereksinimlerinde herhangi bir değişiklik olması durumunda dokümanlar güncellenmekte midir?

3.5.2. Eğitim ve Farkındalık Faaliyetleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.5.2.1	1	Farkındalık Eğitimleri Verilmesi	Tüm kurum personeline düzenli aralıklarla; • Bilgi güvenliği ve siber güvenlik temel kavramları, • Kurumsal bilgi güvenliği ve siber güvenlik politikaları, • Parola güvenliği, • E-posta kullanımında güvenlik, • İnternet kullanımında güvenlik, • Mobil güvenlik, • Fiziksel güvenlik, • Sosyal ağların riskleri ve güvenli kullanımı, • Kişisel verilerin güvenliği, • Bilinen ve yaygın kullanılan sosyal mühendislik yöntemleri ve bu yöntemlere karşı alınacak önlemler, • Lisanslı ürün kullanımı gibi temel ve güncel konuları içerecek şekilde bilgi güvenliği ve siber güvenlik farkındalık eğitimleri verilmelidir. Farkındalık eğitimlerinin etkinliğine yönelik ölçümler (eğitim öncesi ve sonrası yazılı sınav, sosyal mühendislik saldırıları vb.) yapılmalı ve ölçüm sonucu doğrultusunda aksiyonlar planlanmalıdır.
3.5.2.2	1	Olayların Tespiti ve Raporlanmasına Yönelik Eğitimlerin Verilmesi	Bilgi güvenliği ve SOME personeline, siber olay veya bilgi güvenliği ihlal olayı tespiti ve raporlanması konularında eğitim verilmelidir.
3.5.2.3	2	Yetenek İhtiyaç Analizi Yapılması	Bilgi güvenliği ve siber güvenlik alanında görev yapan personel için yetenek ihtiyaç analizi yapılmalıdır. Yetenek ihtiyaç analizi çıktıları doğrultusunda eğitim yol haritası çıkarılmalı ve uygulamaya alınmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.5.2.1	Farkındalık Eğitimleri Verilmesi	Mülakat, Gözden Geçirme	Kurum personeline bilgi güvenliği ve siber güvenlik farkındalık eğitimleri verilmekte midir? Eğitim içeriğinde hangi konular ele alınmaktadır? Eğitim içerikleri periyodik olarak güncellenmekte midir? Eğitimin etkinliği nasıl değerlendirilmektedir?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.5.2.2	Olayların Tespiti ve Raporlanmasına Yönelik Eğitimlerin Verilmesi	Mülakat	Bilgi güvenliği ve SOME personeline, siber olay veya bilgi güvenliği ihlal olayı tespiti ve raporlamasının nasıl yapılacağına yönelik eğitim verilmekte midir? Verilen eğitimlerde hangi konular ele alınmaktadır?
3.5.2.3	Yetenek İhtiyaç Analizi Yapılması	Mülakat, Gözden Geçirme	Bilgi güvenliği ve siber güvenlik alanında görev yapan personele yönelik yetenek ihtiyaç analizleri yapılmakta mıdır? Analiz sonuçları göz önünde bulundurularak personel için eğitim yol haritası hazırlanmakta mıdır? Eğitim yol haritası doğrultusunda kurum çalışanlarına düzenli olarak eğitimler verilmekte midir?

3.5.3. Tedarikçi İlişkileri Güvenliği

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.5.3.1	1	Tedarikçi İlişkilerinde Bilgi Güvenliği Politikasının Tanımlanması	Tedarikçiler tarafından erişilen kurum varlıklarının korunmasını sağlamak, tedarikçilerin kurumun bilgi varlıklarına erişimi ile ilgili riskleri azaltmak ve bilgi güvenliği gereksinimlerini karşılamak amacıyla politika tanımlanmalı ve uygulanmalıdır.
3.5.3.2	1	Demo ve Kavram İspatı Çalışmalarında Gizlilik Taahhütnamesi	Kurumun bilgi güvenliği gereksinimleri göz önünde bulundurularak üçüncü taraflar ile yapılan demo ve kavram ispatı (PoC) çalışmalarında, üçüncü tarafın sorumluluklarını içeren gizlilik taahhütnamesi hazırlanmalı ve imza altına alınmalıdır. İlgili taahhütname içeriği periyodik olarak gözden geçirilmelidir.
3.5.3.3	1	Tedarikçi Sözleşmelerinde Bilgi Güvenliğinin Ele Alınması	Kurum varlıklarına erişebilen, işletebilen, depolayabilen, iletebilen veya kurumun bilgi teknolojileri altyapı bileşenlerini temin eden tedarikçilerin her biri ile yapılacak sözleşmelere bilgi güvenliği gereksinimleri eklenmelidir.
3.5.3.4	1	Tedarik Zinciri Güvenliği	Yükleniciler ile yapılan sözleşmelerde, tedarik edilen bilgi ve iletişim teknolojileri ürün ve hizmetleri için tedarik zinciri ile ilişkili riskler göz önünde bulundurulmalı ve ilgili güvenlik gereksinimleri sözleşme içeriklerine eklenmelidir. Bu kapsamda, birlikte çalışılacak kişi ve/veya kuruluşlardan tedarik zinciri güvenliğinin temin edileceğine dair yazılı belge alınmalıdır.
3.5.3.5	1	Kabul Kriterlerinin Belirlenmesi	Tedarik edilen ürünün istenilen güvenlik kriterleri dâhilinde teslim edilmiş olduğunun doğrulanabilmesi için kabul kriterleri belirlenmeli, izleme ve doğrulama metotları tanımlanmalı ve yüklenici ile üzerinde anlaşılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.5.3.6	1	İletişim Metotlarının Belirlenmesi	Garanti süreci dâhil tedarik sürecinin tamamında bilgilendirme amaçlı ya da olası herhangi bir anormal durum ile ilgili olarak kimler ile nasıl iletişime geçileceği, hangi kuralların geçerli olacağı tanımlanmalı ve yüklenici ile üzerinde anlaşılmalıdır.
3.5.3.7	1	Yüklenici Tarafından Tedarik Edilen Ürün/Hizmet Değişikliklerinin Yönetimi	Yüklenici tarafından sağlanan hizmet ve ürün tedariki kapsamında bir değişiklik olması durumu göz önünde bulundurularak hizmet alınan faaliyetin kritikliği ve riskleri gözden geçirilmelidir. Bu değerlendirme hesaba katılarak, yüklenici ile yapılan sözleşmeye gereklilikler yansıtılmalı, bu gibi değişiklik durumlarının nasıl ele alınacağı net bir şekilde tanımlanmalıdır.
3.5.3.8	1	Ana Yüklenici ve Alt Yüklenici Sorumluluklarının Netleştirilmesi	Ana yüklenicinin, tedarik edilen ürün ve hizmetleri sunabilmek için tedarik süresince bir alt yüklenici kullanması durumunda; ana yüklenici ile alt yüklenici rol ve sorumluluklarının dokümante edildiği, bilgi güvenliği gereksinimlerine tedarik sürecinin tamamında alt yüklenici tarafından da uyulacağının taahhüdü ana yükleniciden alınmalıdır.
3.5.3.9	1	Tedarikçi Hizmetlerinin İzlenmesi	Bilgi güvenliği şartlarının sağlandığını garanti altına almak amacıyla tedarikçi hizmetleri düzenli aralıklarla gözden geçirilmeli ve dokümante edilmelidir.
3.5.3.10	2	Tedarik Zinciri İzleme Sürecinin Oluşturulması	Yüklenici tarafından güvenlik gereksinimlerine uyumun garanti altına alınması amacıyla; tedarik zinciri süresince, tedarik edilen hizmet/ürüne yönelik kritik bileşenlerin durumunun izlenebilirliği sağlanmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.5.3.1	Tedarikçi İlişkilerinde Bilgi Güvenliği Politikasının Tanımlanması	Mülakat, Gözden Geçirme	Tedarikçi ilişkilerinde bilgi güvenliği gereksinimlerini karşılamak amacıyla bir politika tanımlanmış mıdır? Bilgi güvenliği politikası hangi hususları içermektedir?
3.5.3.2	Demo ve Kavram İspatı Çalışmalarında Gizlilik Taahhütnamesi	Mülakat, Gözden Geçirme	Üçüncü taraflar ile yapılan demo ve kavram ispatı (PoC) çalışmalarında, üçüncü taraflara gizlilik taahhütnamesi imzalatılmakta mıdır? Taahhütname kurumun bilgi güvenliği gereksinimlerine uygun olarak hazırlanmış mıdır?
3.5.3.3	Tedarikçi Sözleşmelerinde Bilgi Güvenliğinin Ele Alınması	Mülakat, Gözden Geçirme	Tedarikçiler ile yapılan sözleşmelere bilgi güvenliği gereksinimleri eklenmiş midir? Sözleşmelerde yer alan bilgi güvenliği gereksinimleri hangi hususları içermektedir?
3.5.3.4	Tedarik Zinciri Güvenliği	Mülakat, Gözden Geçirme	Yükleniciler ile yapılan sözleşmelerde, tedarik zinciri güvenliğine yönelik maddeler yer almakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.5.3.5	Kabul Kriterlerinin Belirlenmesi	Mülakat, Gözden Geçirme	Tedarik edilecek ürüne yönelik kabul kriterleri belirlenmekte midir? Tedarik edilen ürünün istenilen güvenlik kriterleri ile uyumlu şekilde teslim edilmiş olduğunun doğrulanabilmesi için nasıl bir yöntem izlenmektedir?
3.5.3.6	İletişim Metotlarının Belirlenmesi	Mülakat, Gözden Geçirme	Garanti süreci dâhil tedarik sürecinin tamamında olası herhangi bir anormal durum ile ilgili nasıl iletişime geçileceği ve hangi kuralların geçerli olacağı tanımlanmakta mıdır?
3.5.3.7	Yüklenici Tarafından Tedarik Edilen Ürün/Hizmet Değişikliklerinin Yönetimi	Mülakat, Gözden Geçirme	Yüklenici tarafından sağlanan hizmet ve ürün tedarik süreci kapsamında yaşanan değişikliklerin yönetimi nasıl yapılmaktadır? Yüklenici ile yapılan sözleşmelerde ürün/hizmet değişikliklerinin yönetimine ilişkin gereklilikler yer almakta mıdır?
3.5.3.8	Ana Yüklenici ve Alt Yüklenici Sorumluluklarının Netleştirilmesi	Mülakat, Gözden Geçirme	Ana yüklenicinin, tedarik süresince alt yüklenici kullanması durumunda; ilgili tüm tarafların rol ve sorumluluklarının tanımlandığı, alt yüklenici tarafından bilgi güvenliği gerekliliklerinin yerine getirileceğini garanti altına alan taahhüt ana yükleniciden alınmakta mıdır?
3.5.3.9	Tedarikçi Hizmetlerinin İzlenmesi	Mülakat, Gözden Geçirme	Bilgi güvenliği şartlarının sağlandığını garanti altına almak amacıyla tedarikçi hizmetleri düzenli aralıklarla gözden geçirilmekte midir?
3.5.3.10	Tedarik Zinciri İzleme Sürecinin Oluşturulması	Mülakat, Gözden Geçirme	Tedarik zinciri süresince, tedarik edilen hizmet/ürüne yönelik kritik bileşenlerin durumu izlenebilmekte midir?

3.6. Fiziksel Mekânların Güvenliği

Amaç

Bu güvenlik tedbiri ana başlığının amacı, fiziksel mekânların güvenliği çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. “Fiziksel Mekânların Güvenliği” ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Genel Güvenlik Tedbirleri
- Sistem Odası/Veri Merkezine Yönelik Güvenlik Tedbirleri
- Elektromanyetik Bilgi Kaçaklarından Korunma Yöntemleri (TEMPEST)

3.6.1. Genel Güvenlik Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.6.1.1	1	Fiziksel Güvenlik Sınırı	Kritik bilgi ve bilgi işleme olanakları barındıran alanları korumak için güvenlik sınırları tanımlanmalıdır. Kurum tesislerine girişte ve çıkışta, güvenlik biriminin yer aldığı güvenlik kontrol noktası olmalı ve kuruma fiziksel erişimler yalnızca yetkilendirilmiş personel ile sınırlandırılmalıdır.
3.6.1.2	1	Güvenlik Biriminin Yeterliliği	Tesisin büyüklüğü, bulunduğu coğrafi alan ve var olan izleme sistemleri ile orantılı düzeyde ve bilgi seviyesinde güvenlik personeli bulundurulmalıdır. Güvenlik personelinin görevini tam olarak yerine getirip getirmediği düzenli olarak kontrol edilmelidir.
3.6.1.3	1	Fiziksel Giriş ve Çıkış Kontrolleri	Personelin fiziksel erişimini iş gereksinimleri doğrultusunda sınırlayan, tüm giriş/çıkışları kayıt altına alan kimlik kontrol mekanizması olmalıdır. Personel ve araç giriş kontrolü, güvenlik birimi tarafından yapılmalı ve kuruma giriş/çıkış noktaları sınırlı olmalıdır. Yetkisiz kişilerin tesise giriş yapabileceği; otopark girişleri, teslimat ve yükleme alanları gibi erişim noktaları ve olası diğer noktalar kontrol edilmeli, mümkünse yetkisiz erişimi engellemek için bilgi işleme olanaklarının bulunduğu alanlardan ayrılmalıdır.
3.6.1.4	1	Dış Güvenlik Unsurlarının Kontrolü	Tüm dış güvenlik unsurları (Ör. demir parmaklık, tel örgü, duvarlar, kamera sistemi, alarm sistemi vb.) düzenli olarak sabotaj, hasar veya bozulmalara karşı kontrol edilmelidir. Binalara ait bütün pencereler, kapılar, dış duvarlar ve güvenlik altına alınması gereken yerler yeterli gözetleme ve kontrol tedbirleri ile takip edilmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.6.1.5	1	Ziyaretçi Giriş Çıkış Kontrolleri	Ziyaretçilerin fiziksel erişimini iş gereksinimleri doğrultusunda sınırlayan, giriş ve çıkışlarını kayıt altına alan kimlik kontrol mekanizması olmalıdır. En az aşağıda yer alan ziyaretçi karşılama tedbirleri uygulanmalıdır: • Kuruma gelen ziyaretçilere yönelik kayıtlar; ad, soyad, geliş amacı ve tarihi, refakat eden kişi bilgisi, giriş ve çıkış saati bilgilerini içermek üzere tutulmalıdır. • Ziyaretçi tarafından sunulan resmi kimlik kartlarının güvenlik birimi tarafından teyit edilmesi sonrasında ziyaretçi erişimi için giriş kartı verilmelidir. • Ziyaretçilerin verilen giriş kartını tesis içerisinde bulunduğu süre boyunca üzerinde görünür biçimde taşıması sağlanmalıdır. • Ziyaretçilerin tesis içerisinde refakatçi personel olmadan dolaşmasına izin verilmemelidir. • Ziyaretçi taşıtlarının tesislere giriş ve çıkışı izlenmelidir.
3.6.1.6	1	Yetkisiz Fiziksel Erişim Durumunda İzlenecek Sürecin Tanımlanması	Tesislere yetkisiz girdiğinden şüphelenilen kişi ve araçların tespiti, ihbarı ve gerekli müdahalenin gerçekleştirilmesi için yöntemler, rol ve sorumluluklar tanımlanmalıdır. Bu kapsamda; • Şüpheli durumların nasıl bildirileceği tanımlanmalıdır. (Kurum içi bir telefon numarası veya telsiz kanalının tahsis edilmesi ve bunun tesislerde görülebilecek yerlerde duyurulması vb.), • Bu tip durumlara müdahalenin kim tarafından ve nasıl yapılacağı belirlenmelidir.
3.6.1.7	1	Kablolama Güvenliği	Tüm kablolar yapısal kablo kanallarından geçirilmelidir. Karışmayı engellemek için güç kabloları, haberleşme kablolarından mümkün mertebe ayrılmalıdır. Kablolara yetkisiz aygıtların eklenmesine (fiziksel olarak araya girme saldırılarına karşı) izin verilmemelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.6.1.8	1	Dış ve Çevresel Tehditlere Karşı Koruma	Kurumun faaliyet gösterdiği binalar için depreme karşı dayanıklılık testi yapılmış olmalı ve bu durum belgelendirilmelidir. Kurumun faaliyet gösterdiği binalarda yangın söndürme sistemi olanakları ve acil durumda aranacaklar listesi bulunmalıdır. Acil durumda aranacaklar listesi periyodik olarak gözden geçirilmeli ve herkes tarafından görülebilecek uygun yerlerde asılı olmalıdır. Periyodik yangın ve deprem tatbikatları yapılmalı ve tatbikat sonuçları kayıt altına alınmalıdır. Su baskını ve yangın ihtimalini azaltmak için mutfak ve tuvaletlerin kritik bilgi bulunan yerlere uzak olmasına dikkat edilmelidir. Yangın, su baskını, duman tespiti için dedektörler konumlandırılmalı ve merkezi bir uyarı sistemiyle 7/24 gözlenmelidir. Periyodik olarak binanın topraklama kontrolleri yapılmalı ve kayıt altına alınmalıdır. Bina için yeterli koruma seviyesine sahip bir paratoner kullanılmalı, paratonerin bakımları periyodik olarak yapılmalı ve bakım sonuçları kayıt altına alınmalıdır. Elektrik, su, gaz ve diğer destekleyici altyapı hizmetlerini kesmek için kullanılan acil durum anahtarları ve vanalar acil çıkışların veya ekipman odalarının yakınında konumlandırılmalıdır.
3.6.1.9	1	Kamera Sistemleri	Kurum binasına giriş noktaları, bina içindeki koridorlar, bina çevresi, sistem odası, veri merkezi, kontrollü erişim noktaları ve güvenli alanlar kapalı devre kamera sistemi tarafından izlenip kayıt altına alınmalıdır. Kameralarla izlenmeyen noktalar tespit edilmeli ve periyodik olarak kontrolü sağlanmalıdır. Kamera kayıtlarına yalnızca yetkili personel erişmeli ve bu kayıtlar ilgili sistem odası/veri merkezi haricinde güvenli bir ortamda saklanmalıdır. Kamera kayıtları bilgi güvenliği gereklilikleri göz önünde bulundurularak belirlenmiş süre kadar muhafaza edilmelidir. Kamera sistemleri, dış ağlara açık olmamalıdır.
3.6.1.10	2	Çalışma Alanlarının Güvenliği	Binalarda ziyaretçilerin kabul edileceği lobi ve toplantı odaları, personelin çalışma alanlarından ayrı bir bölgede olmalıdır. İki bölge arasındaki geçiş kontrollü olarak sağlanmalıdır. Kritik veri, doküman ve belgelerin bulunduğu ve/veya görüşmelerin gerçekleştirildiği çalışma odalarında/ortamlarında mobil cihazlar ve veri transferi özelliğine sahip cihazlar bulundurulmamalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.6.1.11	2	Destekleyici Altyapı Hizmetleri	Çalışma alanlarına gelen elektrik enerji hattı yedekli olmalıdır. Jeneratör ve UPS sistemleri bulunmalı, yedekliliği sağlanmalı ve düzenli bakımı (akülerin kontrolü, yeterli mazot bulundurma vb.) yapılmalıdır. Jeneratör ve UPS bakımı, onarımı ve testi için yapılan tüm işlemler kayıt altına alınmalıdır.
3.6.1.12	3	Fiziksel Güvenlik Sistemleri Verilerinin Siber Olay Tespitinde Kullanılması	Kurumda yaşanabilecek siber olayların tespitine girdi sağlamak amacı ile fiziksel güvenlik sistemlerinin desteklemesi durumunda alarm, hata mesajları vb. kayıtlar siber olay tespit sistemlerine iletilmelidir. Bk. Tedbir No: 3.6.2.13
3.6.1.13	3	Ziyaretçi Fiziksel Erişim Güvenliği	Ziyaretçi giriş ve çıkışı refakatçi ile sağlanmalıdır. Ziyaretçi giriş kartı yalnızca ilgili alanlara erişim sağlayacak şekilde tanımlanmalıdır. Ziyaretçilerin tesis içerisinde refakatçi personel olmadan dolaşmasına izin verilmemelidir. Ziyaretçilerin giriş ve çıkışlarda üstleri ve eşyaları uygun yöntemlerle (elle arama, x-ray vb.) aranmalıdır. Ziyaretçilerin bilgisayar, cep telefonu, akıllı saat vb. elektronik cihazları istisnai izne tabi olmalıdır. Bu cihazların kurum içerisine alınmasına izin verilmeden önce, güvenlik birimi tarafından kuruma girişi yapılacak cihazın seri numarası, marka, modeli ve hangi amaçla kullanılacağı bilgileri kayıt altına alınmalıdır.
3.6.1.14	3	Fiziksel Erişim Güvenliği	Personelin hangi bölgelere erişebileceği konusunda bir tanımlama yapılmalıdır. Emniyet ve güvenlik açısından önem taşıyan yerlere girişte güvenlik birimine ek güvenlik önlemlerinin olması (kartlı giriş sistemi, biyometrik veriler ile kimlik doğrulama sistemi vb.) sağlanmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.6.1.1	Fiziksel Güvenlik Sınırı	Mülakat, Gözden Geçirme	Kritik bilgi ve bilgi işleme olanakları barındıran alanları korumak için güvenlik sınırları tanımlanmış mıdır? Bu alanlara giriş ve çıkış noktalarında güvenlik kontrol mekanizması bulunmakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.6.1.2	Güvenlik Biriminin Yeterliliği	Mülakat, Gözden Geçirme	Tesis içerisinde güvenlik kontrollerini sağlayabilecek yetkinlikte ve yeterli sayıda güvenlik personeli görevlendirilmekte midir? Güvenlik birimi tarafından gerçekleştirilen işlemler periyodik olarak denetlenmekte midir? Güvenlik biriminde çalışan personel, bilgi güvenliği farkındalık eğitimlerine katılım sağlamakta mıdır?
3.6.1.3	Fiziksel Giriş ve Çıkış Kontrolleri	Mülakat, Gözden Geçirme	Kuruma fiziksel giriş/çıkış işlemlerinin güvenliği sağlamak için hangi tedbirler alınmaktadır? Kargo ve kurye gibi özel teslimat hizmeti veren tarafların kuruma giriş yetkileri var mıdır? Kargo ve kuryelerin kuruma giriş/çıkış faaliyetleri nasıl gerçekleştirilmektedir? Kurumda dağıtım ve yükleme ile ilgili belirlenmiş özel alanlar var mıdır? Bu alanlara girişler ve bu alanların kullanımı ile ilgili kontroller nasıl yapılmaktadır?
3.6.1.4	Dış Güvenlik Unsurlarının Kontrolü	Mülakat, Gözden Geçirme	Binalara ait bütün pencereler, kapılar, dış duvarlar ve güvenlik altına alınması gereken yerler gözetleme veya diğer güvenlik kontrolleri ile takip edilmekte midir?
3.6.1.5	Ziyaretçi Giriş Çıkış Kontrolleri	Mülakat, Gözden Geçirme	Binaya girişte ziyaretçi bilgileri kayıt altına alınmakta mıdır? İlgili kayıtlar ne kadar süre saklanmaktadır? Bu kayıtlara kimlerin erişim yetkisi bulunmaktadır? Bina içerisindeki ziyaretçi hareketleri nasıl takip edilmektedir? Otoparktan girişler nasıl kontrol edilmektedir? Binaya giriş yapan kişilerin üzerinde ve araçlarında herhangi bir sakıncalı, şüpheli, yanıcı ve patlayıcı madde bulunup bulunmadığı yönünde tarama yapılmakta mıdır? Bina girişi, otopark girişi gibi alanlarda güvenliği sağlamaya yönelik hangi kontroller alınmaktadır?
3.6.1.6	Yetkisiz Fiziksel Erişim Durumunda İzlenecek Sürecin Tanımlanması	Mülakat, Gözden Geçirme	Yetkisiz giriş tespit edildiğinde izlenecek adımlar, bildirim yapılacak kişiler ve bu tip durumlarda müdahalenin kim tarafından gerçekleştirileceği tanımlanmış ve kurum içerisinde duyurulmuş mudur?
3.6.1.7	Kablolama Güvenliği	Mülakat, Gözden Geçirme	Kablolama güvenliğini sağlamak için hangi kontroller uygulanmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.6.1.8	Dış ve Çevresel Tehditlere Karşı Koruma	Mülakat, Gözden Geçirme	Bina çevresinde güvenliği tehdit edebilecek yerler (petrol istasyonu, yüksek voltaj elektrik dağıtım hatları, sıkıştırılmış gaz istasyonları vb.) bulunmakta mıdır? Yangın, sel, deprem, saldırı vb. felaket durumlarında kurum personeli tarafından yapılması gerekenler tanımlanmış mıdır? Acil durumlarda aranacaklar listesi oluşturulmuş mudur, oluşturulan liste güncel midir? Liste herkes tarafından görünür bir şekilde tutulmakta mıdır? Paratoner ve topraklama ile ilgili periyodik kontroller yapılmakta mıdır? Yapılan kontroller kayıt altına alınmakta mıdır?
3.6.1.9	Kamera Sistemleri	Mülakat, Gözden Geçirme	Kapalı devre kamera sistemi tesis edilmiş midir? Kameralarla izlenmeyen noktalar tespit edilmekte ve periyodik olarak kontrolü sağlanmakta mıdır? Kamera sistemi tarafından hangi alanlar izlenmektedir? Kamera kayıtları ne kadar süre tutulmaktadır? Kamera kayıtları nerede muhafaza edilmektedir? Kamera kayıtlarına kimler erişim sağlamaktadır?
3.6.1.10	Çalışma Alanlarının Güvenliği	Mülakat, Gözden Geçirme	Binalarda ziyaretçilerin kabul edileceği lobi ve toplantı odaları, personelin çalışma alanlarından ayrı ve fiziksel erişimin kontrollü olduğu bir bölgede midir? Kritik veri, doküman ve belgelerin bulunduğu ve/veya görüşmelerin gerçekleştirildiği çalışma odalarında/ortamlarında; mobil cihazlar ve veri transferi özelliğine sahip cihazların olup olmadığına yönelik kontrol yapılmakta mıdır?
3.6.1.11	Destekleyici Altyapı Hizmetleri	Mülakat, Gözden Geçirme	Periyodik bakım listesinde hangi teçhizatlar bulunmaktadır? Bakım kayıtları tutulmakta mıdır?
3.6.1.12	Fiziksel Güvenlik Sistemleri Verilerinin Siber Olay Tespitinde Kullanılması	Mülakat, Güvenlik Denetimi	Fiziksel güvenlik sistemlerinin hangi kayıtları siber olay tespit sistemlerine aktarılmaktadır? Aktarılan kayıtlar aracılığıyla hangi senaryoların tespiti sağlanmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.6.1.13	Ziyaretçi Fiziksel Erişim Güvenliği	Mülakat, Gözden Geçirme	Kurum bünyesinde işletilen bir ziyaretçi kabul prosedürü bulunmakta mıdır? Ziyaretçilerin kuruma giriş ve çıkışları refakatçi eşliğinde sağlanmakta mıdır? Ziyaretçiler giriş ve çıkışlarda uygun yöntemlerle aranmakta mıdır? Ziyaretçilerin bilgisayar, cep telefonu, akıllı saat vb. elektronik cihazları kurum içerisine alınmadan önce yetkili kişilerden izin alınmakta mıdır? Kurum içerisine alınacak cihazların hangi bilgileri kayıt altına alınmaktadır?
3.6.1.14	Fiziksel Erişim Güvenliği	Mülakat, Gözden Geçirme	Personelin hangi bölgelere erişebileceği konusunda bir tanımlama yapılmış mıdır? Fiziksel erişim yetkileri hangi zaman aralıklarında, nasıl kontrol edilmektedir? Emniyet ve güvenlik açısından önem taşıyan yerlere girişte yeterli seviyede güvenlik kontrolleri uygulanmakta mıdır?

3.6.2. Sistem Odası/Veri Merkezine Yönelik Güvenlik Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.6.2.1	1	Sistem Odası/Veri Merkezi Güvenliği Politikası	Güvenli çalışma alanları oluşturmak amacıyla sistem odası/veri merkezi güvenliği politikası oluşturulmalı ve periyodik olarak gözden geçirilmelidir.
3.6.2.2	1	Fiziksel Varlıkların Sistem Odası/Veri Merkezi Dışına Transferi	Sistem odası/veri merkezinde bulunan varlıkların sistem odası/veri merkezi dışına transferi durumunda, bilgi güvenliği gereksinimleri çerçevesinde gerekli onay ve yetkilendirme işlemleri tamamlanmalıdır.
3.6.2.3	1	Güvenli Alan Yetkilendirmesinin Yapılması	Bilgi güvenliği kontrollerinin yeterli seviyede sağlanmasının büyük öneme sahip olduğu, kilitlenmiş bir büro veya içinde birçok oda bulunan alan, içinde kilitlenebilir dolaplar veya korumalar içeren fiziki bir güvenlik çevresi olarak tanımlanan güvenli alanlarda çalışma için yetkilendirme ve izleme prosedürleri oluşturulmalı, erişim kontrol mekanizmaları devreye alınmalıdır. Güvenli alanlara erişim yetkileri düzenli olarak gözden geçirilmelidir.
3.6.2.4	1	Üçüncü Taraf Hizmetlerin Güvenliği	Güvenli alanlara veya kritik bilgi işleme ortamlarına; destek, bakım gibi hizmetler için gelen üçüncü taraf personeline, yetkili kurum personeli nezaretinde sınırlandırılmış şekilde erişim izni verilmelidir. Ziyaretçilere yönelik; ad, soyad, geliş amacı ve tarihi, refakat eden personel, giriş/çıkış saat bilgilerini içeren kayıt tutulmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.6.2.5	1	Ortam Koşullarının Kontrolü	Sistem odası/veri merkezinde; su, elektrik, nem, sıcaklık ve duman kontrolünü düzenli olarak yapacak sistemler devreye alınmalıdır. Bu sistemlerin normal ve eşik değerleri belirlenmeli, bu eşik değerlerin aşılması durumunda ilgili personele uyarı mesajlarının gönderileceği bir alarm mekanizması kurulmalıdır. Ortam izleme sistemleri uzaktan izleme ve denetim amacıyla dışarıya açık olarak kurulmamalıdır.
3.6.2.6	1	Kamera Sistemleri	Bk. Tedbir No: 3.6.1.9
3.6.2.7	1	Destekleyici Altyapı Hizmetleri	Sistem odası/veri merkezine gelen elektrik enerji hattı yedekli olmalıdır. Elektrik kesintilerinde jeneratör devreye girinceye kadar sistem odası beslemesi UPS tarafından sağlanmalı ve bu UPS sistemine başka cihazlar bağlanmamalıdır. UPS'lerin periyodik bakım, ölçüm ve test işlemleri gerçekleştirilmeli ve kayıt altına alınmalıdır. Jeneratör(lerin) periyodik bakım, ölçüm ve test işlemleri gerçekleştirilmeli ve kayıt altına alınmalıdır. Jeneratör yakıt deposu her zaman dolu ve yedekli olmalıdır. Belli periyotlarda ve uzun süreli jeneratör kullanımlarında düzenli olarak jeneratör yakıt durumu kontrol edilerek kayıt altına alınmalıdır. Sistem odası/veri merkezi destekleyici servisler arasında yer alan UPS, jeneratör, klima vb. olanakların bakımları üreticileri tarafından tavsiye edilen aralıklarda konusunda yetkin uzmanlar tarafından yapılmalı ve ilgili tüm işlemler kayıt altına alınmalıdır. Veri merkezi topraklama ölçümleri periyodik olarak yapılmalı ve sonuçlar kayıt altına alınmalıdır.
3.6.2.8	1	Dış ve Çevresel Tehditlere Karşı Koruma	Sistem odası/veri merkezi duvarları ve zemini neme ve aleve dayanıklı yalıtım malzemeleri ile kapatılmalıdır. Sistem odası/veri merkezi; ısı, nem ve hava yalıtımı için oda içerisinde açıklık kalmayacak şekilde kapatılmalıdır. Sistem odası/veri merkezi; yemekhane, su, havalandırma, atık su gideri, sulu yangın söndürme, havalandırma kanalları ve üniteleri, doğal gaz ve yanıcı bileşenlerin depolandığı yerler gibi risk teşkil edecek noktalardan mümkün olabildiğince uzakta konumlandırılmalıdır. Sistem odası/veri merkezinin depreme karşı dayanıklılık testi yapılmış olmalı ve bu durum belgelendirilmelidir. Veri merkezi yerleşkesinde, gerekli yıldırım koruma tertibatı sağlanmalıdır. Sistem odası/ veri merkezinde yanıcı, yakıcı, parlayıcı ve toz oluşturan maddeler bulundurulmamalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.6.2.9	1	Donanım Bakımı ve Güvenliği	Bilgisayar, iletişim cihazları ve veri depolama donanımları kullanım veya depolama amacıyla yerleştirilirken; donanım üreticisinin belirttiği teknik standartlara uygun ortamlar sağlanmalıdır. Donanım bakımları üreticileri tarafından tavsiye edilen aralıklarda konusunda yetkin uzmanlar tarafından yapılmalı ve ilgili tüm işlemler kayıt altına alınmalıdır.
3.6.2.10	1	Kablolama Güvenliği	Kablolama düzgün ve kolay ayırt edilecek şekilde yapılmalı, bütün kablolar tek tek etiketlenmeli ve kayıt altına alınmalıdır. Sistem/veri merkezi odasında yer alan kablolar ayrı kablo kanalları içerisinden geçirilmelidir.
3.6.2.11	1	Fiziksel Giriş Kontrolleri	Sistem odası/veri merkezine giriş ve çıkış işlemlerinde kimlik doğrulama mekanizmaları kullanılmalıdır. Sistem/veri merkezine gerçekleştirilen giriş/çıkışlar kayıt altına alınmalıdır.
3.6.2.12	2	Ortam Koşullarının Gerçek Zamanlı İzlenmesi	Sistem odası/veri merkezindeki su, nem, sıcaklık ve duman kontrolü için üretilen veri gerçek zamanlı izlenebilmeli, merkezi izleme sistemlerine güvenli bir protokolle aktarılabilmelidir.
3.6.2.13	2	Siber Olay Tespitinde İz Kayıtlarının Kullanılması	Siber olay tespitinde; gerekli olması durumunda, sistem odası/veri merkezi fiziksel güvenlik ve ortam kontrolü yapılarına ait iz kayıtları, girdi olarak kullanılabilmelidir.
3.6.2.14	3	Kontrollü Erişim Noktalarının Oluşturulması	Kritik veriyi ve bilgi sistemlerini korumak adına kontrollü erişim noktaları tanımlanmalı, yetkisiz erişimi engelleyecek önlemler alınmalıdır.
3.6.2.15	3	İklimlendirme Kontrolü	Sistem odası/veri merkezinde yedekli olacak şekilde hassas kontrollü klima bulunmalıdır. Klimalardan bir tanesi bekleme konumunda çalışmalı ve diğer klima herhangi bir sebepten devre dışı kaldığında ya da gerekli soğutmayı yapamadığında bekleme konumundaki klima otomatik olarak devreye girmelidir. Hassas kontrollü klimalar sistem odası/veri merkezi kapasitesine uygun olarak seçilmeli, tam otomatik elektronik kontrollü olmalıdır. Arızalara yönelik alarm üretebilmeli, enerjinin herhangi bir anda kesilip gelmesiyle otomatik olarak devreye girebilmelidir. Klimaların periyodik bakım, ölçüm ve test işlemleri gerçekleştirilmeli ve kayıt altına alınmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.6.2.1	Sistem Odası/Veri Merkezi Güvenliği Politikası	Mülakat, Gözden Geçirme	Sistem odası/veri merkezi güvenliği politikası hazırlanmış mıdır? Sistem odası/veri merkezi güvenliği politikası ne kadar sürede bir gözden geçirilmektedir? Sistem odası/veri merkezi güvenliği politikasının ihlali durumunda nasıl bir yöntem izlenmektedir?
3.6.2.2	Fiziksel Varlıkların Sistem Odası/Veri Merkezi Dışına Transferi	Mülakat, Gözden Geçirme	Sistem odası/veri merkezinde yer alan varlıkların sistem odası/veri merkezi dışına transferi durumunda gerekli onay ve yetkilendirme işlemi yapılmakta mıdır? Sistem odası/veri merkezi dışına transfer edilen varlıklara ait kayıt bulunmakta mıdır?
3.6.2.3	Güvenli Alan Yetkilendirmesinin Yapılması	Mülakat, Gözden Geçirme	Güvenli alanlar nasıl belirlenmektedir? Güvenli alanlar için yetkilendirme mekanizması nasıl işletilmektedir? Güvenli alanlara giriş yetkisi olan personel yetkileri periyodik olarak gözden geçirilmekte midir?
3.6.2.4	Üçüncü Taraf Hizmetlerin Güvenliği	Mülakat, Gözden Geçirme	Destek, bakım gibi hizmetler için gelen üçüncü taraf personeline refakat edilmekte midir? Üçüncü taraf personeli tarafından yapılan işlemler kayıt altına alınmakta mıdır?
3.6.2.5	Ortam Koşullarının Kontrolü	Mülakat, Gözden Geçirme	Sistem odası/veri merkezi nem, sıcaklık ve duman kontrolü nasıl yapılmaktadır? Merkezi izleme sistemi kullanılmakta mıdır?
3.6.2.6	Kamera Sistemleri	Mülakat, Gözden Geçirme	Bk. Denetim No: 3.6.1.9
3.6.2.7	Destekleyici Altyapı Hizmetleri	Mülakat, Gözden Geçirme	Periyodik bakım listesinde hangi teçhizatlar bulunmaktadır? Teçhizat bakımlarına yönelik yapılan işlemler ve sonuçları kayıt altına alınmakta mıdır? Topraklama ölçümleri ne kadar sıklıkta bir yaptırılmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.6.2.8	Dış ve Çevresel Tehditlere Karşı Koruma	Mülakat, Gözden Geçirme	Sistem odası/veri merkezi duvarları neme ve aleve dayanıklı malzeme ile kaplanmış mıdır? Sistem odası/veri merkezi; ısı, nem ve hava yalıtımı için oda içerisinde açıklık kalmayacak şekilde yapılandırılmış mıdır? Sistem odası/veri merkezi yerleşimi yapılırken hangi konular dikkate alınmıştır? Veri merkezi çevresinde güvenliği tehdit edebilecek alanlar bulunmakta mıdır? Veri merkezi yerleşkesinde, gerekli yıldırım koruma tertibatı sağlanmakta mıdır?
3.6.2.9	Donanım Bakımı ve Güvenliği	Mülakat, Gözden Geçirme	Bilgisayar, iletişim cihazları ve veri depolama donanımları, kullanım veya depolama amacıyla yerleştirilirken; donanım üreticisinin belirttiği teknik standartlara uygun ortamlar sağlanmakta mıdır? Donanım bakımlarına yönelik yapılan işlemler kayıt altına alınmakta mıdır?
3.6.2.10	Kablolama Güvenliği	Mülakat, Gözden Geçirme	Kablolama güvenliğini sağlamak için ne gibi kontroller uygulanmaktadır?
3.6.2.11	Fiziksel Giriş Kontrolleri	Mülakat, Gözden Geçirme	Sistem odasına/veri merkezine giriş ve çıkışlara yönelik güvenliği sağlamak için hangi kontroller uygulanmaktadır? Sistem odası/veri merkezine giriş ve çıkış kayıtları tutulmakta mıdır? Bu kayıtlar düzenli olarak gözden geçirilmekte midir?
3.6.2.12	Ortam Koşullarının Gerçek Zamanlı İzlenmesi	Mülakat, Gözden Geçirme	Sistem odası/veri merkezi su, nem, sıcaklık ve duman kontrolü için üretilen veri gerçek zamanlı izlenebilmekte midir?
3.6.2.13	Siber Olay Tespitinde İz Kayıtlarının Kullanılması	Mülakat, Gözden Geçirme	Sistem odası/veri merkezi fiziksel güvenlik ve ortam kontrolü yapılarına ait iz kayıtları, siber olay tespitine girdi sağlayacak şekilde tutulmakta mıdır?
3.6.2.14	Kontrollü Erişim Noktalarının Oluşturulması	Mülakat, Gözden Geçirme	Kontrollü erişim noktaları nasıl belirlenmektedir? Kontrollü erişim noktaları için alınan güvenlik önlemleri nelerdir?
3.6.2.15	İklimlendirme Kontrolü	Mülakat, Gözden Geçirme	Sistem odası/veri merkezi iklimlendirmesi için ne tip klima kullanılmaktadır? Sistem odası/veri merkezinde kullanılan klimalar yedekli midir? Klimaların periyodik olarak bakımları yapılmakta mıdır? Bakımlarına yönelik kayıtlar tutulmakta mıdır?

3.6.3. Elektromanyetik Bilgi Kaçaklarından Korunma Yöntemleri (TEMPEST)

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.6.3.1	1	Sistem Odası/Veri Merkezi Cihaz Yerleşim Planı	Sistem odası/veri merkezinde kullanılan tüm gizlilik seviyeli bilgi işleyen cihazların hangi odalarda/bölümlerde kullanıldığını gösteren bir liste tutulmalıdır.
3.6.3.2	2	Gizlilik Seviyeli Bilgi İşleyen Cihazların TEMPEST Onayı	Sistem odası/veri merkezinde kullanılan tüm gizlilik seviyeli bilgi işleyen cihazların TEMPEST onayları olmalıdır. TEMPEST onayı bulunan cihazların envanteri tutulmalıdır.
3.6.3.3	3	TEMPEST Tesisat Kurallarına Uyum	Sistem odası/veri merkezindeki cihazların bulunduğu odalarda/bölümlerde elektromanyetik bilgi kaçaklarına karşı TEMPEST tesisat kurallarına/ilgili mevzuatlara uygun önlemler alınmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.6.3.1	Sistem Odası/Veri Merkezi Cihaz Yerleşim Planı	Mülakat, Gözden Geçirme	Kurumda sistem odası/veri merkezinde kullanılan tüm gizlilik seviyeli bilgi işleyen cihazların hangi odalarda/bölümlerde kullanıldığını gösteren bir liste bulunmakta mıdır?
3.6.3.2	Gizlilik Seviyeli Bilgi İşleyen Cihazların TEMPEST Onayı	Mülakat, Gözden Geçirme	Sistem odası/veri merkezinde kullanılan gizlilik seviyeli bilgi işleyen cihazların TEMPEST onayları bulunmakta mıdır? TEMPEST onayı bulunan cihazların envanteri tutulmakta mıdır?
3.6.3.3	TEMPEST Tesisat Kurallarına Uyum	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Sistem odası/veri merkezindeki cihazların bulunduğu odalarda/bölümlerde elektromanyetik bilgi kaçaklarına karşı TEMPEST tesisat kurallarına uygun önlemler alınmakta mıdır?

UYGULAMA VE TEKNOLOJİ ALANLARINA YÖNELİK GÜVENLİK TEDBİRLERİ

4. BÖLÜM

4. UYGULAMA VE TEKNOLOJİ ALANLARINA YÖNELİK GÜVENLİK TEDBİRLERİ

4.1. Kişisel Verilerin Güvenliği

Amaç

Bu güvenlik tedbiri ana başlığının amacı, kişisel verilerin güvenliği çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. "Kişisel Verilerin Güvenliği" ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Kayıt Yönetimi
- Erişim Kayıtları Yönetimi
- Yetkilendirme
- Şifreleme
- Yedekleme, Silme, Yok Etme ve Anonim Hale Getirme
- Aydınlatma Yönetimi
- Açık Rıza Yönetimi
- Kişisel Veri Yönetim Sürecinin İşletilmesi

4.1.1. Kayıt Yönetimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.1.1.1	1	Kişisel Veri İşleme Envanterinin Hazırlanması ve Yönetimi	Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirdikleri kişisel veri işleme faaliyetlerini; • Kişisel veri işleme amaçları ve hukuki dayanağını, • Veri kategorisini, • Aktarılan alıcı grubunu, • Kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, • Yabancı ülkelere aktarımı öngörülen kişisel verileri, • Veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları kişisel veri envanteri oluşturulmalı ve belirli periyotlarda güncellenmelidir. Hazırlanan envanter, Veri Sorumluları Sicili Hakkında Yönetmelik'e uygun olmalıdır.
4.1.1.2	1	Kişisel Veri Saklama ve İmha Politikasının Hazırlanması	Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'e uygun olarak ve kurum tarafından hazırlanan kişisel veri işleme envanteri göz önünde bulundurularak kişisel veri saklama ve imha politikası hazırlanmalıdır.
4.1.1.3	1	Kişisel Verilerin Veri Tabanlarında Birincil Anahtar Olarak Kullanılmaması	Veri tabanı tablolarının tasarımında kişisel veriler (T.C. kimlik numarası, pasaport numarası vb.) birincil anahtar olarak kullanılmamalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.1.1.4	1	Veri Tabanının Dışarıya Aktarımının Yetkili Kullanıcı Tarafından Yapılması	Kişisel veri barındıran veri tabanının dışarıya aktarımı (dosya olarak kaydetme, yerel veya uzak uygulamalara transfer etme vb.) yalnızca yetkilendirilmiş kullanıcılar tarafından yapılmalıdır. Bk. Tedbir No: 3.2.7.4
4.1.1.5	1	Kişisel Verilerin Güvensiz Ortamlarda Saklanmaması	Kişisel veri barındıran kayıtlar (resimler, ofis dosyaları vb.) güvensiz ortamlarda (yetkisiz erişim sağlanabilen ortak dizin, harici bellek, disk vb.) saklanmamalıdır. Kayıtların saklanmasının zorunlu olduğu durumlarda ulusal/uluslararası standartlar/otoriteler tarafından kabul edilen güvenli yöntemlerden yararlanılmalıdır.
4.1.1.6	1	Kişisel Veri Üzerinde Girdi/Çıktı Denetimi Yapılması	Uygulamanın girdi olarak kullandığı kişisel veri üzerinde girdi/çıktı doğrulama eksikliğinden kaynaklı zafiyetlere karşı güvenlik kontrolleri uygulanmalıdır. Bk. Tedbir Başlık No: 3.2.10
4.1.1.7	1	Kişisel Verinin Gizli Alanlarda Saklanmaması	İlgili kişinin açık rızası olmadan kişisel veri web sayfalarının gizli alanlarında saklanmamalıdır. Kişisel veri, tarayıcı ön belleğinde (cache) saklanmamalıdır. Uygulamada kullanılan çerezlerin kişisel veri içermesi zorunluluk ise secure bayrağı (secure flag) kullanılmalıdır. Ayrıca, istemci tarafında web depolama (web storage) özelliği ile kişisel veriler kayıt altına alınmamalıdır.
4.1.1.8	1	Hata Mesajlarında Mahremiyetin Korunması	Bk. Tedbir No: 3.2.8.3
4.1.1.9	1	Özel Nitelikli Kişisel Verinin Saklanması	Özel nitelikli kişisel veriyi barındıran kayıtlar ulusal/uluslararası kabul görmüş güvenli yöntemlerle (şifreli metin olarak, güçlü şifreleme algoritmaları kullanarak, disk seviyesinde şifreleme vb.) saklanmalıdır. Bk. Tedbir No: 3.2.7.10
4.1.1.10	1	Geçici Olarak Tutulan Kişisel Verinin Yok Edilmesi	İstemci ve sunucu uygulamalarında dosyalarda ve çerezlerde geçici olarak tutulan kişisel verilerin işleme gereksinimi veya kanuni saklama süresi sona erdiğinde güvenlik ihlali oluşturamayacak şekilde (geri getirilemeyecek, tekrar elde edilemeyecek vb.) yok edilmelidir.
4.1.1.11	2	Veri Tabanı Tasarımı	Veri tabanı tasarımı kişisel verilerin yedekleme, anonimleştirme ve veri aktarımı işlemlerini kolaylaştıracak şekilde yapılmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.1.1.1	Kişisel Veri İşleme Envanterinin Hazırlanması ve Yönetimi	Mülakat, Gözden Geçirme	Veri Sorumluları Sicili Hakkında Yönetmelik'e uygun kişisel veri işleme envanteri hazırlanmış mıdır? Envanter belirli periyotlarda güncellenmekte midir?
4.1.1.2	Kişisel Veri Saklama ve İmha Politikasının Hazırlanması	Mülakat, Gözden Geçirme	Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'e uygun kişisel veri saklama ve imha politikası hazırlanmış, ilgili taraflara duyurulmuş ve uygulanıyor mu?
4.1.1.3	Kişisel Verilerin Veri Tabanlarında Birincil Anahtar Olarak Kullanılmaması	Mülakat, Gözden Geçirme	Veri tabanı tablolarının tasarımında kişisel veriler (T.C. kimlik numarası, pasaport numarası vb.) birincil anahtar olarak kullanılmakta mıdır?
4.1.1.4	Veri Tabanının Dışarıya Aktarımının Yetkili Kullanıcı Tarafından Yapılması	Mülakat, Güvenlik Denetimi	Veri tabanı işlemlerinde kullanılan hesaplarda minimum yetki prensibi uygulanmakta mıdır? Veri tabanının kısmen/tamamen dışa aktarımı için hangi hesap(lar) kullanılmaktadır?
4.1.1.5	Kişisel Verilerin Güvensiz Ortamlarda Saklanmaması	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Kişisel verinin hangi ortamlarda saklanabileceği tanımlanmış mıdır? Tanımlanan ortamlarda ulusal/uluslararası standartlara uygun güvenlik önlemleri alınmakta mıdır?
4.1.1.6	Kişisel Veri Üzerinde Girdi/Çıktı Denetimi Yapılması	Mülakat, Gözden Geçirme, Sızma Testi	Uygulamanın girdi olarak kullandığı kişisel veri üzerinde girdi/çıktı doğrulama eksikliğinden kaynaklı zafiyetlere karşı güvenlik kontrolleri uygulanmakta mıdır?
4.1.1.7	Kişisel Verinin Gizli Alanlarda Saklanmaması	Mülakat, Gözden Geçirme, Sızma Testi	Kişisel veriler web sayfalarının gizli alanlarında ya da web depolama özelliği üzerinde saklanmakta mıdır? Kişisel veriler tarayıcı ön belleğinde saklanmakta mıdır? Çerezlerde bulunan kişisel verinin güvenliği nasıl sağlanmaktadır?
4.1.1.8	Hata Mesajlarında Mahremiyetin Korunması	Mülakat, Gözden Geçirme	Hata mesajlarında mahremiyetin korunması amacı ile hangi önlemler alınmaktadır?
4.1.1.9	Özel Nitelikli Kişisel Verinin Saklanması	Mülakat, Gözden Geçirme, Sızma Testi	Özel nitelikli kişisel veri barındıran kayıtların güvenliği için ne gibi önlemler alınıyor? Alınan önlemler ulusal ve/veya uluslararası kabul görmüş uygulamalar mıdır?
4.1.1.10	Geçici Olarak Tutulan Kişisel Verinin Yok Edilmesi	Mülakat, Gözden Geçirme, Sızma Testi	İstemci ve sunucu uygulamalarında kişisel verinin geçici kopyalarının yok edilmesi (geri getirilemeyecek, tekrar elde edilemeyecek vb. şekilde silme) amacıyla yöntemler/süreçler belirlenmiş midir? Belirlenen yöntemler/süreçler uygulanmakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.1.1.11	Veri Tabanı Tasarımı	Mülakat, Gözden Geçirme	Kişisel verilerin yedekleme, anonimleştirme ve veri aktarımı işlemlerini kolaylaştırmak için veri tabanı tasarımında hangi adımlar atılmıştır?

4.1.2. Erişim Kayıtları Yönetimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.1.2.1	1	Erişimlerin Kayıt Altına Alınması	Kişisel veri barındıran ortamlara yapılan başarılı ve başarısız erişimler kayıt altına alınmalıdır.
4.1.2.2	1	Erişim Kayıtlarının Arşivlenmesi	Kişisel verilere gerçekleştirilen erişim kayıtları, kurumun tabi olduğu ilgili mevzuata ve ikincil düzenlemelere uygun şekilde arşivlenmelidir.
4.1.2.3	1	Erişim Kayıtlarının Güvenliğinin Sağlanması	Kişisel veriye gerçekleştirilen erişim kayıtlarının yetkisiz okunması, değiştirilmesi veya silinmesi önlenmelidir. Bk. Tedbir No: 3.1.8.1
4.1.2.4	1	Erişim Kayıtlarının Aktarımı	Kişisel veriye gerçekleştirilen erişim kayıtları dışarı ve içeri aktarılabilir olmalıdır. Çalışan sistem üzerinde yapılacak içeri aktarma işlemi mevcut kayıtları yok etmemeli veya değiştirmemelidir.
4.1.2.5	2	Yetkisiz Erişimlerin Tespiti	Kişisel veriye gerçekleştirilen yetkisiz işlemleri tespit edebilmek için erişim kayıtları analiz edilmelidir.
4.1.2.6	3	Erişim Kayıtlarında Özel Nitelikli Kişisel Veri Bulundurulmaması	Erişim kayıtları özel nitelikli kişisel veri barındırmamalıdır. Kayıtlarda özel nitelikli kişisel verinin bulundurulmasının zorunlu olduğu durumlarda, işlem detayının anlaşılabileceği şekilde kişisel verilerin güvenliği maskeleme vb. yöntemler ile sağlanmalıdır. Bk. Tedbir No: 3.2.8.3

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.1.2.1	Erişimlerin Kayıt Altına Alınması	Mülakat, Gözden Geçirme	Kişisel veri barındıran ortamlara yapılan başarılı ve başarısız erişimler kayıt altına alınmakta mıdır? Alınan kayıtlar hangi periyotlarda gözden geçirilmektedir?
4.1.2.2	Erişim Kayıtlarının Arşivlenmesi	Mülakat, Gözden Geçirme	Kişisel verilere gerçekleştirilen erişim kayıtları ilgili mevzuatlara ve ikincil düzenlemelere uygun şekilde arşivlenmekte midir?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.1.2.3	Erişim Kayıtlarının Güvenliğinin Sağlanması	Mülakat, Gözden Geçirme	Kişisel veriye gerçekleştirilen erişim kayıtlarının güvenliği nasıl sağlanmaktadır?
4.1.2.4	Erişim Kayıtlarının Aktarımı	Mülakat, Gözden Geçirme	Erişim kayıtlarının dışarı/içeri aktarılması için bir mekanizma mevcut mudur? Erişim kayıtlarının dışarı/içeri aktarılması için kullanılan mekanizmada mevcut kayıtların güvenliğini sağlamak için ne gibi önlemler alınmaktadır?
4.1.2.5	Yetkisiz Erişimlerin Tespiti	Mülakat, Gözden Geçirme	Erişim kayıtları üzerinden yetkisiz işlemleri tespit edebilmek amacıyla analiz faaliyetleri gerçekleştirilmekte midir?
4.1.2.6	Erişim Kayıtlarında Özel Nitelikli Kişisel Veri Bulundurulmaması	Mülakat, Gözden Geçirme	Erişim kayıtlarının hangi bilgileri içereceği tanımlanmış mı? Erişim kayıtları özel nitelikli kişisel veri barındırıyor mu?

4.1.3. Yetkilendirme

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.1.3.1	1	Yetkilendirme Mekanizmasının Kullanılması	Kullanıcıların sadece erişim yetki matrislerinde yetkilendirildiği kişisel veriye erişmesi sağlanmalıdır. Yetkisiz erişim durumunda veya beklenmeyen bir durum oluştuğunda kişisel veriye erişim varsayılan olarak engellenmelidir. Bk. Tedbir No: 3.2.3.1 Bk. Tedbir No: 3.2.8.1
4.1.3.2	1	Kimlik Doğrulama Mekanizmasının Kullanılması	Kişisel veri barındıran tüm ortamlara (web sayfası, dosya vb.) erişim için kimlik doğrulaması yapılmalıdır.
4.1.3.3	1	Erişimin Sınırlandırılması	Kişisel veri barındıran ortamlara (veri tabanı sunucusu, dosya sunucusu vb.) sadece uygulamadan erişim sağlanmalı ve bu ortamlara alternatif ve güvenli olmayan yöntemler (veri tabanı istemcileri ile doğrudan erişim, güvenli olmayan protokoller ile erişim vb.) ile yapılabilecek yetkisiz erişimler engellenmelidir.
4.1.3.4	1	Erişim Denetim Politikalarının Oluşturulması	Kişisel verilerin bulunduğu ortamlar/kaynaklar belirlenmelidir. Belirlenen ortamlar/kaynaklar için erişim denetim politikaları oluşturulmalıdır. Bu politikalarda, kullanıcı rolleri ve erişim yetkilerini açıklayan matris tanımlanmalıdır.
4.1.3.5	2	Çok Faktörlü Kimlik Doğrulama Mekanizmasının Kullanılması	Özel nitelikli kişisel verilerin tutulduğu ortamlara erişim için çok faktörlü kimlik doğrulaması yapılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.1.3.6	2	Dış Sistemler / Uygulamalar Arası Veri Akışı için Erişimlerin Doğrulanması	Dış sistemler/uygulamalar arası kişisel veri akışı için erişim doğrulama kontrolü yapılmalıdır. Dış sistemler ve uygulamalar arasındaki kişisel veri akışlarında erişim ile ilgili girdi parametreleri ve sonuçlar kayıt altına alınmalıdır.
4.1.3.7	3	Alt Bileşenler Arasında Veri Akışı için Erişimlerin Doğrulanması	Sistem içi kişisel verinin akışı için erişim doğrulama kontrolü yapılmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.1.3.1	Yetkilendirme Mekanizmasının Kullanılması	Mülakat, Gözden Geçirme, Sızma Testi	Kişisel veriye erişim istekleri için yetkilendirme mekanizması kullanılmakta mıdır? Kişisel veriye erişim isteklerinde kullanılan yetkilendirme mekanizmasında hangi kurallar uygulanmaktadır? Kişisel veriye yetkisiz erişimi engellemek amacıyla hangi önlemler alınmaktadır?
4.1.3.2	Kimlik Doğrulama Mekanizmasının Kullanılması	Mülakat, Gözden Geçirme, Sızma Testi	Kişisel veri barındıran ortamlara (web sayfası, dosya vb.) erişimde kimlik doğrulama mekanizması kullanılıyor mu?
4.1.3.3	Erişimin Sınırlandırılması	Mülakat, Gözden Geçirme, Sızma Testi	Kişisel veri barındıran ortamlara hangi yöntemlerle erişim sağlanmaktadır? Belirlenen yöntemler kullanılmadan gerçekleştirilmek istenen erişimlerin engellenmesi amacıyla hangi önlemler alınmaktadır?
4.1.3.4	Erişim Denetim Politikalarının Oluşturulması	Mülakat, Gözden Geçirme	Kişisel verilerin bulunduğu ortamlara/kaynaklara yapılacak erişimleri denetlemek amacıyla politika oluşturulmuş mudur? Belirlenen politika hangi hususları içermektedir?
4.1.3.5	Çok Faktörlü Kimlik Doğrulama Mekanizmasının Kullanılması	Mülakat, Gözden Geçirme, Sızma Testi	Özel nitelikli kişisel veri barındıran ortamlara erişim için kullanılan kimlik doğrulama mekanizmaları nelerdir?
4.1.3.6	Dış Sistemler / Uygulamalar Arası Veri Akışı için Erişimlerin Doğrulanması	Mülakat, Gözden Geçirme, Sızma Testi	Dış sistemler/uygulamalar arası kişisel veri akışı için erişim doğrulama kontrolü yapılmakta mıdır? Erişim ile ilgili girdi parametreleri ve sonuçlar kayıt altına alınmakta mıdır?
4.1.3.7	Alt Bileşenler Arasında Veri Akışı için Erişimlerin Doğrulanması	Mülakat, Gözden Geçirme, Sızma Testi	Sistem içi kişisel verinin akışı için erişim doğrulama kontrolü yapılmakta mıdır?

4.1.4. Şifreleme

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.1.4.1	1	İletişimin Şifrelenmesi	Kişisel verinin paylaşımında sistemler (kurum uygulamaları, dış web servisler) arası iletişim şifreli olarak gerçekleştirilmelidir. Bk. Tedbir No: 3.2.9.1
4.1.4.2	2	Verinin Maskelenmesi	Kişisel veri üzerinde işlem yapılması ana amaç olmayan durumlarda (Adres bilgileri güncellenirken T.C. kimlik numarasının maskelenmesi, hesap numarasına havale işleminde alıcının adının maskelenmesi vb.) uygulama kişisel veriyi maskeleyerek göstermelidir.
4.1.4.3	2	Verinin Bütünlüğünün Korunması	Kişisel verinin yetkisiz bir şekilde değiştirilmesini engellemek için uygun kriptografik yöntemler uygulanmalıdır.
4.1.4.4	3	Sistemin Alt Bileşenleri Arasındaki İletişimin Şifreli Yapılması	Bk. Tedbir No: 3.2.5.11

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.1.4.1	İletişimin Şifrelenmesi	Mülakat, Gözden Geçirme, Sızma Testi	Kişisel verinin paylaşımında sistemler arası iletişim şifreli olarak gerçekleştirilmekte midir?
4.1.4.2	Verinin Maskelenmesi	Mülakat, Güvenlik Denetimi	Kişisel veri üzerinde işlem yapılması ana amaç olmayan durumlarda verinin mahremiyeti için hangi önlemler alınmaktadır? Alınan önlemlerde maskeleme yöntemleri kullanılmakta mıdır? Kullanılan maskeleme yöntemleri nelerdir?
4.1.4.3	Verinin Bütünlüğünün Korunması	Mülakat, Gözden Geçirme	Kişisel verinin yetkisiz bir şekilde değiştirilmesini engellemek için hangi yöntemler kullanılmaktadır? Kullanılan yöntemlerde kriptografik kontroller yer almakta mıdır?
4.1.4.4	Sistemin Alt Bileşenleri Arasındaki İletişimin Şifreli Yapılması	Mülakat, Gözden Geçirme, Sızma Testi	Bk. Denetim No: 3.2.5.11

4.1.5. Yedekleme, Silme, Yok Etme ve Anonim Hale Getirme

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.1.5.1	1	Sistem Yedeklerinin Yetkili Kullanıcılar Tarafından Alınması	Kişisel veri barındıran sistem yedeklerinin sadece yetkili kullanıcılar tarafından alınması sağlanmalıdır. İlgili yedekleme işlemlerine ait iz kayıtları tutulmalıdır. Bk. Tedbir No: 3.1.8.1
4.1.5.2	1	Kişisel Verilerin Silinmesi	Silme işlemine konu teşkil edecek kişisel verilerin belirlenerek, bu verilere erişim yetkisi olan ilgili kullanıcıların tespit edilmesi ve ilgili kullanıcıların erişim, geri getirme, tekrar kullanma gibi yetkilerinin ortadan kaldırılması amacıyla gerekli süreçler tanımlanmalı ve uygulanmalıdır.
4.1.5.3	1	Kişisel Verilerin Yok Edilmesi	İşleme süresi biten kişisel verilerin hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi amacıyla gerekli süreçler tanımlanmalı ve uygulanmalıdır.
4.1.5.4	1	Kişisel Verilerin Anonim Hale Getirilmesi	Kişisel veri saklama ve imha politikası çerçevesinde, saklama süresi dolan ve anonim hale getirilmesi uygun görülen kişisel veriler ile gerçek ortam hariç test, eğitim ve geliştirme gibi ortamlarda kullanılacak kişisel veriler ulusal/uluslararası standartlar/otoriteler tarafından kabul görmüş yöntemlerle anonim hale getirilmelidir.
4.1.5.5	1	Kişisel Veri Barındıran Yedeklerin Güvenliğinin Sağlanması	Kişisel veriyi barındıran yedekler etkin güvenlik kontrollerinin uygulandığı ortamlarda saklanmalıdır. Kişisel veri barındıran yedeklerin yetkisiz okunması, değiştirilmesi veya silinmesi engellenmelidir. Yedeklere yapılan erişimlerin iz kayıtları tutulmalıdır. Bk. Tedbir No: 3.1.8.1
4.1.5.6	2	Kişisel Veri Barındıran Yedeklerin Yok Edilmesi	Kişisel veri barındıran yedeklerin güvenli şekilde yok edilmesi (geri getirilemeyecek, tekrar elde edilemeyecek vb. şekilde silme) için gerekli süreç tanımlanmalı ve uygulanmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.1.5.1	Sistem Yedeklerinin Yetkili Kullanıcılar Tarafından Alınması	Mülakat, Güvenlik Denetimi	Kişisel veri barından sistem yedeklerini almak amacıyla yetkilendirilmiş kullanıcılar bulunmakta mıdır? Yedekleme işlemlerine ait iz kayıtları tutulmakta mıdır? Tutulan kayıtlar ne kadar süre ile muhafaza edilmektedir?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.1.5.2	Kişisel Verilerin Silinmesi	Mülakat, Gözden Geçirme	Kişisel verilerin silinmesine yönelik süreç tanımlanmış ve uygulanmakta mıdır?
4.1.5.3	Kişisel Verilerin Yok Edilmesi	Mülakat, Gözden Geçirme	İşleme süresi biten kişisel veriler nasıl belirlenmektedir? Kişisel verilerin saklanmasına ve imhasına yönelik politika oluşturulmuş ve uygulanmakta mıdır?
4.1.5.4	Kişisel Verilerin Anonim Hale Getirilmesi	Mülakat, Gözden Geçirme, Sızma Testi	Anonim hale getirilmesi planlanan kişisel veriler nasıl belirlenmektedir? Kişisel verileri anonim hale getirmek amacıyla hangi yöntemlerden faydalanılmaktadır? Test, geliştirme vb. ortamlarda kullanılan kişisel veriler anonim hale getirilmekte midir?
4.1.5.5	Kişisel Veri Barındıran Yedeklerin Güvenliğinin Sağlanması	Mülakat, Gözden Geçirme	Kişisel veri barındıran yedeklerin güvenliğinin sağlanması için uygulanacak faaliyetler/süreçler belirlenmiş midir? Yedeklere yapılan erişimlerin iz kayıtları tutulmakta mıdır?
4.1.5.6	Kişisel Veri Barındıran Yedeklerin Yok Edilmesi	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Kişisel veri barındıran yedeklerin güvenli şekilde yok edilmesi amacıyla bir mekanizma/süreç uygulanmakta mıdır?

4.1.6. Aydınlatma Yönetimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.1.6.1	1	Aydınlatmanın Doğru Zamanda Yapılması	İlgili kişiden elde edilecek kişisel verilerle ilgili işleme faaliyetine başlamadan önce ilgili kişinin talebine bağlı olmadan aydınlatma yapılmalıdır. Kişisel veri ilgili kişiden elde edilmiyorsa; • Kişisel verilerin elde edilmesinden itibaren makul bir süre içerisinde, • Kişisel verilerin ilgili kişi ile iletişim amacıyla kullanılacak olması durumunda, ilk iletişim kurulması esnasında, • Kişisel verilerin aktarılacak olması halinde, en geç kişisel verilerin ilk kez aktarımının yapılacağı esnada ilgili kişi aydınlatılmalıdır. Aydınlatma ile ilgili yükümlülüğün yerine getirilmesi süreci Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'e uygun olarak yürütülmelidir.
4.1.6.2	1	Aydınlatmanın Yerine Getirildiğinin İspat Edilmesi	Aydınlatma metninin ilgili kişi tarafından okunup anlaşıldığına dair kayıtlar tutulmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.1.6.3	2	Uygulama Üzerinden Aydınlatma Metninin Güncellenmesi	Aydınlatma metni, yetkili kullanıcılar tarafından uygulama üzerinden güncellenebilmelidir. Aydınlatma metninin güncelleme işlemi öncesi durumu kayıt altına alınmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.1.6.1	Aydınlatmanın Doğru Zamanda Yapılması	Mülakat, Gözden Geçirme	İlgili kişilere aydınlatmanın doğru zamanda yapılması amacıyla bir süreç oluşturulmuş mudur?
4.1.6.2	Aydınlatmanın Yerine Getirildiğinin İspat Edilmesi	Mülakat, Gözden Geçirme	Aydınlatmanın yerine getirildiğini ispat edecek bir mekanizma oluşturulmuş mudur?
4.1.6.3	Uygulama Üzerinden Aydınlatma Metninin Güncellenmesi	Mülakat, Gözden Geçirme	Aydınlatma metni uygulama üzerinden güncellenebilmekte midir? Aydınlatma metninin güncelleme işlemi öncesi durumu kayıt altına alınmakta mıdır?

4.1.7. Açık Rıza Yönetimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.1.7.1	1	Açık Rıza Unsurlarının Belirlenmesi	Kişisel verilerin işlenmesi amacıyla açık rıza alınması gereken durumlarda, kişisel veri işleme amacının açıkça ifade edildiği açık rıza metni hazırlanmalı ve ilgili kişilere sunulmalıdır. Kişisel verilerin yurt içi veya yurt dışı aktarımı söz konusu ise bu husus açık rıza metninde ifade edilerek ayrı bir bölüm halinde düzenlenmeli ve ilgili kişilerden ayrı bir açık rıza alınmalıdır. Kişisel verilerin farklı işleme amaçları varsa her biri için ayrı açık rıza alınmalıdır.
4.1.7.2	1	Açık Rızanın Kayıt Altına Alınması	İlgili kişiden alınmış açık rızanın inkâr edilemezliğini sağlamak amacıyla alınan açık rıza kayıt zaman damgası ile kayıt altına alınmalıdır. Bk. Tedbir No: 3.1.8.4
4.1.7.3	1	Açık Rıza Durumunun Sorgulanması	Açık rıza metninin onay tarihi ve onay durumu saklanmalıdır. İlgili kişiye ait açık rıza durumu ilgili kişi ve yetkili kişi(ler) tarafından görüntülenebilmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.1.7.4	3	Uygulama Üzerinden Açık Rıza Alınması	Özel nitelikli kişisel verinin işlenmesi ve kişisel verinin üçüncü kişilere aktarılması durumunda açık rıza uygulama üzerinden alınmalı ve açık rıza beyan durumu sorgulanabilmelidir.
4.1.7.5	3	Açık Rıza Metninin Güncellenmesi	Uygulama üzerinde açık rıza metni yetkili kişiler tarafından güncellenebilmelidir. Güncelleme öncesindeki açık rıza metinleri saklanmalıdır. Güncellenen açık rıza metinleri için kullanıcılardan tekrar açık rıza alınması sağlanmalıdır.
4.1.7.6	3	Açık Rıza ile İlgili Taleplerin Yönetilmesi	İlgili kişi, açık rızasını geri alma talebini uygulama üzerinden gerçekleştirebilmelidir. İlgili kişinin açık rızasını geri alma talebi veri sorumlusu tarafından uygulanmalı ve ilgili kişinin açık rızasına dayanarak yapılan veri işleme faaliyetleri durdurulmalıdır.
4.1.7.7	3	Islak İmzalı Açık Rıza Metninin Saklanması	İlgili kişiden alınmış ıslak imzalı (fiziksel) açık rıza metninin aslı ya da taranmış kopyası saklanmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.1.7.1	Açık Rıza Unsurlarının Belirlenmesi	Mülakat, Gözden Geçirme	Kişisel verilerin işlenmesi amacıyla açık rıza alınması gereken durumlar belirlenmiş midir? Açık rıza alınması amacıyla aydınlatma metni hazırlanarak ilgili kişilere sunulmakta mıdır?
4.1.7.2	Açık Rızanın Kayıt Altına Alınması	Mülakat, Gözden Geçirme	Açık rızanın kayıt altına alınması için bir mekanizma/süreç işletilmekte midir?
4.1.7.3	Açık Rıza Durumunun Sorgulanması	Mülakat, Gözden Geçirme	İlgili kişiye ait açık rıza metninin onay durumu, onay tarihi saklanmakta mıdır? İlgili kişi tarafından açık rıza durumu sorgulanabilmekte midir? Yetkili kişi(ler)ce hangi kullanıcılardan açık rıza alındığı sorgulanabilmekte midir?
4.1.7.4	Uygulama Üzerinden Açık Rıza Alınması	Mülakat, Gözden Geçirme	Uygulama üzerinden açık rızanın alınması ve açık rıza beyan durumunun sorgulanması için bir mekanizma/süreç işletilmekte midir?
4.1.7.5	Açık Rıza Metninin Güncellenmesi	Mülakat, Gözden Geçirme	Uygulama üzerinde açık rıza metninin güncellenebilmesi için bir mekanizma/süreç tanımlanmış mıdır? Güncelleme öncesindeki açık rıza metinleri saklanmakta mıdır? Güncellenen açık rıza metinleri için kullanıcılardan tekrar açık rıza alınmakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.1.7.6	Açık Rıza ile İlgili Taleplerin Yönetilmesi	Mülakat, Gözden Geçirme	Uygulama üzerinden açık rıza ile ilgili taleplerin yönetimi sağlanabilmekte midir?
4.1.7.7	Islak İmzalı Açık Rıza Metninin Saklanması	Mülakat, Gözden Geçirme	Islak imzalı açık rıza metinlerinin taranmış halinin saklanması amacıyla bir süreç işletilmekte midir?

4.1.8. Kişisel Veri Yönetim Sürecinin İşletilmesi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.1.8.1	1	İlgili Kişinin Başvuru Hakkının Yönetilmesi	İlgili kişinin veri sorumlusuna başvuruda bulunabilmesi ve bu başvuruya süresinde cevap verilebilmesi için bir süreç oluşturulmalıdır. Bu süreç Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'e uygun olmalıdır.
4.1.8.2	1	Kişisel Veriye Yapılan İşlemlerin Elde Edilmesi	İlgili kişinin, kişisel verisine yapılan işlemleri öğrenme talebine istinaden veri sorumlusu tarafından bu işlemler elde edilmelidir. Bk. Tedbir No: 4.1.8.1
4.1.8.3	1	Güncelleme, Anonimleştirme, Silme ve Yok Etme İşlemlerinin Gerçekleştirilmesi	İlgili kişi tarafından talep edilen; güncelleme, anonimleştirme, silme, yok etme işlemleri gerçekleştirilmelidir. Talep edilmesi durumunda bu işlemler kişisel verinin aktarıldığı üçüncü taraflara da iletilmelidir. Yapılacak işlemlerle ilgili bilgilendirme Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'e uygun olarak gerçekleştirilmelidir. Bk. Tedbir No: 4.1.8.1
4.1.8.4	1	Kişisel Verinin Aktarıldığı Üçüncü Tarafların Tespit Edilmesi	Kişisel verinin kimlere aktarıldığı, aktarılma amacı ve aktarılma tarihine ait bilgiler kayıt altına alınmalı ve bu bilgiler talep edilmesi durumunda ilgili kişiye bildirilmelidir. Bk. Tedbir No: 4.1.8.1
4.1.8.5	2	Kişisel Verisi Etkilenen veya Etkilenmesi Muhtemel Kişilerin Bilgilendirilmesi	Kişisel verinin kanuni olmayan yollarla başkaları tarafından ele geçirilmesi, yayımlanması, ifşa edilmesi veya bütünlüğünün bozulması durumunda ilgili kişi ve mevzuat gereği bilgilendirilmesi gereken kurum ve kuruluşlar bilgilendirilmelidir. İlgili kişiye yapılacak bildirimler uygun yöntemlerle (internet sayfası, e-posta, SMS vb.) gerçekleştirilmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.1.8.1	İlgili Kişinin Başvuru Hakkının Yönetilmesi	Mülakat, Gözden Geçirme	İlgili kişinin veri sorumlusuna başvuru hakkının yönetilmesi amacıyla bir süreç işletilmekte midir? Bu süreç yürürlükte olan ilgili mevzuata uygun mudur?
4.1.8.2	Kişisel Veriye Yapılan İşlemlerin Elde Edilmesi	Mülakat, Gözden Geçirme	İlgili kişinin verisine yapılan işlemler kayıt altında tutulmakta mıdır?
4.1.8.3	Güncelleme, Anonimleştirme, Silme ve Yok Etme İşlemlerinin Gerçekleştirilmesi	Mülakat, Gözden Geçirme	İlgili kişi tarafından talep edilen güncelleme, anonimleştirme, silme ve yok etme işlemlerinin yapılabilmesi amacıyla bir süreç işletilmekte midir? Tanımlanan süreç yürürlükte olan mevzuata uygun mudur?
4.1.8.4	Kişisel Verinin Aktarıldığı Üçüncü Tarafların Tespit Edilmesi	Mülakat, Gözden Geçirme	Kişisel veriler üçüncü taraflara aktarıldığında aktarım işlemi ile ilgili hangi bilgiler kayıt altına alınmaktadır?
4.1.8.5	Kişisel Verisi Etkilenen veya Etkilenmesi Muhtemel Kişilerin Bilgilendirilmesi	Mülakat, Gözden Geçirme	Kişisel veri ihlalinin kamuoyuna, yetkili kurum ve kuruluşlar ile ilgili kişiye bildirilmesi amacıyla bir süreç işletilmekte midir?

4.2. Anlık Mesajlaşma Güvenliği

Amaç

Bu güvenlik tedbiri ana başlığının amacı, anlık mesajlaşma güvenliği çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. “Anlık Mesajlaşma Güvenliği” ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Genel Güvenlik Tedbirleri

4.2.1. Genel Güvenlik Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.2.1.1	1	Mesajlaşma Uygulaması Seçimi	Kurumsal haberleşme amacıyla sunucuları kurum kontrolünde olan mesajlaşma uygulamaları kullanılmalıdır. Kurumun kendine ait bir haberleşme uygulaması yoksa mesajlaşma amacıyla sunucuları yurt içinde bulunan yerli ve milli uygulamalar tercih edilmelidir.
4.2.1.2	1	İletim Ortamı Güvenliği	Mesajlaşma uygulamasının iletim katmanı güvenliği, bilinen zafiyetleri olmayan, güncel bir SSL/TLS sürümü ile sağlanmalıdır ve uygulamada SSL Pinning kullanılmalıdır. Bk. Tedbir No: 3.2.9.1

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.2.1.3	1	Gizlilik Dereceli Veri Paylaşımı	Mevzuatta kodlu veya kriptolu haberleşmeye yetkilendirilmiş kurumlar tarafından geliştirilen yerli mobil uygulamalar hariç olmak üzere mobil uygulamalar üzerinden gizlilik dereceli veri paylaşımı ve haberleşme yapılmamalıdır.
4.2.1.4	1	Çoklu Cihaz Kullanımı	Uygulama birden fazla mobil cihaz üzerinde eş zamanlı olarak çalışmamalıdır. Hesaba farklı bir mobil cihazdan giriş yapılmak istendiğinde kullanıcı kimlik doğrulamaya zorlanmalı, başarılı kimlik doğrulama sonrası uygulama sadece yeni giriş yapılan cihaz üzerinde kullanılabilmelidir.
4.2.1.5	2	Uçtan Uca Şifreleme	Uygulamadan gönderilen tüm mesajlar ve uygulama kullanılarak yapılan tüm sesli ve görüntülü aramalar uçtan uca şifrelenmelidir.
4.2.1.6	2	Şifreleme Anahtarlarının Saklanması	Uygulama şifreleme için kullandığı anahtarları işletim sisteminin güvenli depolama alanlarında (TEE, HSM, keystore, keychain vb.) tutmalıdır.
4.2.1.7	2	Yönetim Arayüzüne Erişim	Mesajlaşma sistemlerine ait yönetim arayüzlerine yetkili tarafların erişimi, yeterli en düşük haklarla güvenli bir şekilde yapılmalıdır. Yönetim arayüzüne erişilerek yapılan işlemlere ait denetim izleri tutulmalıdır. Bk. Tedbir No: 3.1.8.1
4.2.1.8	3	Cihaz Üzerindeki Verinin Şifrelenmesi	Uygulama cihaz üzerinde sakladığı tüm veriyi şifreli olarak tutmalıdır.
4.2.1.9	3	Kritik Haberleşmenin Güvenliği	Kritik veri içeren her türlü sesli, yazılı ve görüntülü haberleşme uygulamalarında, kaynak kodları kurum tarafından talep edildiğinde denetlenebilen, işletmesi ve yönetimi yerel olarak yapılabilen yerli ve milli uygulamalar tercih edilmelidir.

Denetim Maddeleri

Tedbir No.	Denetim Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.2.1.1	Mesajlaşma Uygulaması Seçimi	Mülakat, Güvenlik Denetimi	Kurum içi mesajlaşma için hangi uygulama kullanılmaktadır?
4.2.1.2	İletim Ortamı Güvenliği	Mülakat, Güvenlik Denetimi	Mesajlaşma sistemlerinde iletim ortamı güvenliği nasıl sağlanmaktadır? Kullanılan protokol ve sürümleri nelerdir? Bilinen ve yayımlanmış zafiyetleri var mıdır? Kullanılan algoritma takımları ve anahtarlar yeterli güvenlik seviyesinde midir?
4.2.1.3	Gizlilik Dereceli Veri Paylaşımı	Mülakat, Güvenlik Denetimi	Mobil uygulamalar üzerinden gizlilik dereceli veri paylaşımı ve haberleşmesi nasıl engellenmektedir?

Tedbir No.	Denetim Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.2.1.4	Çoklu Cihaz Kullanımı	Mülakat, Güvenlik Denetimi	Kullanıcı hesabına aynı anda birden fazla mobil cihaz üzerinden erişilebiliyor mu? Yeni cihaz üzerine kurulum yapılırken kimlik doğrulaması yapılıyor mu?
4.2.1.5	Uçtan Uca Şifreleme	Mülakat, Güvenlik Denetimi, Sızma Testi	Anlık mesajlaşma uygulaması mesajları uçtan uca şifrelemekte midir?
4.2.1.6	Şifreleme Anahtarlarının Saklanması	Mülakat, Güvenlik Denetimi, Sızma Testi	Mesajlaşma uygulaması şifreleme anahtarlarını nasıl saklamaktadır? Anahtarlar cihazdan çıkartılabilir mi?
4.2.1.7	Yönetim Arayüzüne Erişim	Mülakat, Güvenlik Denetimi, Sızma Testi	Mesajlaşma sistemleri yönetim arayüzlerine güvenli erişim nasıl sağlanmaktadır? Erişim yetkileri, bilgi güvenliği gereksinimleri doğrultusunda bilmesi gereken prensibi göz önünde bulundurularak tanımlanmakta mıdır? Yönetim arayüzüne erişilerek gerçekleştirilen işlemler kayıt altına alınmakta mıdır? Eğer kullanılıyor ise kullanıcıların gizli anahtarı, biyometrik bilgisi güvenli bir şekilde tutulmakta mıdır?
4.2.1.8	Cihaz Üzerindeki Verinin Şifrelenmesi	Güvenlik Denetimi, Sızma Testi	Uygulama çalıştığı cihaz üzerinde hangi bilgileri tutmaktadır? Cihaz üzerinde tutulan veri şifreli olarak saklanmakta mıdır? Şifreli veriyi çözmek için gerekli anahtar nerede saklanmaktadır?
4.2.1.9	Kritik Haberleşmenin Güvenliği	Mülakat, Güvenlik Denetimi	Kritik veri iletimini sağlayan uygulamanın yönetimi ve işletimi yerel olarak yapılmakta mıdır? Kaynak kodları talep halinde denetlenebilmekte midir?

4.3. Bulut Bilişim Güvenliği

Amaç

Bu güvenlik tedbiri ana başlığının amacı, bulut bilişim güvenliği çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. “Bulut Bilişim Güvenliği” ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Genel Güvenlik Tedbirleri

4.3.1. Genel Güvenlik Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.3.1.1	1	Bulut Hizmeti Kullanımı	Kritik verilerin yurt içinde depolandığı ve yurt dışında barındırılmayacağı garanti altına alınmalıdır. Kurumlara ait özel bulut sistemleri haricinde, bulut servis sağlayıcılardan yer, sunucu veya servis tabanlı bulut hizmeti kullanılacaksa, • Erişen personel, yetki ve yetkinlik düzeyleri • Erişim, işlem ve ağ trafiği iz kayıtlarının izlenmesi • Güncelleme durum alarmları • Siber olay alarmları • Performans ve kapasite göstergeleri kurum tarafından kontrol edilmelidir.
4.3.1.2	1	Hizmet Kapsamı ile Rol ve Sorumlulukların Belirlenmesi	Bulut bilişim hizmeti kapsamında hizmet alınan taraf ile hizmet alan kurum arasında, karşılıklı yükümlülükleri ve gizlilik maddelerini içeren bir sözleşme yapılmalıdır. Alınan hizmetin kapsamı sözleşme içerisinde tam olarak belirtilmeli ve hizmet kapsamında işlenen verinin kritikliği doğrultusunda yeterli seviyede güvenlik önlemleri alınmalıdır. İlgili sözleşmenin geçerlilik süresi belirlenmeli ve periyodik olarak gözden geçirilmesi sağlanmalıdır. Bk. Tedbir No: 3.5.3.1 Bk. Tedbir No: 3.5.3.3
4.3.1.3	1	Veri İletimi Güvenliği	Bulut bilişim kapsamında çalışan tüm sistemler arasındaki veri trafiği zafiyet içermeyen güvenli ve güncel iletişim protokolleriyle gerçekleştirilmelidir. Bulut ortamına doğru veri iletimi sağlanırken iletimin tek yönlü olması sağlanmalı, kurumsal ağ bulut ortamından gelecek tehditlere karşı izole olmalıdır.
4.3.1.4	1	Kaynakların İzole Edilmesi	Aynı bulut ortamını kullanan kurumların sistemleri ağ seviyesinde birbirlerinden mantıksal ve/veya fiziksel olarak izole edilmelidir. Kurumların yalnızca kendilerine ait veriye erişim imkânı sağlanmalıdır.
4.3.1.5	1	İmajların İmha Edilmesi	Bulut hizmeti kapsamında, ihtiyaç olması durumunda şablon olarak kullanılan imajların geri döndürülemeyecek şekilde silinmesine servis sağlayıcı tarafından imkân tanınmalıdır.
4.3.1.6	1	Sanal Makineye Ait Belleklerin İmhası	Bulut hizmeti kapsamında herhangi bir sanal makinenin hizmetinin sonlandırılması durumunda, sanal makinenin bulut bilişim sunucularında bulunan bellek bölgeleri otomatik olarak servis sağlayıcı tarafından geri döndürülemeyecek şekilde silinmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.3.1.7	1	Bulut Ortamı Güvenliği	Servis sağlayıcılar kendi kaynaklarını DDoS saldırılarına karşı koruyabilmeli ve kapasitesinin üzerinde gelen yüksek boyutlu DDoS saldırılarına karşı iş ve hizmet sürekliliğini sağlayabilmelidir. Hizmet alan taraf ile imzalanan sözleşme ve taahhütlerde bu husus yer almalıdır. Servis sağlayıcılar, servis verdikleri herhangi bir hizmet alanına gelen bir siber saldırıdan (servis dışı bırakma, zararlı yazılım vb.) veya saldırının sistemlerde oluşturabileceği performans problemlerinden diğer hizmet alanlarının etkilenmemesi için güvenlik duvarı, saldırı tespit sistemi gibi güvenlik önlemlerini almalıdır. Servis sağlayıcıların verdikleri hizmetler ile ilgili hizmet seviye taahhüt koşulları belirlenmeli, ölçülmeli ve raporlanabilmelidir. Kurumlar, varlık gruplarının kritiklik derecesine uygun güvenlik tedbirlerini uygulayan ve periyodik güvenlik denetimlerini gerçekleştiren bulut hizmeti sağlayıcılarından hizmet almalıdır. Operatörler tarafından sunuculara erişimde trafiğin yurt içinde kalmasına yönelik tedbirler uygulanmalıdır. Bulut hizmeti kullanımında kuruma ait şifreleme anahtarları hizmeti alan kurum tarafından yönetilmelidir. Bulut yönetim arayüzü üzerinden işlem yapmak için IPSec veya SSL VPN geçidi kullanılmalı ve bulut yönetim arayüzüne erişim sadece bu kanallardan yapılmalıdır.
4.3.1.8	1	Sanal Makineye Ait Disk Bölgelerinin İmhası	Bulut hizmeti kapsamında herhangi bir sanal makinenin hizmetinin sonlandırılması durumunda, sanal makinenin bulut bilişim sunucularında bulunan disk bölgeleri otomatik olarak servis sağlayıcı tarafından geri döndürülemeyecek şekilde silinmelidir.
4.3.1.9	1	İş Sürekliliğinin Sağlanması	Bulut bilişim hizmeti sunacak servis sağlayıcı iş sürekliliğini sağlamak amacıyla felaket kurtarma merkezi veya yedekleme mekanizmaları ile ilgili yeterlilikleri kurumun bilgi güvenliği gereksinimlerine uygun olarak sağlamalıdır. Bk. Tedbir Başlık No: 3.1.13
4.3.1.10	1	Erişim Yetkilerinin Yönetiminin Sağlanması	Bulut hizmet sağlayıcısının, hizmet alan kurumun sistemine giriş yapması gerektiğinde önceden belirlenmiş kurum yetkililerinden onay almalıdır. Yetkilendirme süreli olmalı ve sorun giderildiğinde erişim yetkisi kaldırılmalıdır. Hizmet sağlayıcı bu süreçte yapılan tüm işlemleri kayıt altına almalı ve bunları raporlamalıdır. Hizmet sağlayıcının bu süreci sistem üzerinde yönetecek ve raporlayacak özellikleri ve tanımlı süreçleri olmalıdır.
4.3.1.11	1	Hizmetin Sonlandırılması Hususları	Paylaşımlı/bulut ortamdan hizmet sağlayan servis sağlayıcılar hizmetin sonlanması durumunda hizmet alan tarafa ait profil ayarları, hizmet raporları vb. hizmete ilişkin tanımları silmelidir. Bulut sistemlerde barındırılan veriler, kullanımının sonlandırılması durumunda sistemlerden geri getirilemeyecek şekilde silinmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.3.1.12	2	Güvenli Veri Depolama Politikasının Uygulanması	Bulut bilişim hizmeti sunacak servis sağlayıcının veri güvenliğini (ifşa, değiştirme, bozulma vb. durumlara karşı) sağlamak adına güvenli veri depolama politikası bulunmalıdır.
4.3.1.13	2	Bulut Ortamı İşlem Kayıtlarının Tutulması	Bulut sistemlerde gerçekleştirilen yönetimsel işlemler kayıt altına alınmalı ve değişmezliği sağlanmalıdır. Bk. Tedbir No: 3.1.8.1
4.3.1.14	3	Kaynakların Fiziksel Olarak İzole Edilmesi	Bulut sistemler üzerinde kuruma ait kritik veri bulundurulacaksa, kritik veriler kurum dışı başka kaynaklar ile aynı fiziksel cihaz üzerinde bulundurulmamalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.3.1.1	Bulut Hizmeti Kullanımı	Mülakat, Gözden Geçirme	Kuruma ait hangi veriler bulut sistemler üzerinde tutulmaktadır? Bulut hizmet sağlayıcı tarafından kuruma hangi kontroller sağlanmaktadır?
4.3.1.2	Hizmet Kapsamı ile Rol ve Sorumlulukların Belirlenmesi	Mülakat, Gözden Geçirme	Bulut bilişim hizmeti kapsamında, hizmet alınan taraf ile hizmet alan kurum arasında, karşılıklı yükümlülükleri ve gizlilik maddelerini içeren bir sözleşme var mıdır? Sözleşme içeriği, geçerlilik süresi boyunca düzenli olarak gözden geçirilmekte midir?
4.3.1.3	Veri İletimi Güvenliği	Mülakat, Güvenlik Denetimi	Bulut bilişim kapsamında çalışan sistemler arasındaki veri trafiği için hangi şifreli iletim protokolü kullanılmaktadır? Bulut ortamından kuruma yönelik trafiğe izin verilmekte midir?
4.3.1.4	Kaynakların İzole Edilmesi	Mülakat, Güvenlik Denetimi	Aynı bulut ortamını kullanan kurumların sistemleri birbirlerinden mantıksal ve/veya fiziksel olarak izole edilmekte midir?
4.3.1.5	İmajların İmha Edilmesi	Mülakat, Güvenlik Denetimi	Bulut hizmeti kapsamında, ihtiyaç olması durumunda şablon olarak kullanılan imajlar geri döndürülemeyecek şekilde silinebilmekte midir?
4.3.1.6	Sanal Makineye Ait Belleklerin İmhası	Mülakat, Güvenlik Denetimi	Herhangi bir sanal makine hizmetinin sonlandırılması ile birlikte, sanal makinenin bulut bilişim sunucularında bulunan bellek bölgeleri servis sağlayıcı tarafından geri döndürülemeyecek şekilde otomatik olarak silinmekte midir?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.3.1.7	Bulut Ortamı Güvenliği	Mülakat, Güvenlik Denetimi, Sızma Testi	Bulut ortamı internet güvenliğine yönelik hangi uygulamalar devrededir? Alınan bulut hizmetlerinde varlık gruplarının kritiklik derecesine uygun güvenlik tedbirlerinin tesis edildiği kontrol edilmekte midir? Hizmet alınan servis sağlayıcı kendi kaynaklarını DDoS saldırılarına karşı nasıl koruyabilmektedir, yüksek boyutlu DDoS saldırılarına karşı iş ve hizmet sürekliliğini nasıl sağlanmaktadır? Hizmet alan taraf ile imzalanan sözleşme ve taahhütlerde bu husus nasıl yer almaktadır? Hizmet alınan servis sağlayıcı, herhangi bir hizmet alanına gelen bir siber saldırıdan (servis dışı bırakma, zararlı yazılım vb.) veya saldırının sistemlerde oluşturabileceği performans problemlerinden diğer hizmet alanların etkilenmemesi için nasıl önlem almışlardır? Hizmet alınan servis sağlayıcıların verdikleri hizmetler ile ilgili hizmet seviye taahhüt koşulları net belirlenmiş, ölçülüyor ve raporlanabiliyor durumda mıdır?
4.3.1.8	Sanal Makineye Ait Disk Bölgelerinin İmhası	Mülakat, Güvenlik Denetimi	Bulut hizmeti kapsamında herhangi bir sanal makinenin hizmetinin sonlandırılması durumunda, sanal makinenin bulut bilişim sunucularında bulunan disk bölgeleri otomatik olarak servis sağlayıcı tarafından geri döndürülemeyecek şekilde silinmekte midir?
4.3.1.9	İş Sürekliliğinin Sağlanması	Mülakat, Gözden Geçirme	Bulut bilişim hizmeti sunan servis sağlayıcı iş sürekliliğini sağlamak amacıyla hangi kontrolleri uygulamaktadır? Uygulanan kontroller kurumun bilgi güvenliği gereksinimleri ile örtüşmekte midir?
4.3.1.10	Erişim Yetkilerinin Yönetiminin Sağlanması	Mülakat, Gözden Geçirme	Bulut hizmet sağlayıcısının, hizmet alan kurumun sistemine giriş yapması gerektiği durumlarda kurum tarafında onay alınması gereken yetkililer belirlenmiş midir? Bulut hizmet sağlayıcısı tarafından kurum sistemine erişilmesi durumunda gerçekleştirilen tüm işlemler kayıt altına alınmakta mıdır? Alınan kayıtlara ilişkin bir rapor oluşturularak kurum ile paylaşılmakta mıdır?
4.3.1.11	Hizmetin Sonlandırılması Hususları	Mülakat, Gözden Geçirme	Bulut hizmet sağlayıcıdan alınan hizmetin sonlandırılması durumunda kuruma ait veriler sistemlerden geri getirilemeyecek şekilde silinmekte midir? Güvenli silme işlemi için hangi yöntemler kullanılmaktadır? Bulut hizmet sağlayıcıdan alınan hizmetin sonlanması durumunda kuruma ait profil ayarları, hizmet raporları vb. bilgilerin hizmet sağlayıcı tarafından silindiği garanti altına alınmakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.3.1.12	Güvenli Veri Depolama Politikasının Uygulanması	Mülakat, Gözden Geçirme	Bulut bilişim hizmet sağlayıcı tarafından güvenli veri depolama politikası hazırlanmış mıdır? Politika düzenli olarak gözden geçirilmekte midir? Politikanın ihlali durumunda hangi prosedür işletilmektedir?
4.3.1.13	Bulut Ortamı İşlem Kayıtlarının Tutulması	Mülakat, Gözden Geçirme	Bulut sistemler üzerinde gerçekleştirilen işlemler kayıt altına alınmakta mıdır? Kayıtların bütünlüğünü sağlamaya yönelik hangi kontroller uygulanmaktadır?
4.3.1.14	Kaynakların Fiziksel Olarak İzole Edilmesi	Mülakat, Gözden Geçirme	Bulut sistemler üzerinde tutulan kuruma ait kritik verilerin kurum dışı başka varlıklar ile aynı fiziksel cihazda bulundurulmaması garanti altına alınmakta mıdır?

4.4. Kripto Uygulamaları Güvenliği

Amaç

Bu güvenlik tedbiri ana başlığının amacı, kripto uygulamaları güvenliği çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. “Kripto Uygulamaları Güvenliği” ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Kriptografik Algoritmalar ve Kullanımı
- Şifreleme ve Anahtar Yönetimi
- Kriptografik Uygulamalar

4.4.1. Kriptografik Algoritmalar ve Kullanımı

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.4.1.1	1	Kriptografik Algoritma Tipinin Seçilmesi	Kriptografik algoritma seçimi; algoritma kullanım amacı, algoritmayı kullanacak taraflar ve bu kapsamda işlenecek bilgi/verinin kritiklik seviyesi göz önünde bulundurularak yapılmalıdır.
4.4.1.2	1	Kripto Uygulama, Cihaz ve Sistemlerin Kriptografik Algoritma Güvenliği	Kurum bünyesinde, standartlaştırılmış ve güvenli kriptografik algoritma takımında yer alan algoritmaları barındıran uygulama, cihaz ve sistemler kullanılmalıdır. Standartlaştırılmış ve güvenli kriptografik algoritmalara yönelik endüstri standartları ve en iyi uygulama örnekleri dikkate alınmalıdır. Standartlaştırılmış kriptografik algoritma takımında yer almayan kriptografik algoritmaların kullanımının gerekmesi durumunda kullanım öncesinde, yetkilendirilmiş kripto analiz laboratuvarı tarafından yeterli güvenlik seviyesinde olup olmadıklarının analizi ve değerlendirilmesi yapılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.4.1.3	1	Standart Kriptografik Algoritmaları İçeren Kripto Modüllerinin Güvenliği	Kullanılacak standart kriptografik algoritmaları içeren kripto modüllerinin uygun güvenlik hedefi veya koruma profili olan Ortak Kriterlere ve/veya TS ISO/EC 19790 – 24759 standardına uygunluğu yetkili laboratuvarlarca test edilmelidir. Bu testler sonucunda, kurum varlıklarının kritiklik derecesine uygun kripto modüller kullanılmalıdır.
4.4.1.4	3	Milli Kriptografik Algoritmaların Gerçeklendiği Kripto Cihazlarının Tedariki	Kritik bilgi/veri işleyen kurumların, kritiklik seviyesine uygun tipte milli kriptografik algoritmaların gerçeklendiği cihazlar temin edilmelidir. Yetkili kripto analiz laboratuvarından güvenli şekilde kullanılabileceğine dair kripto analiz raporu bulunan milli kriptografik algoritmaların donanımsal olarak gerçeklendiği bu kripto cihazların, yetkili laboratuvar tarafından yapılan COMSEC güvenlik testlerinden başarılı bir şekilde geçmiş olmaları gerekmektedir. COMSEC güvenlik testlerine tabi tutulan kripto modüller için Ortak Kriter ve/veya TS ISO/EC 19790 – 24759 standardına uyum gerekliliği bulunmamaktadır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.4.1.1	Kriptografik Algoritma Tipinin Seçilmesi	Mülakat, Gözden Geçirme	Kriptografik algoritma seçimi nasıl yapılmaktadır? Kriptografik algoritma seçiminde varlık grubuna ait kritiklik derecesi, kullanım amacı ve kullanım ortamı gereksinimleri dikkate alınmakta mıdır?
4.4.1.2	Kripto Uygulama, Cihaz ve Sistemlerin Kriptografik Algoritma Güvenliği	Mülakat, Gözden Geçirme	Kripto uygulama, cihaz ve sistemler tarafından kullanılan kriptografik algoritmalar standartlaştırılmış kriptografik algoritma takımında yer almakta mıdır? Standartlaştırılmış kriptografik algoritma takımında yer almayan kriptografik algoritmaların kullanılmadan önce yetkilendirilmiş kripto analiz laboratuvarı tarafından analiz ve değerlendirme işlemleri yapılmakta mıdır? Kripto algoritmalarının güvenlik seviyeleri düzenli aralıklarla gözden geçirilmekte midir?
4.4.1.3	Standart Kriptografik Algoritmaları İçeren Kripto Modüllerinin Güvenliği	Mülakat, Gözden Geçirme	Kullanılan kriptografik sistemde standart kriptografik algoritmaları içeren kripto modüllerinin güvenliği Ortak Kriter ve/veya TS ISO/IEC 19790-24759 onaylı mıdır?
4.4.1.4	Milli Kriptografik Algoritmaların Gerçeklendiği Kripto Cihazlarının Tedariki	Mülakat, Gözden Geçirme	Milli kriptografik algoritmalar, milli üreticilerden tedarik edilen cihazlarda mı gerçeklenmiştir? Yetkili kripto analiz laboratuvarı tarafından hazırlanan, ilgili cihazlarda kullanılan milli kriptografik algoritmaların güvenli bir şekilde kullanılabileceğine dair kripto analiz raporu bulunmaktadır? Bu algoritmaların gerçeklendiği kriptografik cihazlar, yetkili COMSEC laboratuvarı tarafından uygulanan güvenlik testlerinden başarılı bir şekilde geçmiş midir?

4.4.2. Şifreleme ve Anahtar Yönetimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.4.2.1	1	Kriptografik Anahtara İlişkin Güvenlik Gereksinimleri Analizi	Kriptografik anahtarlar üretilirken; kullanım amacına uygun, bilgi güvenliği gereksinimlerini karşılayacak seviyede, ulusal ve uluslararası düzeyde kabul görmüş anahtar uzunlukları kullanılmalıdır. Anahtar uzunlukları, bilgi güvenliği gereksinimleri doğrultusunda endüstri standartları ve en iyi uygulama örnekleri dikkate alınarak belirlenmelidir.
4.4.2.2	1	Kriptografik Anahtarların Üretilmesi	Anahtar üretim aşamasında, anahtarın tahmin edilebilir olmasını engellemek için anahtarın entropisinin anahtar boyundan daha düşük olmaması sağlanmalıdır. Üretim esnasında ulusal ve/veya uluslararası standartlar kapsamında kabul görmüş ve yetkili test ve değerlendirme merkezi tarafından güvenlik testleri yapılmış bir gerçek rassal sayı üreteci "True Random Number Generator (TRNG)" veya sanki rassal sayı üreteci "Pseudo Random Number Generator" kullanılmalıdır.
4.4.2.3	1	Anahtar Üretim ve Dağıtım Cihazlarına Erişim	Anahtar üretim ve dağıtım cihazlarının bulunduğu fiziksel ve elektronik ortamlara yalnızca erişim yetkisi olan tarafların erişimi mümkün kılınmalıdır. Tüm işlemlerin kayıtları alınmalı ve bu kayıtlar uygun güvenlik seviyesiyle korunmalıdır.
4.4.2.4	1	Güvenli Yedekleme	Anahtarın yedeğinin alındığı fiziksel ve elektronik ortamların güvenliği sağlanmalıdır. Tüm işlemlerin kayıtları alınmalı ve bu kayıtlar uygun güvenlik seviyesiyle korunmalıdır.
4.4.2.5	1	Kriptografik Anahtarlara Erişim Kontrolü	Kriptografik anahtarlara erişim sadece kullanım amacına özel olarak erişim yetkisi tanımlanmış personel ile sınırlandırılmalıdır. Tüm işlemlerin kayıtları alınmalı ve bu kayıtlar uygun güvenlik seviyesiyle korunmalıdır.
4.4.2.6	1	Kriptografik Anahtarların Revize Edilmesi	Kriptografik anahtarlar aşağıdaki maddelerin herhangi birisinin ortaya çıkması durumunda revize edilmelidir: • Kriptografik anahtar ile ilgili herhangi bir zafiyet durumu oluşması ya da zafiyet şüphesinin olması • Kriptografik anahtarlara erişim yetkisi olan personelin kurumdan ayrılması veya görev değiştirmesi • Kriptografik anahtarların, kullanım periyodunun tamamlanması ile birlikte geçerlilik sürelerinin dolması

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.4.2.7	1	Güvenli Anahtar Ulaştırma / İletimi	Anahtar dağıtım protokolünün analiz edilerek güvenli olması sağlanmalıdır. Gizli kriptografik anahtar bir ağ ortamından iletilecek ise trafik iki uç arasında şifreli ve araya girme saldırılarına karşı korumalı olmalıdır. Ayrıca, trafiğin şifrelemesi taşınan anahtarın gizlilik seviyesi ile uyumlu olmalıdır. Kullanım amacı ve içerdiği bilgi/verinin kritiklik derecesine göre anahtarın birden fazla parçaya ayrılarak farklı kanallarla iletilmesi sağlanmalıdır. Kriptografik anahtar dijital bir kanal ile iletilmiş ise iletilen anahtarın bütünlük kontrolü yapılmalı ve iletilen anahtarın orijinal anahtar ile aynı olduğu doğrulanmalıdır. Dijital kanal açık bir kanalsa, anahtarın şifrelenmesi de sağlanmalıdır. Anahtar dağıtımı ve üretimi için uygun görüldüğü durumlarda HSM tabanlı bir teknoloji tercih edilerek yukarıda bahsi geçen gereksinimler HSM aracılığı ile sağlanmalıdır. Bu durumda, HSM sistemi uygun şekilde yapılandırılmalı ve erişimleri kontrol altına alınmalıdır.
4.4.2.8	1	Anahtar Taşıma Cihazlarının Muhafazası ve Cihaza Erişim	Anahtar taşıma cihazları güvenli alanlarda muhafaza edilmelidir. Anahtar taşıma cihazlarına ve depolama medyasına sadece yetkilendirilmiş personelin ulaşabilmesi sağlanmalıdır. Tüm erişim kayıtları tutularak takibinin yapılması sağlanmalıdır.
4.4.2.9	1	Anahtar Üretim Ortamlarına Güvenli Erişim	Anahtar üretim ortamlarına erişim HTTPS, SSH gibi şifreleme desteği sunan protokoller kullanılarak yapılmalıdır.
4.4.2.10	1	İz Kayıtlarının Oluşturulması	Yasal yükümlülükleri yerine getirmek, şüpheli davranışları tespit etmek ve güvenlik ihlali durumunda adli soruşturma yetenekleri sağlamak için anahtarlar üzerinde gerçekleştirilen yetkilendirme, yetki değişikliği, iptal etme, silme, yedekleme vb. tüm işlemler kayıt altına alınmalıdır. Bk. Tedbir No: 3.1.8.1
4.4.2.11	1	Kriptografik Anahtarların İptal Edilmesi/Güvenli Yok Edilmesi	Kriptografik anahtarlar, kabul edilebilir sınırlı bir geçerlilik süresine ve/veya kullanım sayısına sahip olmalıdır. Yaşam süresi devam ederken kaybedilen ve/veya saldırgan tarafından kısmen ya da tamamen ele geçirilen bir kriptografik anahtarın iptal işlemi gerçekleştirilmelidir. Yetkisini yitirmiş kriptografik anahtar ve/veya akıllı kart, token vb. kriptografik anahtar ihtiva eden donanımlar geri dönülemez biçimde yok edilmelidir.
4.4.2.12	1	Kriptografik Anahtar Sorumlusu Zimmet Tutanağının Hazırlanması	Anahtar dağıtım ve teslim şeklinin imkân vermesi durumunda kriptografik anahtarların sadece gerekli ve geçerli iş amaçları için kullanılacağını, kriptografik anahtarlar ile yapılmış olan tüm işlemlerin sorumluluğunun kişiye ait olduğunu vurgulayan bir zimmet tutanağının hazırlanmalı, kriptografik anahtarların zimmetlendiği personele imzalatılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.4.2.13	1	Kriptografik Anahtar Yetkilendirme	Üretilen anahtarların kullanım kabiliyetleri (şifreleme, şifre çözme, imzalama, doğrulama vb.) dokümante edilmeli ve yetkilendirme bu doğrultuda yapılmalıdır.
4.4.2.14	1	Anahtarların Üretim Yerinden Sonra Kopyalanamaması ve Çoğaltılamaması	Anahtarların üretim yerinden sonra kontrolsüz şekilde kopyalanması ve çoğaltılması engellenmelidir. Anahtar kaç kopya üretildi ise o sayıda dağıtım ve kullanım sağlanmalıdır.
4.4.2.15	1	Anahtarlara Açık Metin Olarak Erişilmemesi	Anahtar malzemesi elektronik ortamda tutulduğu veri tabanında veya yayımlandığı taşıma ortamlarında açık olarak görülememelidir. (Anahtarı kullanan cihazlara aktarımın kâğıt üzerinde olması durumu kapsam dışıdır.) Açık anahtar görülmesi ihlal kapsamında değerlendirilmelidir ve anahtar kullanımdan çıkarılmalıdır.
4.4.2.16	1	İhlal Raporlama	Anahtarların ifşa olması ve anahtar kullanım süreçlerindeki ihlal durumlarını raporlama (compromise reporting) mekanizması kurulmalıdır.
4.4.2.17	1	Yedek Anahtar	Anahtar üretim ve dağıtımın hızlı olamadığı uygulamalarda, ihlal/ifşa durumlarında kullanılmak üzere yedek anahtarlar hazırlanmalıdır.
4.4.2.18	1	Anahtar Üretim ve Yönetim Sistemi Testi	Kullanılacak anahtar üretim ve yönetim sistemleri ile kripto cihazların yerli ve milli üreticilerden temini tercih edilmelidir. Kullanılacak anahtar üretim ve yönetim sisteminin uygun güvenlik hedefi veya koruma profili olan Ortak Kriterlere ve/veya TS ISO/IEC 19790 – 24759 standardına uygunluğu yetkili laboratuvarlarca test edilmelidir. Bu testler sonucunda, kurum varlıklarının kritiklik derecesine uygun kripto modüller kullanılmalıdır.
4.4.2.19	2	Güvenli Anahtar Saklama	Kriptografik anahtar şifreleme anahtarları ile veri şifreleme anahtarları birbirlerinden izole edilmiş ortamlarda saklanmalıdır. Her iki özellikteki anahtar da dışarıdan yapılabilecek müdahaleye karşı korunmuş modüllerde (TRSM) saklanmalıdır. Bu mümkün değilse bilgiyi parçalı olarak korumak gereklidir. Parçalı koruma işleminde parçalar ayrı yerlerde tutulmalı, bilgi kullanılacağı zaman bir araya gelmesi sağlanmalıdır. Üretilen anahtarlar özellikle güvenli saklama için tasarlanmış USB token, akıllı kart vb. teknolojilerde saklanmalıdır. Eğer yazılımsal token vb. bir teknoloji kullanılacak ise ilave olarak hard tokenda fiziksel olarak sağlanan sahip olma özelliğinin, kişinin bilgisayar, tablet vb. da sağlanması gerekmektedir. Soft token siber saldırılara karşı dayanıklı olmalı ve gizli anahtarı sızdırmamalıdır.
4.4.2.20	3	Anahtar Taşıma Cihazlarında Yapılan Tüm Anahtar İşlemlerinin Kaydının Tutulması	Anahtar taşıma cihazlarında yalnızca anahtar alma ve yayımlama yetkisi olan personel işlem yapabilmelidir. Yapılan tüm işlemler anahtar bilgisi ve işlemi gerçekleştiren kullanıcı ile birlikte kayıt altına alınmalıdır. Kayıtlar uygun şekilde korunmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.4.2.21	3	Anahtar Taşıma Cihazlarında Bulunan Anahtarın Onaylı Kriptografik Yöntemlerle Şifreli Olarak Tutulması	Anahtar taşıma cihazlarında bulunan anahtarlar bellek gölgesinde öznitelikleri listelenerek ulaşılacak şekilde, onaylı kriptografik yöntemlerle şifreli olarak tutulmalıdır ve sadece yüklenirken açılmalıdır.
4.4.2.22	3	Anahtar Alma ve Depolama İşlemlerinde Bütünlük Hatası Oluşması Durumunda Anahtar Malzemesinin İmha Edilmesi	Anahtar alma işleminde bütünlük hatası tespit edilirse veya depolanan anahtarda bütünlük hatası oluşması durumunda anahtar malzemesi hemen imha edilmeli ve işlem kayıt altına alınmalıdır.
4.4.2.23	3	Kripto Güvenlik Belgesi Kontrolü	Kriptografik anahtarlara erişim sadece yetki sahibi kleranslı (kripto güvenlik belgesi) personel ile sınırlanlandırılmalıdır.
4.4.2.24	3	Anahtar Kimliği	Anahtarlar mümkünse tekil olarak adreslenebilir olmalıdır. Örneğin, anahtarların üzerinde veya yanlarında kimlik bilgisi bulunmalıdır. Anahtarın kimliği kullanılarak, alınan kayıtlar üzerinden anahtarın geçmişine ulaşılabilmelidir.
4.4.2.25	3	Anahtar Sayımı	Planlı veya plansız olarak anahtar sayımı yapılmalıdır.
4.4.2.26	3	Anahtar Üretim ve Yönetim Sistemi Testi	Anahtar üretim ve yönetim sistemleri için kullanılacak kripto cihazlar milli üreticilerden temin edilmelidir. Kripto cihazların kullanımı öncesinde, yetkili kripto analiz laboratuvarı tarafından COMSEC güvenlik testleri yapılmalı ve test sonuçlarının onaylanması durumunda kullanıma alınmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.4.2.1	Kriptografik Anahtara İlişkin Güvenlik Gereksinimleri Analizi	Mülakat, Gözden Geçirme	Kriptografik anahtarlar; kullanım amacına uygun güvenlik gereksinimlerini karşılayacak şekilde, ulusal ve uluslararası düzeyde kabul görmüş anahtar uzunlukları kullanılarak mı üretilmektedir?
4.4.2.2	Kriptografik Anahtarların Üretilmesi	Mülakat, Gözden Geçirme	Anahtar üretim aşamasında, anahtarın tahmin edilebilir olmasını engellemek için hangi kontroller uygulanmaktadır? Anahtar üretilirken kullanılan TRNG ve/veya PRNG ulusal ve/veya uluslararası standartları sağlamakta olan, testleri (COMSEC veya ISO) ulusal bir laboratuvarda yapılmış bir cihaz mıdır?
4.4.2.3	Anahtar Üretim ve Dağıtım Cihazlarına Erişim	Mülakat, Gözden Geçirme	Anahtar üretim ve dağıtım cihazları fiziksel tedbirler alınmış yalnızca yetkili kişilerin girebildiği korumalı alanda tutulmakta mıdır?
4.4.2.4	Güvenli Yedekleme	Mülakat, Gözden Geçirme	Sayısal sertifika ve anahtarın yedeğinin alındığı ortamlar nasıl korunmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.4.2.5	Kriptografik Anahtarlara Erişim Kontrolü	Mülakat, Gözden Geçirme	Kriptografik anahtarlara erişim yetkileri nasıl verilmektedir?
4.4.2.6	Kriptografik Anahtarların Revize Edilmesi	Mülakat, Gözden Geçirme	Anahtarlara erişim yetkisi olan personelin kurumdan ayrılması veya görev değiştirmesi durumunda nasıl bir yol izlenmektedir?
4.4.2.7	Güvenli Anahtar Ulaştırma / İletimi	Mülakat, Güvenlik Denetimi	Gizli kriptografik anahtar bir ağ ortamından iletilecek ise bu iletim aşamasının güvenli gerçekleştirildiğine yönelik ne gibi önlemler alınmaktadır? Kriptografik anahtarın fiziksel olarak ulaştırılması esnasında alınan fiziksel güvenlik önlemler nelerdir?
4.4.2.8	Anahtar Taşıma Cihazlarının Muhafazası ve Cihaza Erişim	Mülakat, Güvenlik Denetimi	Anahtar taşıma cihazlarına ve depolama medyasına erişim kontrolü nasıl sağlanmaktadır? Erişim kayıtları tutulmakta mıdır ve bu kayıtların denetimi düzenli aralıklar ile yapılmakta mıdır?
4.4.2.9	Anahtar Üretim Ortamlarına Güvenli Erişim	Mülakat, Güvenlik Denetimi	Üretim ortamlarına erişimde hangi yöntemler kullanılmaktadır?
4.4.2.10	İz Kayıtlarının Oluşturulması	Mülakat, Gözden Geçirme	Kriptografik anahtarlar üzerinde gerçekleştirilen hangi işlemler kayıt altına alınmaktadır?
4.4.2.11	Kriptografik Anahtarların İptal Edilmesi/Güvenli Yok Edilmesi	Mülakat, Gözden Geçirme	Kriptografik anahtarlar için tanımlanmış bir imha periyodu var mıdır? Kriptografik anahtarların gizliliğinin ihlal edildiği durumlarda nasıl bir yöntem uygulanmaktadır?
4.4.2.12	Kriptografik Anahtar Sorumlusu Zimmet Tutanağının Hazırlanması	Mülakat, Gözden Geçirme	Kriptografik anahtarların zimmetlendiği personele sorumluluklarını tanımlayan bir tutanak ya da taahhütname imzalatılmakta mıdır?
4.4.2.13	Kriptografik Anahtar Yetkilendirme	Mülakat, Gözden Geçirme	Üretilen anahtarların kullanım kabiliyetleri dokümante edilmekte midir?
4.4.2.14	Anahtarların Üretim Yerinden Sonra Kopyalanamaması ve Çoğaltılamaması	Mülakat, Gözden Geçirme, Sızma Testi	Anahtarlar üretildikten sonra kopyalama ve çoğaltılmaya karşı önlem olarak hangi kontroller uygulanmaktadır? Dağıtım nasıl gerçekleştirilmektedir? Anahtar dağıtım kontrol süreçleri belirlenmiş midir?
4.4.2.15	Anahtarlara Açık Metin Olarak Erişilmemesi	Mülakat, Gözden Geçirme	Elektronik dağıtımı yapılan kripto malzemesinin çıktı alınıp görülebilmesi engellenmiş midir? Yetki ihlali teknik imkânlar la engellenmiş midir? Kaydedilmeyen, yakalanamayan ihlal olasılığı var mıdır?
4.4.2.16	İhlal Raporlama	Mülakat, Gözden Geçirme	Anahtarların ifşa olması ve anahtar süreçlerindeki ihlal durumlarını raporlamak için bir mekanizma bulunmakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.4.2.17	Yedek Anahtar	Mülakat, Gözden Geçirme	Anahtar üretim ve dağıtımın hızlı olamadığı uygulamalarda, ihlal/ifşa durumlarında kullanmak üzere yedek anahtarlar bulunmakta mıdır?
4.4.2.18	Anahtar Üretim ve Yönetim Sistemi Testi	Mülakat, Gözden Geçirme	Anahtar üretim ve yönetim sistemi Ortak Kriterler ve/veya TS ISO/IEC 19790-24759 standardı ile uyumlu mudur?
4.4.2.19	Güvenli Anahtar Saklama	Mülakat, Gözden Geçirme	Kriptografik anahtar şifreleme anahtarları ile veri şifreleme anahtarları saklanırken nasıl bir yöntem izlenmektedir?
4.4.2.20	Anahtar Taşıma Cihazlarında Yapılan Tüm Anahtar İşlemlerinin Kaydının Tutulması	Mülakat, Gözden Geçirme	Anahtar taşıma cihazlarında yetkili kullanıcının yaptığı tüm işlemler kayıt altına alınmakta mıdır? Kayıtlar uygun güvenlik seviyesiyle korunmakta mıdır?
4.4.2.21	Anahtar Taşıma Cihazlarında Bulunan Anahtarın Onaylı Kriptografik Yöntemlerle Şifreli Olarak Tutulması	Mülakat, Gözden Geçirme	Anahtar taşıma cihazlarında bulunan anahtarlar onaylı kriptografik yöntemlerle şifreli olarak tutulmakta mıdır?
4.4.2.22	Anahtar Alma ve Depolama İşlemlerinde Bütünlük Hatası Oluşması Durumunda Anahtar Malzemesinin İmha Edilmesi	Mülakat, Gözden Geçirme	Anahtar alma işleminde bütünlük hatası tespit edilirse veya depolanan anahtarda bütünlük hatası oluşması durumunda nasıl bir yol izlenmektedir?
4.4.2.23	Kripto Güvenlik Belgesi Kontrolü	Mülakat, Gözden Geçirme	Kriptografik anahtarlara erişim yetkisi verilecek personel için kripto güvenlik belgesi kontrolü yapılmakta mıdır?
4.4.2.24	Anahtar Kimliği	Mülakat, Gözden Geçirme	Anahtarlar tekil olarak adreslenmekte ve yaşam çevrim aşamaları takip edilmekte midir?
4.4.2.25	Anahtar Sayımı	Mülakat, Gözden Geçirme	Planlı veya plansız anahtar sayımı yapılmakta mıdır?
4.4.2.26	Anahtar Üretim ve Yönetim Sistemi Testi	Mülakat, Gözden Geçirme	Anahtar üretim ve yönetim sistemi milli üreticilerden temin edilmekte midir? Yetkili kripto analiz laboratuvarı tarafından hazırlanmış, anahtar üretim ve yönetim sisteminin güvenli bir şekilde kullanılabileceğine dair kripto analiz raporu bulunmakta mıdır? Anahtar üretim ve yönetim sistemi, yetkili COMSEC laboratuvarı tarafından uygulanan güvenlik testlerinden başarılı şekilde geçmiş midir?

4.4.3. Kriptografik Uygulamalar

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.4.3.1	1	Güvensiz Ağlar Üzerinden Güvenli Haberleşme	Güvenli ağların, güvensiz bir ağ üzerinden haberleşmesinin gerekmesi durumunda VPN teknolojileri kullanılmalıdır.
4.4.3.2	1	Envanter Yönetimi	Kurumda aktif olarak kullanılan ve aktif olarak kullanılmayan tüm kriptografik ürünlerin güncel bir listesi tutulmalıdır. Liste içeriğinde kullanılan ürünlerin hangi işlemler için hangi amaçla kullanıldıkları tanımlanmalı, envantere yalnızca yetkilendirilmiş personelin erişimi mümkün kılınmalıdır.
4.4.3.3	1	Güvenlik Değerlendirme ve Onay Durumu Yönetimi	Kullanılan kriptografik ürünlerin işlediği verinin gizlilik derecesine uygun olarak kullanılmasını sağlamak amacıyla ilgili güvenlik değerlendirmesi ve gizlilik derecesi ile uyumlu olarak onay sürecinin işletilip işletilmediği kontrol edilmelidir.
4.4.3.4	2	Kripto Protokollerinin En Güncel ve Güvenilir Versiyonlarının Kullanımı	Kriptografik algoritmaların ve protokollerin en güncel ve güvenli olan versiyonlarının kullanımı sağlanmalıdır. Anahtar uzunlukları, bilgi güvenliği gereksinimleri doğrultusunda endüstri standartları ve en iyi uygulama örnekleri dikkate alınarak belirlenmelidir. Sistemde kullanılan taşıma katmanı protokollerine ait sürümler belirli aralıklarla değerlendirilmeli ve denetlenmelidir.
4.4.3.5	2	Envanter Yönetim Araçları ile Kriptografik Ürünlerin Yönetimi ve İzlenmesi	Kullanılan kriptografik ürünlerin kullanım durumları, versiyon kontrolü, güvenlik değerlendirmesi ve onay durumu gibi bilgilerin takibi ve raporlaması envanter yönetim sistemi ile yapılmalıdır. Envanter yönetim sistemine yalnızca yetkilendirilmiş personelin erişimi mümkün kılınmalıdır.
4.4.3.6	3	Kripto Cihazları TEMPEST Laboratuvar Onayı	Kritik bilgi/veri işleyen kurumlarda, bu bilgilerin işlenmesinde kullanılan kriptografik sistemler için kullanılan kripto cihazlarının TEMPEST testlerinin yapılmalıdır.
4.4.3.7	3	Kripto Cihazları Kripto Analiz Laboratuvar Onayı	Kritik bilgi/veri işleyen kurumlarda, bu bilgilerin işlenmesinde kullanılan kriptografik ürünlerin yetkili kripto analiz laboratuvarı tarafından kriptografik mimari ve algoritma analizi yapılmalıdır.
4.4.3.8	3	Kripto Cihazları COMSEC Laboratuvar Onayı	Kritik bilgi/veri işleyen kurumlarda, bu bilgilerin işlenmesinde kullanılan kriptografik ürünlere ait (milli veya standart algoritma içeren) kriptografik algoritmaların kullanacakları anahtarları üretecek, taşıyacak ve kullanacak sistem ve cihazlar, yetkili COMSEC laboratuvarında gerekli testlerden geçmeli ve güvenlik onayı almalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.4.3.1	Güvensiz Ağlar Üzerinden Güvenli Haberleşme	Mülakat, Güvenlik Denetimi	Güvenli ağların, güvensiz bir ağ üzerinden haberleşmesinin gerekmesi durumunda nasıl bir yöntem izlenmektedir?
4.4.3.2	Envanter Yönetimi	Mülakat, Gözden Geçirme	Kurumda kullanılan kriptografik ürünlerin envanteri tutulmakta mıdır? Envanter kapsamında hangi bilgiler yer almaktadır? Envanter nerede tutulmaktadır? Envantere erişim yetkileri düzenli aralıklar ile gözden geçirilmekte midir?
4.4.3.3	Güvenlik Değerlendirme ve Onay Durumu Yönetimi	Mülakat, Güvenlik Denetimi	Kurum tarafından hangi kriptografik ürünler kullanılmaktadır? Kullanılan kriptografik ürünler hangi gizlilik seviyelerinde veri işlemektedir? Kullanılan kriptografik ürünlere yönelik yapılan güvenlik değerlendirmeleri nelerdir? Kriptografik ürünlere yönelik hangi sertifikalar bulunmaktadır? Kriptografik ürünlerin işledikleri verilerin gizlilik seviyesine uygun olarak gerekli güvenlik değerlendirmeleri yapılmış ve ilgili onaylar alınmış mıdır?
4.4.3.4	Kripto Protokollerinin En Güncel ve Güvenilir Versiyonlarının Kullanımı	Mülakat, Güvenlik Denetimi	Güncel ve güvenilir kriptolama algoritmalarının kullanıldığı nasıl kontrol edilmektedir? Kriptografik protokollerin güvenli sürümleri desteklenmekte midir? Kriptografik protokollerin eski sürümleri ile yapılan iletişim istekleri reddedilmekte midir?
4.4.3.5	Envanter Yönetim Araçları ile Kriptografik Ürünlerin Yönetimi ve İzlenmesi	Mülakat, Gözden Geçirme	Envanter yönetimi amacıyla hangi araç kullanılmaktadır? Envantere hangi personel erişim sağlamaktadır?
4.4.3.6	Kripto Cihazları TEMPEST Laboratuvar Onayı	Mülakat, Güvenlik Denetimi	Kriptografik sistemler için kullanılan kripto cihazlarının TEMPEST testleri yapılmakta mıdır?
4.4.3.7	Kripto Cihazları Kripto Analiz Laboratuvar Onayı	Mülakat, Güvenlik Denetimi	Kriptografik sistemler için kriptografik mimari ve algoritma analizi yapılmış mıdır?
4.3.8	Kripto Cihazları COMSEC Laboratuvar Onayı	Mülakat, Güvenlik Denetimi	Kriptografik algoritmaların kullanacakları anahtarları üretecek, taşıyacak ve kullanacak sistemin kullanımı öncesinde; sistem, yetkili bir COMSEC laboratuvarında gerekli testlerden geçirilip güvenlik onayı alınmış mıdır?

4.5. Kritik Altyapılar Güvenliği

Amaç

Bu güvenlik tedbiri ana başlığının amacı, kritik altyapılar güvenliği çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. "Kritik Altyapılar Güvenliği" ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Genel Güvenlik Tedbirleri
- Enerji Sektörü Özelinde Güvenlik Tedbirleri
- Elektronik Haberleşme Sektörü Özelinde Güvenlik Tedbirleri

Kritik altyapılar güvenliği kapsamında uygulanacak enerji ve elektronik haberleşme sektörü özelindeki güvenlik tedbirlerinin yanı sıra varlık gruplarına yönelik güvenlik tedbirlerinin yer aldığı alt başlıklar da dikkate alınmalıdır.

4.5.1. Genel Güvenlik Tedbirleri

Tedbirler

Aşağıda listelenen rehber ana başlıklarında yer alan tedbirler uygulanır:

- Ağ ve Sistem Güvenliği
- Uygulama ve Veri Güvenliği
- Taşınabilir Cihaz ve Ortam Güvenliği
- Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği
- Personel Güvenliği
- Fiziksel Mekânların Güvenliği

Denetim Maddeleri

Aşağıda listelenen rehber ana başlıklarında yer alan denetim soru önerileri uygulanır:

- Ağ ve Sistem Güvenliği
- Uygulama ve Veri Güvenliği
- Taşınabilir Cihaz ve Ortam Güvenliği
- Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği
- Personel Güvenliği
- Fiziksel Mekânların Güvenliği

4.5.2. Enerji Sektörü Özelinde Güvenlik Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.5.2.1	1	Cihaz Konfigürasyonları	EKS içerisinde yer alan hiçbir cihaz varsayılan ayarlarıyla sistem içerisinde konumlandırılmamalıdır. Cihaz konfigürasyonları bilgi güvenliği gereksinimlerine uygun olarak yapılmalıdır.
4.5.2.2	1	Ağ Erişim Kontrolü	EKS ağı ve kurumsal BT ağı arasındaki iletişimler için erişim kontrolü sağlanmalı ve yetkisiz erişimler engellenmelidir.
4.5.2.3	1	Ağ Segmentasyonu	Operasyonel faaliyetlerin kritikliği değerlendirilmeli ve EKS ağı belirlenen kritiklik derecesine göre segmentlere ayrılmalıdır. Oluşturulan ağlar birbirlerinden izole edilmeli ve erişim güvenliğine yönelik kısıtlayıcı önlemler alınmalıdır.
4.5.2.4	1	Kimlik Doğrulama	EKS kullanıcıları ve kurum ağı kullanıcıları için ayrı kimlik doğrulama sistemi kullanılmalıdır.
4.5.2.5	1	Erişim Yönetimi	EKS ağı internete kapalı konumda tutulmalıdır. Söz konusu sistemlerin internete açık olmasının zorunlu olduğu durumlarda ise internet ve uzaktan erişim faaliyetlerine güvenlik güncellemeleri ve sıkılaştırma politikaları uygulanarak asgari seviyede izin verilmelidir.
4.5.2.6	1	Fiziksel Erişim Güvenliği	EKS ortamındaki herhangi bir bilgi varlığına, yetkisiz kişiler tarafından yapılacak aktif (hırsızlık, modifikasyon, manipülasyon) veya pasif (görsel gözlem, not alma, fotoğraf çekme) fiziksel erişimi sınırlamak amacıyla sistemlerin bulunduğu ortamlara erişimde; • Çok faktörlü kimlik doğrulama, • Kamera ve/veya hareket dedektörleri kullanımı • Ziyaretçi kabul kuralları için süreç tanımlanması ve uygulanması • Cihaz manipülasyonu için alarm mekanizmaları gibi güvenlik önlemleri alınmalıdır.
4.5.2.7	1	Sistem Sürekliliğinin Sağlanması	EKS sistem sürekliliğini sağlamak amacıyla sistem mimarisi dağıtık ve/veya yedekli bir yapıda oluşturulmalıdır.
4.5.2.8	1	Veri Manipülasyonunun Engellenmesi	EKS ağı pasif olarak (mirror trafik kullanılarak) izlenerek veri manipülasyonunu engellemeye yönelik önlemler alınmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.5.2.9	1	Kullanıcı Erişim Yönetimi	IED ve RTU cihazlarında hizmet veren web sunucusu olması durumunda, internet üzerinden sunucuya erişim kapatılmalı ve iç ağda kimlik doğrulama mekanizmaları doğrultusunda erişim sağlanmalıdır. Sunucuya internet üzerinden erişime ihtiyaç olduğu durumlarda VPN üzerinden erişim sağlanmalıdır. MMS protokolünde kimlik doğrulama özelliği aktif bir şekilde kullanılmalıdır.
4.5.2.10	1	SSL/TLS Korumalı İletişim	EKS ağındaki MMS protokolü ile sağlanan dikey iletişim, SSL/TLS üzerinden şifreli bir şekilde sağlanmalı, IED'lerde ve HMI/SCADA cihazlarında desteklenmesi durumunda SSL/TLS özelliği aktif hale getirilmelidir.
4.5.2.11	1	GPS İletişim ve Senkronizasyonunun Güvenliği	Enerji alt yapılarında kullanılan GPS teknolojileri spoofing saldırılarına karşı korunmalıdır.
4.5.2.12	1	Ekipman Güvenliğinin Sağlanması	Kullanılan ekipman, çevresel tehditlerden kaynaklanacak olumsuz etkilere karşı gerekli önlemler alınarak korunmalıdır.
4.5.2.13	1	Tehdit İstihbaratı Yönetimi	Siber güvenlik tehdit istihbaratı ile ilgili güncel ve güvenilir bilgiyi almak için gerekli tehdit istihbaratı çalışmaları yapılmalı ve tehdit istihbaratı verilerini yönetmek amacıyla bir süreç/mekanizma tanımlanmalıdır.
4.5.2.14	1	Otoritelerle İletişim	Tehdit yönetim faaliyetlerini destekleyecek otoritelere ilişkin iletişim listesi tanımlanmalıdır.
4.5.2.15	2	Veri İletimi	Ağ üzerindeki verilerin iletimi için güvenli aktarım yöntemleri (hava boşluğu, veri diyodu vb.) kullanılmalıdır. Bk. Tedbir No: 3.1.6.36

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.5.2.1	Cihaz Konfigürasyonları	Mülakat, Güvenlik Denetimi	EKS içerisinde yer alan tüm cihazların konfigürasyonları bilgi güvenliği gereksinimleri göz önünde bulundurularak yapılandırılmakta mıdır?
4.5.2.2	Ağ Erişim Kontrolü	Mülakat, Güvenlik Denetimi	KBS ağı ve EKS ağı doğrudan iletişim kurmakta mıdır? EKS ağı güvenliğini sağlamak amacıyla hangi kontroller uygulanmaktadır?
4.5.2.3	Ağ Segmentasyonu	Mülakat, Güvenlik Denetimi	Operasyonel faaliyetler göz önünde bulundurularak EKS ağı segmentlere ayrılmış mıdır? Segmentler arası erişim güvenliği nasıl sağlanmaktadır?
4.5.2.4	Kimlik Doğrulama	Mülakat, Güvenlik Denetimi	EKS kullanıcıları kapsamında kimlik doğrulama nasıl yapılmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.5.2.5	Erişim Yönetimi	Mülakat, Güvenlik Denetimi	EKS ağı internete kapalı mıdır? EKS ağına uzaktan erişim için hangi kontroller uygulanmaktadır?
4.5.2.6	Fiziksel Erişim Güvenliği	Mülakat, Güvenlik Denetimi	EKS ortamındaki herhangi bir bilgi varlığına, yetkisiz kişiler tarafından yapılacak aktif veya pasif fiziksel erişimi sınırlamak amacıyla hangi güvenlik kontrolleri uygulanmaktadır?
4.5.2.7	Sistem Sürekliliğinin Sağlanması	Mülakat, Güvenlik Denetimi	EKS merkezi ile hizmet verilen bölge arasında dağıtık ve/veya yedekli bir sistem mimarisi oluşturulmuş mudur?
4.5.2.8	Veri Manipülasyonunun Engellenmesi	Mülakat, Güvenlik Denetimi	EKS ağı düzenli olarak izlenmekte midir? Veri manipülasyonunu engellemek için hangi kontroller uygulanmaktadır?
4.5.2.9	Kullanıcı Erişim Yönetimi	Mülakat, Güvenlik Denetimi	Kimlik doğrulama mekanizmaları kullanılmakta mıdır? MMS protokolünde kimlik doğrulama mekanizmaları aktif midir?
4.5.2.10	SSL/TLS Korumalı İletişim	Mülakat, Güvenlik Denetimi	Trafo merkezleri içerisindeki MMS protokolü ile sağlanan dikey iletişim, SSL/TLS üzerinden şifreli bir şekilde sağlanmakta mıdır?
4.5.2.11	GPS İletişim ve Senkronizasyonunun Güvenliği	Mülakat, Güvenlik Denetimi	Enerji alt yapılarında kullanılan GPS teknolojileri spoofing saldırılarına karşı nasıl koruma altına alınmaktadır?
4.5.2.12	Ekipman Güvenliğinin Sağlanması	Mülakat, Güvenlik Denetimi	Enerji sektörü özelinde kullanılan ekipmanı çevresel tehditler sebebi ile kaynaklanacak olumsuz etkilere karşı korumak amacıyla hangi önlemler alınmaktadır?
4.5.2.13	Tehdit İstihbaratı Yönetimi	Mülakat, Güvenlik Denetimi	Siber güvenlik tehdit istihbaratı ile ilgili güncel ve güvenilir bilgiyi almak için ne tür çalışmalar yapılmaktadır? Tehdit istihbarat verilerini yönetmek amacıyla bir süreç/mekanizma tanımlanmış mıdır?
4.5.2.14	Otoritelerle İletişim	Mülakat, Güvenlik Denetimi	Tehdit yönetim faaliyetlerini destekleyecek otoritelere ilişkin iletişim listesi tanımlanmış mıdır?
4.5.2.15	Veri İletimi	Mülakat, Güvenlik Denetimi	Ağ üzerindeki verilerin iletimi için hangi güvenli aktarım yöntemleri kullanılmaktadır?

4.5.3. Elektronik Haberleşme Sektörü Özelinde Güvenlik Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.5.3.1	1	Hizmet Güvenliği ve Sürekliliği	Sağlanan iletişim hizmetlerinin güvenliğini ve sürekliliğini ele alan bir güvenlik politikası belirlenmeli ve uygulanmalıdır. Güvenlik politikası; geçmişte yaşanan güvenlik olayları ve ihlalleri, hizmet kesintileri ve sektördeki diğer sağlayıcıları etkileyen olaylar dikkate alınarak periyodik olarak güncellenmelidir. Özellikle kilit personelin belirlenen güvenlik politikasına yönelik farkındalığı arttırılmalıdır.
4.5.3.2	1	Üçüncü Taraflara İlişkin Güvenlik Gereksinimleri	Üçüncü taraflardan temin edilen/hizmet alınan BT ürünlerine, BT hizmetlerine, dış kaynaklı iş süreçlerine, yardım masalarına, çağrı merkezlerine, ara bağlantılara, ortak tesislere vb. yönelik güvenlik gereksinimleri sözleşmelerde detaylı olarak ele alınmalıdır. Bk. Tedbir No: 3.5.3.3
4.5.3.3	1	Altyapı Servislerinin Güvenliği	Haberleşme hizmetlerindeki altyapı servislerinin kötüye kullanımından kaynaklanacak ve müşterileri/diğer hizmet sağlayıcıları olumsuz olarak etkileyebilecek tehditler için gerekli önlemler alınmalıdır.
4.5.3.4	1	Sahtecilik İşlemlerini Tespit ve Önleme	Sinyalleşme trafiğindeki olası sahtecilik işlemlerini tanımlamak, tespit etmek ve önlemek için bir sistem kurulmalı ve işletilmelidir.
4.5.3.5	1	Sinyalleşme Trafiğinin Güvenliği	Sinyalleşme sistem ve protokollerindeki zafiyetler kullanılarak yapılabilecek saldırıların tespiti/önlenmesi amacıyla sinyalleşme trafiği izlenmeli, gizlilik ve bütünlüğünü tesis edecek önlemler alınmalıdır.
4.5.3.6	1	Güvenilir İletişimin Tesisi	Sağlanan iletişim hizmetlerinde müşterilerin kaynak IP adreslerinin doğrulanmasına olanak tanıyan sistemler kullanılmalı, hatalı, değiştirilmiş (spoofed) IP adreslerinin şebekede dolaşımını engellemek için gerekli önlemler alınmalıdır.
4.5.3.7	1	Sıkılaştırma Faaliyetleri	Sunucular, yönlendiriciler ve diğer şebeke elemanlarının saldırı yüzeyini azaltmak için gerekli sıkılaştırma kontrolleri uygulanmalıdır. Bk. Bölüm 5
4.5.3.8	1	Ekipman Arızalarının İzlenmesi	Güvenlik ve iş sürekliliği gereksinimlerini sağlamak amacıyla altyapıda yer alan ekipmanlara ait arıza sinyallerinin izlenmesi için alarm mekanizması kurulmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.5.3.9	1	Ekipman Güvenliğinin Sağlanması	Haberleşme sistemlerinde kullanılan ekipmanı, çevresel tehditler ile enerji destek sistemlerinden kaynaklanacak olumsuz etkilere karşı korumak amacıyla gerekli önlemler alınmalıdır.
4.5.3.10	1	Tehdit İstihbaratı Yönetimi	Siber güvenlik tehdit istihbaratı ile ilgili güncel ve güvenilir bilgiyi almak için gerekli tehdit istihbaratı çalışmaları yapılmalı ve tehdit istihbaratı verilerini yönetmek amacıyla bir süreç/mekanizma tanımlanmalıdır.
4.5.3.11	1	Otoritelerle İletişim	Tehdit yönetim faaliyetlerini destekleyecek otoritelere ilişkin iletişim listesi tanımlanmalıdır.
4.5.3.12	1	Arayan Hat Bilgisi Kullanımı	Haberleşme hizmetinde, arayan numara manipülasyonunu (Caller ID Manipulation) engellemeye yönelik teknik ve hukuki tedbirler alınmalıdır.
4.5.3.13	1	İnternet Değişim Noktası	Yurt içi iletişim trafiğinin ülke sınırları içerisinde kalması sağlanmalı, bu trafiğin ve abone kayıtlarının yurt dışına çıkarılarak tekrar yurt içine yönlendirilmesi engellenmelidir.
4.5.3.14	3	Kritik Haberleşme Güvenliği	Telekomünikasyon hizmeti veren işletmelerce yerine getirilmek üzere, Cumhurbaşkanlığı ve milli güvenliğin sağlanması kapsamında görev yürüten kamu kurumlarında iletişimin gizliliği ve güvenliğini artırmak amacıyla, bu kurumların merkez birimlerine ve talep edeceği diğer birimlerine doğrudan hizmet sağlayan haberleşme ve transmisyon altyapısında ilk toplama noktasına kadar radyolink vb. kablosuz teknolojiler kullanılmamalı, kullanımın zorunlu olması durumunda ihtiyaç duyulan gizlilik seviyesine uygun donanımsal veya yazılımsal milli kripto sistemleriyle birlikte kullanılmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.5.3.1	Hizmet Güvenliği ve Sürekliliği	Mülakat, Gözden Geçirme	Sağlanan iletişim hizmetlerinin güvenliğini ve sürekliliğini ele alan bir güvenlik politikası belirlenmiş midir? Güvenlik politikası kapsamında hangi konular ele alınmaktadır? Güvenlik politikası hangi periyotlarda gözden geçirilmektedir?
4.5.3.2	Üçüncü Taraflara İlişkin Güvenlik Gereksinimleri	Mülakat, Gözden Geçirme	Üçüncü taraflardan temin edilen/hizmet alınan BT ürünlerine, BT hizmetlerine, dış kaynaklı iş süreçlerine, yardım masalarına, çağrı merkezlerine, ara bağlantılara, ortak tesislere vb. yönelik güvenlik gereksinimleri ilgili sözleşmelerde nasıl adreslenmektedir?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.5.3.3	Altyapı Servislerinin Güvenliği	Mülakat, Güvenlik Denetimi	Haberleşme hizmetlerindeki altyapı servislerinin kötüye kullanımından kaynaklanacak ve müşterileri / diğer hizmet sağlayıcıları olumsuz olarak etkileyebilecek tehditleri önlemek amacıyla hangi güvenlik kontrolleri uygulanmaktadır?
4.5.3.4	Sahtecilik İşlemlerini Tespit ve Önleme	Mülakat, Güvenlik Denetimi	Sinyalleşme trafiğindeki olası sahtecilik işlemlerini tanımlamak, tespit etmek ve önlemek için bir sistem kurulmuş mudur? İlgili sistem nasıl işletilmektedir?
4.5.3.5	Sinyalleşme Trafiğinin Güvenliği	Mülakat, Güvenlik Denetimi	Sinyalleşme sistem ve protokollerindeki zafiyetlere yönelik hangi önlemler alınmaktadır?
4.5.3.6	Güvenilir İletişimin Tesisi	Mülakat, Güvenlik Denetimi	Sağlanan iletişim hizmetlerinde, müşterilerin kendisine tahsis edilmemiş kaynak adresi üzerinden iletişim sağlamamasına yönelik hangi önlemler alınmaktadır?
4.5.3.7	Sıkılaştırma Faaliyetleri	Mülakat, Güvenlik Denetimi	Sunucular, yönlendiriciler ve diğer şebeke elemanlarının saldırı yüzeyini azaltmak amacıyla hangi sıkılaştırma kontrolleri uygulanmaktadır?
4.5.3.8	Ekipman Arızalarının İzlenmesi	Mülakat, Gözden Geçirme	Güvenlik ve iş sürekliliği gereksinimlerini sağlamak amacıyla altyapıda yer alan ekipmanlara ait arıza sinyallerinin izlenmesi için alarm mekanizması mevcut mudur?
4.5.3.9	Ekipman Güvenliğinin Sağlanması	Mülakat, Güvenlik Denetimi	Haberleşme sistemlerinde kullanılan ekipmanı, çevresel tehditler ile enerji destek sistemlerinden kaynaklanacak olumsuz etkilere karşı korumak amacıyla hangi önlemler alınmaktadır?
4.5.3.10	Tehdit İstihbaratı Yönetimi	Mülakat, Gözden Geçirme	Siber güvenlik tehdit istihbaratı ile ilgili güncel ve güvenilir bilgiyi almak için ne tür çalışmalar yapılmaktadır? Tehdit istihbarat verilerini yönetmek amacıyla bir süreç/mekanizma tanımlanmış mıdır?
4.5.3.11	Otoritelerle İletişim	Mülakat, Gözden Geçirme	Tehdit yönetim faaliyetlerini destekleyecek otoritelere ilişkin iletişim listesi tanımlanmış mıdır?
4.5.3.12	Arayan Hat Bilgisi Kullanımı	Mülakat, Güvenlik Denetimi	Arayan numara manipülasyonunu engellemeye yönelik hangi tedbirler alınmaktadır?
4.5.3.13	İnternet Değişim Noktası	Mülakat, Güvenlik Denetimi	Yurt içi iletişim trafiğinin ülke sınırları içerisinde kalmasına yönelik ne tür çalışmalar yapılmaktadır?
4.5.3.14	Kritik Haberleşme Güvenliği	Mülakat, Güvenlik Denetimi	Kritik altyapı sektörlerinde faaliyet gösteren kurumlarda haberleşmesi ve transmisyon hizmeti nasıl sağlanmaktadır?

4.6. Yeni Geliştirmeler ve Tedarik

Amaç

Bu güvenlik tedbiri ana başlığının amacı, yeni geliştirmeler ve tedarik güvenliği çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. "Yeni Geliştirmeler ve Tedarik" ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Genel Güvenlik Tedbirleri

4.6.1. Genel Güvenlik Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.6.1.1	1	Politika ve Prosedürlerin Tanımlanması	Tedarik edilen yazılımların, donanımların ve sistem bileşenlerinin temini ve kabul aşamasında gerçekleştirilmesi gereken testlere yönelik politika ve prosedürler tanımlanmış olmalıdır. Bileşenler, sorumlu personelin/birimin onayı ile kurum envanterine eklenmelidir.
4.6.1.2	1	Yazılım Varlık Envanterine Kayıt Edilmemiş Yazılımların Yönetimi	Bk. Tedbir No: 3.1.2.4
4.6.1.3	1	Donanım Varlık Envanterine Kayıt Edilmemiş Donanımların Yönetimi	Bk. Tedbir No: 3.1.1.3
4.6.1.4	1	Arayüzün Türkçe Dil Desteğine Sahip Olması	Geliştirilen uygulama/sistem kapsamında sunulan arayüzün kullanıcılar tarafından açıkça anlaşılabilir olması adına Türkçe dil desteği sağlanmalı, tedarik edilen ürünlerde ise Türkçe dil desteği olan ürünler tercih edilmelidir.
4.6.1.5	2	Alt Yüklenici Yönetimi	Yeni geliştirmeler ve ürün/hizmet tedariki kapsamında alt yüklenici ile çalışılması durumunda işletilecek politika ve prosedürler tanımlanmış olmalıdır. Alt yüklenici tarafından gerçekleştirilecek değişiklik ve sürüm yönetimi faaliyetleri kurumun politika ve prosedürleri ile uyumlu olmalıdır.
4.6.1.6	2	Fonksiyonel ve Fonksiyonel Olmayan Testlerin Yapılması	Yeni geliştirmeler ve ürün/hizmet tedariki kapsamında kurumun fonksiyonel ve fonksiyonel olmayan testlere (yük, performans, güvenlik vb.) yönelik uygulanacak süreçleri tanımlı olmalı ve uygulanmalıdır. Bu süreçler düzenli olarak gözden geçirilmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.6.1.1	Politika ve Prosedürlerin Tanımlanması	Mülakat, Gözden Geçirme	Tedarik edilen yeni ürünlerin alımıyla ilgili işleyişi ve kuralları içeren politika ve prosedürler tanımlı mıdır? Tedarik edilen yeni ürünler kurum envanterine sorumlu personelin/birimin onayı dâhilinde mi eklenmektedir?
4.6.1.2	Yazılım Varlık Envanterine Kayıt Edilmemiş Yazılımların Yönetimi	Mülakat, Güvenlik Denetimi	Bk. Denetim No: 3.1.2.4
4.6.1.3	Donanım Varlık Envanterine Kayıt Edilmemiş Donanımların Yönetimi	Mülakat, Güvenlik Denetimi	Bk. Denetim No: 3.1.1.3
4.6.1.4	Arayüzün Türkçe Dil Desteğine Sahip Olması	Mülakat	Geliştirilen uygulama/sistem kapsamında sunulan arayüz, kullanıcılar tarafından açıkça anlaşılabilir olması adına Türkçe dil desteğine imkân sağlamakta mıdır?
4.6.1.5	Alt Yüklenici Yönetimi	Mülakat	Alt yüklenici ile çalışılma durumunda kurum tarafından işletilecek politika ve prosedürler tanımlanmış mıdır? Alt yüklenici tarafından gerçekleştirilen değişiklik ve sürüm yönetimi faaliyetleri kurumun politika ve prosedürleri ile uyumlu mudur?
4.6.1.6	Fonksiyonel ve Fonksiyonel Olmayan Testlerin Yapılması	Mülakat	Kurumun fonksiyonel ve fonksiyonel olmayan testlere yönelik uygulanacak süreçleri tanımlı mıdır? İlgili süreçler işletilmekte ve periyodik olarak gözden geçirilmekte midir?

SIKILAŞTIRMA TEDBİRLERİ

5. BÖLÜM

5. SIKILAŞTIRMA TEDBİRLERİ

5.1. İşletim Sistemi Sıkılaştırma Tedbirleri

Amaç

Bu güvenlik tedbiri ana başlığının amacı, işletim sistemi güvenlik sıkılaştırmaları çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. "İşletim Sistemi Sıkılaştırma Tedbirleri" ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Genel Sıkılaştırma Tedbirleri
- Linux İşletim Sistemi Sıkılaştırma Tedbirleri
- Windows İşletim Sistemi Sıkılaştırma Tedbirleri

5.1.1. Genel Sıkılaştırma Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.1.1.1	1	Kurulum Güvenliği	Kurulum esnasında kullanılan işletim sistemi dosyalarının özet bilgisi orijinal dağıtıcı özet değerleriyle teyit edilmelidir.
5.1.1.2	1	Servis Güvenliği	Sunucuların normal işleyişi için gerekli olmayan tüm servisler kapatılmalıdır. Sistemlerde çalışan servisler ihtiyaçları olan en az yetki ile çalışmalıdır. Servis kullanıcılarının yetkileri ayrıca kısıtlanmalıdır. Servislerin döndüğü başlık bilgileri (banner) bilgi ifşasına yol açmayacak şekilde değiştirilmelidir.
5.1.1.3	1	Güncel İşletim Sistemi ve Uygulamaların Kullanılması	Güncel ve güvenlik desteği devam eden işletim sistemleri kullanılmalıdır. Uygulama sürümleri periyodik olarak kontrol edilmelidir.
5.1.1.4	1	Şifreli Haberleşen Servislerin Kullanılması	Şifresiz kimlik doğrulama ve haberleşme kullanan servisler (Telnet, FTP, rlogin, HTTP, SMTP vb.), eğer varsa şifreli haberleşme imkânı sağlayan muadilleri (SSH, SFTP, HTTPS, SMTPS vb.) ile değiştirilmelidir.
5.1.1.5	1	Parola Politikasının Belirlenmesi	Tüm makinelerde kullanıcı parolaları için güçlü bir parola politikası belirlenmelidir. Kullanıcılar ilk girişten sonra parolalarını değiştirmeye zorlanmalı ve parolaların belirli bir süreden sonra geçerliliğini yitirip yenilenmesi sağlanmalıdır. Ayrıca belirli bir sayıda hatalı giriş denemesinden sonra kullanıcı hesapları kilitlenmelidir.
5.1.1.6	1	Son Kullanıcı Bilgisayarlarında Ağ Erişiminin Kısıtlanması	Kullanıcı bilgisayarlarında, bilgisayara ağ üzerinden erişim yetkisi, sadece yönetici hesapları ve uzak masaüstü kullanıcıları veya grupları ile sınırlandırılmalıdır.
5.1.1.7	1	Hata ve Sorun Bilgilerinin Üretici ile Paylaşılmaması	İşletim sistemi kurulumu ile gelen hata ve sorun bilgilerinin üretici ile paylaşılması özelliği pasif hale getirilmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.1.1.8	1	Kablosuz Ağ Arayüzlerinin Kapatılması	Tüm sunucularda kullanılmayan kablosuz ağ arayüzleri pasif hale getirilmelidir.
5.1.1.9	1	Sistem Üzerinde Düzenli Olarak Zafiyet ve Zararlı Yazılım Taraması Yapılması	Sistemde düzenli olarak zafiyet taraması yapılmalı ve bu zafiyetlerin yönetimi gerçekleştirilmelidir. Sistem zararlı yazılımlara karşı düzenli olarak taranmalıdır. Bk. Tedbir No: 3.1.5.1
5.1.1.10	1	Yerel Güvenlik Duvarı Ayarlarının Yapılması	Bk. Tedbir No: 3.1.6.11
5.1.1.11	1	Sunucularda Zaman Senkronizasyonunun Sağlanması	Sunucularda ilgili NTP ayarlamaları yapılarak tüm sunucularda zaman senkronizasyonu sağlanmalıdır.
5.1.1.12	1	Güvenli Süreç (Process) İşleme Ayarlarının Yapılması	İşletim sistemlerinin DEP, ASLR, XD/NX gibi savunma özellikleri istisnai durumlar haricinde aktif olmalıdır.
5.1.1.13	2	Kullanılmayan Uygulamaların Kaldırılması	Sistemlerde kullanılmayan uygulamalar belirlenerek kaldırılmalıdır.
5.1.1.14	2	Merkezi Güncelleme Sunucusu	İşletim sistemi güncellemeleri için merkezi bir güncelleme sunucusu oluşturulmalıdır.
5.1.1.15	2	IPv6 Pasif Hale Getirilmesi	Eğer kurum içerisinde IPv6 kullanılmıyorsa, IPv6 destekleyen tüm sunucularda IPv6 desteği pasif hale getirilmelidir.
5.1.1.16	2	Sistem İz Kayıtlarının Aktif Edilmesi	Tüm sunucu ve makinelerde iz kayıtları aktif edilmelidir. Sistem zaman ve tarih ayarları, kullanıcı hesapları, ağ yapılandırması, erişim kontrolleri üzerinde yapılan değişiklikler kayıt altına alınmalıdır. Ayrıca giriş ve çıkış bilgileri, yetkisiz dosya okuma denemeleri, dosya silme işlemleri ve sistem yöneticisi hareketleri de kayıt altına alınmalıdır. Bk. Tedbir No: 3.1.8.1
5.1.1.17	2	Sistem İz Kayıtlarının Merkezi Bir Sunucuda Toplanması	Sistemlerden syslog vb. araçlarla toplanan sistem iz kayıtları merkezi bir kayıt yönetim sistemine gönderilmelidir. Burada toplanan iz kayıtları kurum kritiklik seviyesi ve dinamiklerine uygun olarak işlenmelidir. Bk. Tedbir No: 3.1.8.6
5.1.1.18	2	Merkezi Kimlik Yönetimi Servisinin Kullanılması	Tüm makinelerde kullanıcı kimlik doğrulama için merkezi kimlik yönetimi servisi kullanılmalıdır.
5.1.1.19	3	Sunucularda Çalışan Servislerin Takibi	Sunucuların normal işleyişi için gerekli olan servisler dışında başka bir servisin sunucuda açılması halinde alarm üretilmeli ve ilgili servis kapatılmalıdır.
5.1.1.20	3	Bilgisayar Tabanlı Saldırı Tespit ve Engelleme Sistemlerinin Kullanılması	Makine özelinde saldırı tespit ve engelleme sistemi (HIDS/HIPS) kullanılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.1.1.21	3	Disk Kotalarının Belirlenmesi	Tüm makinelerde kullanıcılar için her dosya sistemine özel disk kota politikaları belirlenmeli ve etkinleştirilmelidir.
5.1.1.22	3	Disk Seviyesinde Şifreleme Yapılması	Kritik bilgi içeren ve/veya işleyen makinelerde disk seviyesinde şifreleme yapılmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
5.1.1.1	Kurulum Güvenliği	Mülakat	Kurulumda kullanılan işletim sistemlerinin bütünlüğü, kurulumdan önce özetleri alınarak teyit edilmekte midir?
5.1.1.2	Servis Güvenliği	Mülakat, Güvenlik Denetimi, Sızma Testi	Sistemlerin döndüğü başlık bilgilerinde kısıtlamalar uygulanmakta mıdır? Bu kısıtlamalar nasıl belirlenmiştir? Sunucularda kullanılan ve kullanılmayan servisler belirlenmiş midir? Kullanılmayan servisler kapatılmış mıdır? Çalışan servislerin yetkileri nasıl belirlenmektedir? Yönetici hakları ile çalıştırılan servisler var mıdır?
5.1.1.3	Güncel İşletim Sistemi ve Uygulamaların Kullanılması	Mülakat, Güvenlik Denetimi	İşletim sistemi sürümleri ne sıklıkla güncellenmektedir? Kullanılan işletim sistemi sürümlerinin güncelliği sağlanmakta mıdır? İşletim sistemi üzerinde yer alan uygulamaların güncelliği kontrol edilmekte midir?
5.1.1.4	Şifreli Haberleşen Servislerin Kullanılması	Güvenlik Denetimi, Sızma Testi	Şifresiz haberleşen servisler, şifreli işlem yapan muadilleri ile değiştirilmiş midir?
5.1.1.5	Parola Politikasının Belirlenmesi	Mülakat, Güvenlik Denetimi	Tüm makineler için kullanıcı parolaları hangi prosedürlere göre belirlenmektedir? Parola değişimi ve yenileme hangi politikalara göre yapılmaktadır? Parola geçmişi tutulmakta ve hatalı giriş sayısına göre kullanıcı hesapları kilitlenmekte midir? Parolası olmayan hesaplar için nasıl bir prosedür uygulanmaktadır?
5.1.1.6	Son Kullanıcı Bilgisayarlarında Ağ Erişiminin Kısıtlanması	Güvenlik Denetimi	Son kullanıcı bilgisayarlarında ağ erişimi kısıtlaması yapılmış mıdır?
5.1.1.7	Hata ve Sorun Bilgilerinin Üretici ile Paylaşılmaması	Mülakat, Güvenlik Denetimi	İşletim sistemi kurulumu ile gelen hata ve sorun bilgilerinin üretici ile paylaşılması özelliği pasif hale getirilmiş midir?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
5.1.1.8	Kablosuz Ağ Arayüzlerinin Kapatılması	Mülakat, Güvenlik Denetimi	Tüm sunucularda kullanılmayan kablosuz ağ arayüzleri pasif hale getirilmiş midir?
5.1.1.9	Sistem Üzerinde Düzenli Olarak Zafiyet ve Zararlı Yazılım Taraması Yapılması	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Sistemler için zafiyet yönetimi nasıl sağlanmaktadır? Bu işlem için hangi araçlardan faydalanılmaktadır? Sistemler üzerinde düzenli olarak zararlı yazılım taraması yapılmakta mıdır? Zararlı yazılım taramasında faydalanılan araçlar nelerdir?
5.1.1.10	Yerel Güvenlik Duvarı Ayarlarının Yapılması	Mülakat, Güvenlik Denetimi, Sızma Testi	Tüm sunucularda yerel güvenlik duvarı aktif olarak çalışmakta mıdır? Güvenlik duvarı yapılandırması yaparken neler dikkate alınmaktadır? Güvenlik duvarı kurallarında varsayılan reddetme (deny) kuralı yer almakta mıdır?
5.1.1.11	Sunucularda Zaman Senkronizasyonunun Sağlanması	Mülakat, Güvenlik Denetimi	Sunucularda zaman senkronizasyonu sağlanmış mıdır ve güncel midir?
5.1.1.12	Güvenli Süreç (Process) İşleme Ayarlarının Yapılması	Mülakat, Güvenlik Denetimi	İşletim sistemlerinin DEP, ASLR vb. savunma mekanizmaları etkinleştirilmiş midir?
5.1.1.13	Kullanılmayan Uygulamaların Kaldırılması	Mülakat, Güvenlik Denetimi	Sistemlerde kullanılmayan uygulamaların tespiti nasıl gerçekleştirilmektedir? Sistemde kullanılmayan uygulamalar sistemlerden kaldırılmış mıdır?
5.1.1.14	Merkezi Güncelleme Sunucusu	Mülakat, Güvenlik Denetimi	Sistemlerin güncellik durumları nasıl kontrol edilmektedir? Güncelleştirme işlemleri için merkezi bir güncelleştirme sunucusu kullanılmakta mıdır?
5.1.1.15	IPv6 Pasif Hale Getirilmesi	Mülakat, Güvenlik Denetimi	Kurum içinde IPv6 kullanılmakta mıdır? Kullanılmıyorsa sunucularda IPv6 desteği pasif hale getirilmiş midir?
5.1.1.16	Sistem İz Kayıtlarının Aktif Edilmesi	Mülakat, Güvenlik Denetimi	Tüm sunucu ve makinelerde sistem iz kayıtları alınmakta mıdır? Hangi bilgiler kayıt altına alınmaktadır?
5.1.1.17	Sistem İz Kayıtlarının Merkezi Bir Sunucuda Toplanması	Mülakat, Güvenlik Denetimi	Sistem iz kayıtları merkezi bir kayıt sistemine gönderilmekte midir?
5.1.1.18	Merkezi Kimlik Yönetimi Servisinin Kullanılması	Mülakat, Güvenlik Denetimi	Merkezi bir kullanıcı yönetim sistemi kullanılmakta mıdır? Kullanılıyorsa, nasıl yönetilmektedir?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
5.1.1.19	Sunucularda Çalışan Servislerin Takibi	Mülakat, Güvenlik Denetimi, Sızma Testi	Sunucularda gerekli ve gereksiz servisler belirlenmiş midir? Gerekli ve gereksiz servisler nasıl belirlenmiştir? Listede olmayan bir servis başlatıldığında bunu engellemek/yönetmek için hangi araçlardan faydalanılmaktadır?
5.1.1.20	Bilgisayar Tabanlı Saldırı Tespit ve Engelleme Sistemlerinin Kullanılması	Mülakat, Güvenlik Denetimi	Sistem yerelinde saldırı tespit ve engelleme sistemi (HIDS/HIPS) kullanılmakta mıdır?
5.1.1.21	Disk Kotalarının Belirlenmesi	Mülakat, Güvenlik Denetimi	Kullanıcılar için disk kotaları belirlenmiş midir? Disk kota politikaları uygulanmakta mıdır?
5.1.1.22	Disk Seviyesinde Şifreleme Yapılması	Mülakat, Güvenlik Denetimi	Kritik bilgi içeren ve/veya işleyen makineler için disk seviyesinde şifreleme yapılmakta mıdır?

5.1.2. Linux İşletim Sistemi Sıkılaştırma Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.1.2.1	1	Kullanılmayan Dosya Sistemlerinin Pasif Hale Getirilmesi	Kullanılmayan dosya sistemleri (cramfs, freevxfs, hfs vb.) pasif hale getirilmelidir.
5.1.2.2	1	Yetkili Kullanıcı Hesap Yönetimi	• Sisteme erişecek her kişi için ayrı bir kullanıcı hesabı oluşturulmalıdır. • Oluşturulan kullanıcılar için yetkiler belirlenmelidir. • Kullanılmayan hesaplar kaldırılmalıdır. • Sistem kullanıcılarının kabuğu /sbin/nologin olmalıdır. • Root login mümkünse engellenmelidir. • Tüm makinelerde UID değeri 0 olan tek kullanıcı root olmalıdır. • Ayrıca aynı isme veya UID değerine sahip kullanıcı veya grup bulunmamalıdır. • Servis ve sistem kullanıcıları hariç parolasız kullanıcılar bulunmamalıdır. • Sudoers kullanıcıları değişikliklere karşı takip edilmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.1.2.3	2	Dosya Sistemi Güvenli Erişim Düzenlemeleri	İçeriği değiştiğinde, silindiğinde veya taşındığında sistemin çalışmasını olumsuz yönde etkileyebilecek çalışma dosyalarının, kütüphanelerin ve yapılandırma dosyalarının (SUID ve SGID dosyaları, kayıt dosyaları, cron dosyaları, başlangıç betikleri, /etc/passwd, /etc/shadow vb.) yetkilendirmeleri amacına uygun şekilde düzenlenmeli ve kurum politikaları doğrultusunda denetlenmelidir. Varsayılan kullanıcı umask değeri en az yetki prensibine göre ayarlanmalıdır.
5.1.2.4	2	Güvenli Disk Bölümlendirme	İşletim sistemi dosyaları ile kullanıcı dosyaları, /home, /root, /boot, /tmp vb. birimler ayrı disk bölümlerinde tutulmalıdır.
5.1.2.5	2	Otomatik Başlatma (Mount) Özelliğinin Pasif Hale Getirilmesi	CD/DVD ve USB gibi harici medyanın otomatik olarak mount edilmesini önlemek adına otomatik mount özelliği pasif hale getirilmelidir. Ayrıca /tmp dizini gibi mount noktalarında noexec, nodev, nosuid parametreleriyle çalıştırılabilir dosyalar pasif hale getirilmelidir.
5.1.2.6	2	Dosya Sistemi Bütünlük Kontrollerinin Düzenli Olarak Yapılması	Önemli görülen dosyaların bütünlüğü düzenli olarak kontrol edilmelidir.
5.1.2.7	2	Önyükleme (Boot) Ayarlarının Güvenli Şekilde Yapılandırılması	Kullanılan makinelerde önyükleyici (bootloader) parolası belirlenmeli ve zorunlu tutulmalıdır. Ayrıca tek kullanıcı modu için kimlik doğrulaması yapılmalıdır. Boot edilebilir cihazlar listesi kısıtlanmalıdır. Kullanılmıyorsa USB, Firewire, Thunderbolt, PCMCIA vb. cihazlar iptal edilmelidir.
5.1.2.8	3	Zorunlu Erişim Kontrolünün (MAC) Aktif Edilmesi	İşletim sistemi üzerinde erişim kontrolü, ilgili servisler (SELinux, AppArmor vb.) kullanılarak zorunlu erişim kontrolü (MAC) modeline göre yapılmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
5.1.2.1	Kullanılmayan Dosya Sistemlerinin Pasif Hale Getirilmesi	Mülakat, Güvenlik Denetimi	Kullanılmayan dosya sistemleri (cramfs, freevxfs, hfs vb.) etkisiz hale getirilmiş midir?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
5.1.2.2	Yetkili Kullanıcı Hesap Yönetimi	Mülakat, Güvenlik Denetimi	Kullanıcılar ve yetkileri nasıl yönetilmektedir? Gereksiz kullanıcılar bulunmakta mıdır? Sistem ve servis kullanıcıları hariç diğer kullanıcıların parolaları bulunmakta mıdır? Root ile uzaktan erişim mümkün müdür? UID değeri 0 olan kullanıcı bulunmakta mıdır? Aynı isme ve UID değerine sahip kullanıcılar ve gruplar bulunmakta mıdır? Sistem kullanıcıların kabuğu /sbin/nologin midir? Sudoers kullanıcıları değişikliklere karşı takip edilmekte midir?
5.1.2.3	Dosya Sistemi Güvenli Erişim Düzenlemeleri	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Sistemlerde yer alan kritik dosyalar belirlenmiş midir? Dosya sistemlerine güvenli erişim kapsamında tanımlanmış bir politika var mıdır? Politika içeriğinde hangi hususlar ele alınmaktadır?
5.1.2.4	Güvenli Disk Bölümlendirme	Mülakat, Güvenlik Denetimi	Disk bölümlendirme nasıl yapılmaktadır?
5.1.2.5	Otomatik Başlatma (Mount) Özelliğinin Pasif Hale Getirilmesi	Mülakat, Güvenlik Denetimi	CD/DVD ve USB gibi medya cihazları otomatik olarak başlatılmakta mıdır? Bunu engellemek için ne gibi bir yapılandırma ayarı yapılmıştır?
5.1.2.6	Dosya Sistemi Bütünlük Kontrollerinin Düzenli Olarak Yapılması	Mülakat, Güvenlik Denetimi	Sistemlerde bütünlüğü kritik olan dosyalar belirlenmiş midir? Belirlenen bu dosyaların kontrolünü yapmak için hangi araçlardan/programlardan faydalanılmaktadır? Dosyaların bütünlüğünün bozulduğu durumlar için ne gibi bir süreç işletilmektedir?
5.1.2.7	Önyükleme (Boot) Ayarlarının Güvenli Şekilde Yapılandırılması	Mülakat, Güvenlik Denetimi	Önyükleyici için güvenli bir yapılandırma var mıdır? Boot cihazlarının yönetimi nasıl yapılmaktadır?
5.1.2.8	Zorunlu Erişim Kontrolünün (MAC) Aktif Edilmesi	Mülakat, Güvenlik Denetimi	Zorunlu erişim kontrolü (MAC) için hangi servilerden faydalanılmaktadır? Bu servislerin yönetimi nasıl sağlanmaktadır?

5.1.3. Windows İşletim Sistemi Sıkılaştırma Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.1.3.1	1	Kullanıcı Haklarının Kısıtlanması	Kullanıcı hakları en az yetki prensibi göz önünde bulundurularak sadece ihtiyaç duyulan kullanıcı ve gruplara verilmelidir.
5.1.3.2	1	Otomatik Güncellemenin Aktif Olması	Tüm kullanıcı makinelerinde otomatik güncelleme özelliği aktif hale getirilmelidir.
5.1.3.3	1	SMB Protokolü Güvenliği	Windows işletim sistemlerinde SMB versiyon 1 protokolü yerine daha güvenli ve güncel SMB protokol versiyonları kullanılmalıdır.
5.1.3.4	1	Yerel Yönetici Hesapları Yönetimi	Gerekli kullanıcılar dışında tüm kullanıcıların yerel yönetici hesapları devre dışı bırakılmalıdır. Gerekli kullanıcılar için varsayılan olarak aynı tanımlanan yerel yönetici hesaplarının parolaları değiştirilmelidir.
5.1.3.5	1	Ayrıcalıklı Hesap Sayılarının Sınırlandırılması	Etki alanı yöneticisi (Domain Admin) ve diğer yetkili hesapların (Enterprise Admin, Backup Admin ve Schema Admin) sayısı sınırlandırılmalıdır.
5.1.3.6	1	Yetkili Hesapların Parola Özetlerinin Çalınmasının Engellenmesi	Yetkili hesapların parola özetlerinin çalınmasının engellenmesi için: • Etki alanı yöneticisi (domain admin) hesabıyla kullanıcı bilgisayarlarında gerekli olmadıkça işlem yapılmamalı, işlem yapıldığı durumlarda kullanıcı bilgisayarlarının yeniden başlatılması sağlanmalıdır. • Yerel bilgisayarlarda parola özetleri tutulma sayısı 0 yapılmalıdır. • Ayrıcalıklı kullanıcı hesapları Korunan Kullanıcılar (Protected Users) grubuna alınmalıdır.
5.1.3.7	2	Kullanılmayan Hesapların Devre Dışı Bırakılması	Aktif dizinde uzun süre kullanılmayan kullanıcı ve bilgisayar hesaplarını tespit etmek için bir yordam tanımlanmalıdır. Bk. Tedbir No: 3.1.12.10
5.1.3.8	2	Varsayılan Yönetici ve Misafir Hesaplarının Yapılandırılması	Sistemlerde yer alan varsayılan yönetici ve misafir hesapları pasif hale getirilmelidir.
5.1.3.9	2	Standart Kullanıcıların Betik Çalıştırma Motorlarına Erişiminin Kısıtlanması	Standart kullanıcıların betik çalıştırma motorlarına (Windows Script Host, Powershell, Command Prompt ve Microsoft HTML Application Host vb.) erişimi engellenmeli veya kısıtlanmalıdır.
5.1.3.10	2	Aktif Dizin Sorguları Güvenliği	Aktif dizin sorguları LDAP protokolü yerine güvenli LDAPs protokolü ile yapılacak şekilde konfigüre edilmelidir. Bk. Tedbir No: 3.2.9.1

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.1.3.11	2	Yönetici Hesaplarının İzlenmesi	Ayrıcalıklı etki alanı gruplarına kullanıcı ekleme ve çıkarma işlemleri ve oturum açma kapama işlemleri izlenmelidir. Bk. Tedbir No: 3.1.12.11
5.1.3.12	2	Güvenli Yönetici İş İstasyonu Kullanımı	Yalnızca etki alanı yönetimini (Domain Controller) gerçekleştirmek için güvenli bir yönetici iş istasyonu konumlandırılmalı, ek yazılım veya rol yüklenmemeli, eposta, internet vb. erişimleri için kullanılmamalıdır.
5.1.3.13	2	Devre Dışı Bırakılan Hesabın Mail Erişiminin Engellenmesi	Aktif dizinde devre dışı bırakılan kullanıcı hesabı için activesync mail erişimi hemen kesilmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
5.1.3.1	Kullanıcı Haklarının Kısıtlanması	Mülakat, Güvenlik Denetimi	Kullanıcı haklarının kısıtlanması son kullanıcı bilgisayarlarına uygun olarak yapılandırılmış mıdır?
5.1.3.2	Otomatik Güncellemenin Aktif Olması	Mülakat, Güvenlik Denetimi	İşletim sisteminin otomatik güncelleme ayarı açık mıdır?
5.1.3.3	SMB Protokolü Güvenliği	Mülakat, Gözden Geçirme	SMB versiyon 1 protokolü sunucu ve istemcilerde kapatılmış mıdır, SMB protokolü hangi versiyon u kullanılmaktadır?
5.1.3.4	Yerel Yönetici Hesapları Yönetimi	Mülakat, Gözden Geçirme	Gerekli kullanıcılar dışında tüm kullanıcıların yerel yönetici hesapları devre dışı bırakılmış mıdır? Yerel yönetici hesaplarının parolaları nasıl değiştirilmektedir?
5.1.3.5	Ayrıcalıklı Hesap Sayılarının Sınırlandırılması	Mülakat, Gözden Geçirme	Ayrıcalıklı hesap sayıları sınırlandırılmakta mıdır?
5.1.3.6	Yetkili Hesapların Parola Özetlerinin Çalınmasının Engellenmesi	Mülakat, Gözden Geçirme	Etki alanı yöneticisi (domain admin) hesabıyla kullanıcı bilgisayarlarında ne sıklıkla ve ne gibi işlemler yapılmaktadır? Yerel bilgisayarlarda tutulan hesaplara ait parola özetlerinin tutulma sayısı 0 olarak ayarlanmış mıdır? Ayrıcalıklı kullanıcı hesapları Korunan Kullanıcılar (Protected Users) Grubuna alınmış mıdır?
5.1.3.7	Kullanılmayan Hesapların Devre Dışı Bırakılması	Mülakat, Gözden Geçirme	Aktif dizinde uzun süre kullanılmayan kullanıcı ve bilgisayar hesaplarını tespit etmek için bir yordam tanımlanmış mıdır?
5.1.3.8	Varsayılan Yönetici ve Misafir Hesaplarının Yapılandırılması	Mülakat, Güvenlik Denetimi	Varsayılan yönetici ve misafir hesaplarının yapılandırılması en iyi çözüm önerilerine uygun olarak yapılmış mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
5.1.3.9	Standart Kullanıcıların Betik Çalıştırma Motorlarına Erişiminin Kısıtlanması	Mülakat, Güvenlik Denetimi	Cmd, powershell gibi betik çalıştırma motorlarına erişimler kısıtlandırılmış mıdır?
5.1.3.10	Aktif Dizin Sorguları Güvenliği	Mülakat, Gözden Geçirme	Aktif dizin sorguları güvenli LDAPs protokolü ile yapılmakta mıdır?
5.1.3.11	Yönetici Hesaplarının İzlenmesi	Mülakat, Gözden Geçirme	Ayrıcalıklı etki alanı gruplarına kullanıcı ekleme ve çıkarma işlemleri ve oturum açma kapama işlemleri izlenmekte midir?
5.1.3.12	Güvenli Yönetici İş İstasyonu Kullanımı	Mülakat, Gözden Geçirme	Yalnızca etki alanı yönetimini (Domain Controller) gerçekleştirmek için güvenli bir yönetici iş istasyonu kullanılmakta mıdır?
5.1.3.13	Devre Dışı Bırakılan Hesabın Mail Erişiminin Engellenmesi	Mülakat, Gözden Geçirme	Aktif dizinde devre dışı bırakılan kullanıcı hesabı için activesync mail erişimi hemen kesilmekte midir?

5.2. Veri Tabanı Sıkılaştırma Tedbirleri

Amaç

Bu güvenlik tedbiri ana başlığının amacı, veri tabanı güvenlik sıkılaştırmaları çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. “Veri Tabanı Sıkılaştırma Tedbirleri” ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Genel Sıkılaştırma Tedbirleri

5.2.1. Genel Sıkılaştırma Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.2.1.1	1	Güncelleme ve Yama Yönetimi	Üretici tarafından desteklenmeyen sistemler zafiyet içerebileceğinden, veri tabanı bilinen en kararlı versiyon ile kullanılmalıdır. Bu kapsamda, belirli periyotlar ile sistemlerin güncelliği kontrol edilmeli ve gerekli güncelleştirmeler gerçekleştirilmelidir. Güvenlik yamaları, yayımlandıktan sonra mümkün olan en kısa zamanda ilgili sistemlere yüklenmelidir.
5.2.1.2	1	Veri Tabanı Parametrelerinin Güvenli Yapılandırılması	Veri tabanı için sunulan parametreler ulusal ve/veya uluslararası otoriteler tarafından güvenli olarak kabul görmüş yöntemler ile yapılandırılmalıdır. Ayrıca veri tabanı yönetim sistemi üreticisi tarafından yayımlanan güvenli kullanım önerileri uygulanmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.2.1.3	1	Varsayılan Hesap ve Parolaların Kullanılmaması	Veri tabanlarında varsayılan kullanıcı hesapları ve parolalar kullanılmamalıdır.
5.2.1.4	1	Veri Tabanı Kullanıcıları için Parola Politikalarının Oluşturulması	Veri tabanı kullanıcıları için güçlü parola politikaları oluşturulmalı ve uygulanmalıdır.
5.2.1.5	1	Veri Tabanına Yapılan Uzak Bağlantıların Güvenliğinin Sağlanması	Veri tabanı sunucularına olan uzak bağlantı, mümkün olduğunca sınırlandırılarak yalnızca yetkili kullanıcıların ve/veya uygulamaların uzaktan erişimine olanak sağlayacak şekilde yapılandırılmalıdır. Bu kapsamda, ilgili sunucularda mevcut yapılandırmalar düzenlenmeli ve ağ katmanında gerekli önlemler alınmalıdır.
5.2.1.6	1	Kullanılmayan Hesapların Kapatılması	Düzenli olarak gerçekleştirecek denetimler ile belirli bir süre boyunca kullanılmayan kullanıcılar tespit edilerek pasif hale getirilmelidir.
5.2.1.7	1	Anonim Hesapların Bulunmaması	Veri tabanı kullanıcı hesapları, yapılan işlemlerin izlenebilirliğini sağlayacak ve tekil olarak kişi veya sistemi işaret edecek şekilde yapılmalıdır.
5.2.1.8	1	Veri Tabanı Rol ve Yetkilerinin Kısıtlanması	Tüm ayrıcalıklar, doğrudan kullanıcıya verilmek yerine kullanıcıların atanmış oldukları rollere/profillere tanımlanmalıdır. Düzenli aralıklarla veri tabanı rol ve yetkileri gözden geçirilmelidir. Kullanılmayan roller kaldırılmalı/pasif hale getirilmelidir. Ayrıca, kullanıcı hakları gözden geçirilerek gereksiz olarak tanımlanmış ve/veya ihtiyaç duyulmayan yetkiler kaldırılmalıdır.
5.2.1.9	1	Veri Tabanı Yönetim Sisteminin İşletim Sistemi Üzerindeki Ayrıcalıklarının Sınırlandırılması	Veri tabanının çalıştığı işletim sistemi üzerinde; komut çalıştırma, yerel dosya okuma/yazma vb. işlemlere imkân sağlayabilecek ayrıcalıkların sınırlandırılması için veri tabanı yönetim sistemi, desteklediği ölçüde yapılandırılmalıdır.
5.2.1.10	1	Komut/Sorgu Geçmişi Kayıtlarının Güvenliğinin Sağlanması	Veri tabanı tarafından, üzerinde çalıştırılmış komut/sorgu geçmişinin kayıt altına alındığı durumda ilgili kayıtların/dosyaların güvenliği sağlanmalıdır.
5.2.1.11	1	Yedeklerin Güvenliğinin Sağlanması	Yedek dosyalarına yetkisiz kullanıcıların erişmesini engellemek adına dosya izinlerinin yapılandırılması, şifreleme vb. yöntemler ile güvenlik sağlanmalıdır.
5.2.1.12	1	Adanmış Sunucu Kullanılması	Saldırı yüzeyini düşürmek amacıyla, veri tabanı yönetim sistemi adanmış bir sunucu üzerinde çalışmalıdır.
5.2.1.13	1	Kurulum Dosyalarının Güvenilir Kaynaklardan Temin Edilmesi	Kurulum dosyaları ve/veya kurulum için kullanılan paketler, güvenilir kaynaklardan elde edilmelidir.
5.2.1.14	1	Örnek Verilerin Silinmesi	Veri tabanından, kurulum ile gelen örnek veriler (örnek tablolar, kayıtlar, kullanıcılar vb.) silinmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.2.1.15	2	Veri Tabanı Sistem Dosyalarının ve İz Kayıtlarının Aynı Disk Bölümü Üzerinde Bulunmaması	Veri tabanı tarafından kullanılan sistem dosyaları ve üretilen iz kayıtları farklı disk bölümlerinde tutulmalıdır.
5.2.1.16	2	Veri Tabanında Tablo ve Nesne Düzeyinde Yetkilendirme Yapılması	Kritik veri içeren tablo ve nesneler için tablo ve/veya nesne bazında yetkilendirme yapılmalıdır.
5.2.1.17	2	İşletim Sistemi Üzerinde Veri Tabanı Servisi Çalıştıran Kullanıcıların Yönetici Haklarına Sahip Olmaması	İşletim sistemi üzerinde veri tabanı servis(ler)ini çalıştıran kullanıcılar için en az yetki prensibi uygulanmalıdır. Bu kapsamda ilgili kullanıcılar, ihtiyaç duyulmadığı takdirde yönetici haklarına sahip olmamalıdır.
5.2.1.18	2	Kümeleme veya Replikasyon İçinde Bulunan Veri Tabanı Sunucuları Arası İletişimin Güvenliğinin Sağlanması	Kümeleme (cluster) ve/veya replikasyon içinde bulunan veri tabanı sunucuları arasında gerçekleştirecekleri iletişim şifreli olarak yapılmalıdır. Buna ek olarak, ilgili süreçlerde kullanılacak hesaplar için en az yetki prensibi uygulanmalıdır. Bu kapsamda, replikasyon ve kümeleme faaliyetlerinde kullanılan hesaplar ihtiyaç duyulmadığı takdirde yönetici haklarına sahip olmamalıdır. Bk. Tedbir No: 5.2.1.8 Bk. Tedbir No: 3.2.5.11
5.2.1.19	2	Merkezi Kimlik Doğrulama Sisteminin Kullanılması	Veri tabanı yönetim sisteminin desteklediği ölçüde, merkezi kimlik doğrulama sistemi kullanılmalıdır.
5.2.1.20	3	Kritik Bilgi İçeren Veri Tabanı Sunucularında Durağan Verinin Güvenliğinin Sağlanması	Veri tabanı sunucularında yer alan kritik verinin, depolama motoru (storage engine) ve/veya disk seviyesinde şifreleme gibi yöntemler ile güvenliği sağlanmalıdır. Bk. Tedbir No: 5.1.1.22
5.2.1.21	3	Veri Tabanı Sunucusu ile İstemci Arasındaki İletişimin Şifreli Olması	Veri tabanı sunucusu ile istemci arasındaki iletişim şifreli trafik üzerinden sağlanmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
5.2.1.1	Güncelleme ve Yama Yönetimi	Mülakat, Güvenlik Denetimi	Veri tabanının güncelliği ve güvenlik yamalarının mevcut olup olmadığı belirli periyotlar ile kontrol ediliyor mu? Yeni versiyonun veya güvenlik yamasının tespit edilmesi halinde güncelleştirmeler kontrollü bir şekilde devreye alınıyor mu?
5.2.1.2	Veri Tabanı Parametrelerinin Güvenli Yapılandırılması	Mülakat, Güvenlik Denetimi	Veri tabanı için sunulan parametreler, ulusal ve/veya uluslararası otoriteler tarafından güvenli olarak kabul görmüş yöntemler ile yapılandırılıyor mu?
5.2.1.3	Varsayılan Hesap ve Parolaların Kullanılmaması	Mülakat, Güvenlik Denetimi	Veri tabanında varsayılan hesaplar bulunmakta mıdır? Veri tabanı kullanıcıları arasında varsayılan parola kullanan hesap bulunmakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
5.2.1.4	Veri Tabanı Kullanıcıları için Parola Politikalarının Oluşturulması	Mülakat, Güvenlik Denetimi	Veri tabanı kullanıcılarını güçlü parola kullanmaya zorlayacak politikalar tanımlanmış mıdır? Tanımlanan politikalar tüm kullanıcılar için zorunlu tutulmakta mıdır?
5.2.1.5	Veri Tabanına Yapılan Uzak Bağlantıların Güvenliğinin Sağlanması	Mülakat, Güvenlik Denetimi	Veri tabanı sunucularına yalnızca gerekli/yetkili kullanıcılar ve/veya uygulamalar tarafından uzaktan bağlantının sağlaması için hangi önlemler alınmaktadır?
5.2.1.6	Kullanılmayan Hesapların Kapatılması	Mülakat, Güvenlik Denetimi	Belirli bir süre boyunca kullanılmayan kullanıcılar tespit edilerek pasif hale getiriliyor mu?
5.2.1.7	Anonim Hesapların Bulunmaması	Mülakat, Güvenlik Denetimi	Aynı hesabın birden fazla kullanıcı tarafından kullanılmasını (ortak hesap) önlemek adına tekil kullanıcılar tanımlanmış mıdır?
5.2.1.8	Veri Tabanı Rol ve Yetkilerinin Kısıtlanması	Mülakat, Güvenlik Denetimi	Veri tabanı rol ve yetkileri düzenli aralıklarla gözden geçirilerek kullanılmayan roller pasif hale getiriliyor/kaldırılıyor mu? Kullanıcı hakları gözden geçirilerek gereksiz olarak tanımlanmış ve/veya ihtiyaç duyulmayan yetkiler kaldırılıyor mu?
5.2.1.9	Veri Tabanı Yönetim Sisteminin İşletim Sistemi Üzerindeki Ayrıcalıklarının Sınırlandırılması	Mülakat, Güvenlik Denetimi	Veri tabanının çalıştığı işletim sistemi üzerinde; komut çalıştırma, yerel dosya okuma/yazma vb. işlemlere imkân sağlayabilecek ayrıcalıkların sınırlandırılması için veri tabanı yönetim sistemi, desteklediği ölçüde yapılandırılmış mıdır?
5.2.1.10	Komut/Sorgu Geçmişi Kayıtlarının Güvenliğinin Sağlanması	Mülakat, Güvenlik Denetimi	Veri tabanı tarafından, üzerinde çalıştırılmış komut/sorgu geçmişi kayıt altına alınıyor mu? Böyle bir durumda ilgili kayıtların/dosyaların güvenliği nasıl sağlanmaktadır?
5.2.1.11	Yedeklerin Güvenliğinin Sağlanması	Mülakat, Güvenlik Denetimi	Yedek dosyaların güvenliği hangi yöntemler ile sağlanmaktadır?
5.2.1.12	Adanmış Sunucu Kullanılması	Mülakat, Güvenlik Denetimi	İlgili veri tabanı sunucusu adanmış sunucu mudur?
5.2.1.13	Kurulum Dosyalarının Güvenilir Kaynaklardan Temin Edilmesi	Mülakat, Güvenlik Denetimi	Kurulum dosyalarının/kurulum için kullanılan paketlerin, güvenilir kaynaklardan alınmış olduğu kontrol ediliyor mu?
5.2.1.14	Örnek Verilerin Silinmesi	Mülakat, Güvenlik Denetimi	Veri tabanında, kurulum ile gelen örnek veriler (örnek tablolar, kayıtlar, kullanıcılar vb.) bulunuyor mu?
5.2.1.15	Veri Tabanı Sistem Dosyalarının ve İz Kayıtlarının Aynı Disk Bölümü Üzerinde Bulunmaması	Mülakat, Güvenlik Denetimi	Veri tabanı tarafından kullanılan sistem dosyaları hangi disk bölümü üzerinde bulunmaktadır? Veri tabanı tarafından üretilen iz kayıtları hangi disk bölümü üzerinde bulunmaktadır? Sistem bölümü, hangi disk bölümü üzerindedir?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
5.2.1.16	Veri Tabanında Tablo ve Nesne Düzeyinde Yetkilendirme Yapılması	Mülakat, Güvenlik Denetimi	Kritik veri içeren tablo ve nesneler için tablo ve/veya nesne bazında yetkilendirme kullanılıyor mu?
5.2.1.17	İşletim Sistemi Üzerinde Veri Tabanı Servisi Çalıştıran Kullanıcıların Yönetici Haklarına Sahip Olmaması	Mülakat, Güvenlik Denetimi	İşletim sistemi üzerinde veri tabanı servis(ler)ini çalıştıran kullanıcılar için en az yetki prensibi uygulanmış mıdır?
5.2.1.18	Kümeleme veya Replikasyon İçinde Bulunan Veri Tabanı Sunucuları Arası İletişimin Güvenliğinin Sağlanması	Mülakat, Güvenlik Denetimi	Kümeleme ve/veya replikasyon içinde veri tabanı sunucuları mevcut mudur? Bu sunucular arasında gerçekleşen iletişim şifreli olarak mı yapılmaktadır? İlgili süreçlerde kullanılacak hesaplarda en az yetki prensibi uygulanmakta mıdır?
5.2.1.19	Merkezi Kimlik Doğrulama Sisteminin Kullanılması	Mülakat, Güvenlik Denetimi	Merkezi kimlik doğrulama sistemi kullanılmakta mıdır?
5.2.1.20	Kritik Bilgi İçeren Veri Tabanı Sunucularında Durağan Verinin Güvenliğinin Sağlanması	Mülakat, Güvenlik Denetimi	Kritik veri içeren veri tabanı sunucularında bulunan hareketsiz verinin (data at rest) güvenliği nasıl sağlanmaktadır?
5.2.1.21	Veri Tabanı Sunucusu ile İstemci Arasındaki İletişimin Şifreli Olması	Mülakat, Güvenlik Denetimi	Veri tabanı sunucusu ile istemci arasındaki iletişim şifreli trafik üzerinden mi sağlanmaktadır?

5.3. Sunucu Sıkılaştırma Tedbirleri

Amaç

Bu güvenlik tedbiri ana başlığının amacı, sunucu güvenlik sıkılaştırmaları çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. “Sunucu Sıkılaştırma Tedbirleri” ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Web Sunucusu Sıkılaştırma Tedbirleri
- Sanallaştırma Sunucusu Sıkılaştırma Tedbirleri

5.3.1. Web Sunucusu Sıkılaştırma Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.3.1.1	1	Güncel Web Sunucu Yazılımlarının Kullanılması	Web sunucu yazılımlarının güncel, zafiyet içermeyen ve üreticisi tarafından desteği devam eden kararlı sürümleri kullanılmalıdır. Ayrıca, sunucuda kullanımda olan tüm araçların/paket programların güvenlik yamaları için düzenli aralıklarla kontrol yapılmalıdır.
5.3.1.2	1	WebDAV Desteğinin Kaldırılması	Web sunucusunun WebDAV (Web Distributed Authoring and Versioning) desteği kaldırılmalıdır. WebDAV ile ilgili modüller pasif hale getirilmelidir.
5.3.1.3	1	Web Sunucusu Kullanıcı Yönetimi	Web sunucu yazılımı yönetici hesabıyla değil, bu amaç için özel olarak oluşturulmuş bir hesap ile çalıştırılmalıdır. Web sunucusunda bulunan varsayılan hesaplar/parolalar kullanım dışı bırakılmalıdır.
5.3.1.4	1	Web Sunucusunun Bilgi İfşalarını Önleyecek Şekilde Yapılandırılması	Web sunucusu bilgi ifşalarını önleyecek şekilde yapılandırılmalıdır. Varsayılan hata ve kurulum sayfaları kaldırılmalıdır. Web sunucu teknolojisi hakkında bilgi ifşasına neden olan HTTP başlıkları kaldırılmalıdır. Hatalı HTTP isteklerine dönen cevaplarda bilgi ifşasına izin verilmemelidir.
5.3.1.5	1	Desteklenen HTTP Metotlarının Kısıtlanması	POST, GET, OPTIONS ve HEAD metotları dışında diğer HTTP metotları desteklenmemelidir. PUT, DELETE, PROPFIND gibi metotlar web servisi için kullanılıyorsa, kullanımlarının sadece web servis ihtiyaçları ile sınırlı olup olmadığı kontrol edilmelidir. Bu metotların dosya yükleme veya silme gibi farklı amaçlarla kullanımı engellenmelidir.
5.3.1.6	1	Dizin Listelemenin Pasif Hale Getirilmesi	Dizin listelemesi pasif hale getirilmelidir.
5.3.1.7	1	Debug Modunun Kapalı Olması	Web sunucu yazılımı debug (hata ayıklama) modunda çalıştırılmamalıdır.
5.3.1.8	1	İstek Limitlerinin Tanımlanması	Web sunucu yazılımının desteklediği ölçüde, istekler için limitler belirlenmelidir.
5.3.1.9	1	İz Kayıtlarının Alınması	Web sunucu yazılımına ilişkin iz kayıtları alınmalıdır. Bk. Tedbir No: 3.1.8.1
5.3.1.10	1	Yazma İzni Olan Dizinlerin Kısıtlanması	Yazma izni olan dizinler belirlenmeli, yazma yetkileri sadece dosya yükleme ihtiyacı olan dizinlere verilmelidir. Uygulama üzerinden yüklenen dosyalar için oluşturulmuş dizinlerde çalıştırma izni kaldırılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.3.1.11	1	SSL/TLS Kullanımı	Sunucu SSL/TLS kullanımına elverişli yapılandırılmalıdır. Bu kapsamda, sunucuda sadece, bilinen zafiyet içermeyen güvenilir sürüme sahip SSL/TLS versiyonları kullanılmalıdır. Bk. Tedbir No: 3.2.9.1
5.3.1.12	1	İsteklerin HTTP'den HTTPS'e Yönlendirilmesi	Web sunucusundaki herhangi bir HTTP bağlantı noktası, şifreleme kullanan bir sunucu bağlantı noktasına yönlendirmelidir.
5.3.1.13	1	Kullanılmayan Modüllerin Kaldırılması	Sunucuda sadece kullanılan modüllerin aktif olmalıdır.
5.3.1.14	1	Açık Portların Kısıtlanması	Web sunucusu yalnızca yetkili bağlantı noktalarındaki ağ bağlantılarını dinlemelidir. Kullanımda olmayan portlar kapatılmalıdır. Bk. Tedbir No: 5.1.1.2
5.3.1.15	1	Kaynak Kullanım Optimizasyonu	Uygulama seviyesinde yapılabilecek servis dışı bırakma saldırılarına karşı aşağıdaki sunucu üzerinde aşağıdaki sıkılaştırmalar yapılmalıdır: • Sunucunun kabul edebileceği maksimum kullanıcı sayısı artırılmalıdır. • Tek bir IP adresinden yapılabilecek bağlantı sayısı sınırlandırılmalıdır. • Her bir bağlantının kullanabileceği maksimum ve minimum transfer hızı belirlenmelidir. • Bağlantılar için zaman aşım değeri belirlenmeli, belirli bir süre açık kalan bağlantılar sonlandırılmalıdır.
5.3.1.16	1	Sunucunun Korumalı ve Ayrıştırılmış Şekilde Kurulumu	İnternete açık olarak çalışan web sunucu ayrı bir bölgede (DMZ vb.) tutulmalıdır. Bk. Tedbir No: 3.2.5.3 Bk. Tedbir No: 3.1.6.6
5.3.1.17	1	Sunucuda Koruyucu HTTP Başlıklarının Kullanımı	Sunucu tarafında koruyucu HTTP başlıkları (X-Frame-Options, Strict-Transport-Security vb.) yapılandırılmalıdır.
5.3.1.18	1	Sunucunun Özel Anahtarının (Private Key) Korunması	Sunucunun özel anahtarına (private key) yapılacak yetkisiz erişimlere karşı önlemler alınmalıdır.
5.3.1.19	2	İz Kayıtlarının Merkezi Kayıt Sistemine Gönderilmesi	Web sunucularından alınan iz kayıtları merkezi bir kayıt sistemine gönderilmelidir. Bk. Tedbir No: 3.1.8.6

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.3.1.20	2	Sunucuya IP Adresi Üzerinden Erişimlerin Engellenmesi	Sunucuya IP adresi üzerinden yapılan erişimler engellenmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
5.3.1.1	Güncel Web Sunucu Yazılımlarının Kullanılması	Mülakat, Güvenlik Denetimi	Web sunucu yazılımlarının güncel, zafiyet içermeyen ve üreticisi tarafından desteği devam eden kararlı sürümleri mi kullanılmaktadır?
5.3.1.2	WebDAV Desteğinin Kaldırılması	Mülakat, Güvenlik Denetimi, Sızma Testi	Web sunucusunun WebDAV (Web Distributed Authoring and Versioning) desteği bulunmakta mıdır? WebDAV ile ilgili modullerden aktif durumda olan var mıdır?
5.3.1.3	Web Sunucusu Kullanıcı Yönetimi	Mülakat, Güvenlik Denetimi	Web sunucu yazılımı hangi kullanıcı hesabıyla çalıştırılmaktadır? Web sunucusunda bulunan varsayılan hesaplar/parolalar kullanım dışı bırakılmış mıdır?
5.3.1.4	Web Sunucusunun Bilgi İfşalarını Önleyecek Şekilde Yapılandırılması	Mülakat, Sızma Testi	Web sunucusu bilgi ifşalarını önleyecek şekilde yapılandırılmış mıdır? Web sunucu teknolojisi hakkında bilgi ifşasına neden olan HTTP başlıkları kaldırılmış mıdır? Olağan dışı (hatalı) HTTP isteklerine dönülen yanıtlarda bilgi ifşası olmaması için kontrol sağlanmış mıdır?
5.3.1.5	Desteklenen HTTP Metotlarının Kısıtlanması	Mülakat, Sızma Testi	Uygulama gereksinimleri dışındaki tüm HTTP metotları kısıtlanmış mıdır?
5.3.1.6	Dizin Listelemenin Pasif Hale Getirilmesi	Mülakat, Sızma Testi	Sunucuda dizin listelemesi pasif hale getirilmiş midir?
5.3.1.7	Debug Modunun Kapalı Olması	Mülakat, Gözden Geçirme, Sızma Testi	Web sunucu yazılımı debug modunda çalıştırılabilmekte midir?
5.3.1.8	İstek Limitlerinin Tanımlanması	Mülakat, Gözden Geçirme, Sızma Testi	Web sunucu yazılımının desteklediği ölçüde, istekler için limitler belirlenmiş midir?
5.3.1.9	İz Kayıtlarının Alınması	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Web sunucu yazılımına ilişkin iz kayıtları alınmakta mıdır? Alınan iz kayıtları kurum politikaları ve ilgili mevzuatlarda belirtilen süre boyunca saklanmakta mıdır?
5.3.1.10	Yazma İzni Olan Dizinlerin Kısıtlanması	Mülakat, Güvenlik Denetimi, Sızma Testi	Sunucuda yazma izni olan dizin bulunuyor mudur? Bu dizinlerde düzenleme yapılmış mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
5.3.1.11	SSL/TLS Kullanımı	Mülakat, Gözden Geçirme, Sızma Testi	Sunucu SSL/TLS kullanımına elverişli yapılandırılmış mıdır? Sunucuda hangi SSL/TLS sürümü kullanılmaktadır?
5.3.1.12	İsteklerin HTTP'den HTTPS'e Yönlendirilmesi	Mülakat, Gözden Geçirme, Sızma Testi	Web sunucusundaki tüm HTTP bağlantı noktaları şifreleme kullanan bir sunucu bağlantı noktasına yönlendiriliyor mudur?
5.3.1.13	Kullanılmayan Modüllerin Kaldırılması	Mülakat, Güvenlik Denetimi, Sızma Testi	Sunucuda kullanılmayan modüller kaldırılmış mıdır?
5.3.1.14	Açık Portların Kısıtlanması	Mülakat, Güvenlik Denetimi, Sızma Testi	Web sunucusunun yalnızca yetkili bağlantı noktalarındaki ağ bağlantıları mı dinlenmektedir? Kullanımda olmayan portlar kapatılmış mıdır?
5.3.1.15	Kaynak Kullanım Optimizasyonu	Mülakat, Sızma Testi	Tek bir IP adresi üzerinden yapılabilecek maksimum bağlantı sayısı belirlenmiş midir? Uzun süre açık kalan bağlantılar kapatılmakta mıdır? Bağlantılar için maksimum ve minimum transfer hızı belirlenmiş midir?
5.3.1.16	Sunucunun Korumalı ve Ayrıştırılmış Şekilde Kurulumu	Mülakat, Güvenlik Denetimi, Sızma Testi	İnternete açık olarak çalışan web sunucu DMZ (DeMilitarized Zone) gibi ayrı bir bölgede tutulmakta mıdır?
5.3.1.17	Sunucuda Koruyucu HTTP Başlıklarının Kullanımı	Mülakat, Sızma Testi	Olası saldırılara karşın önlem olarak sunucu tarafında koruyucu HTTP başlıkları yapılandırılmış mıdır?
5.3.1.18	Sunucunun Özel Anahtarının (Private Key) Korunması	Mülakat, Güvenlik Denetimi, Sızma Testi	Sunucunun özel anahtarı (private key) yetkisiz erişime karşı korunmakta mıdır?
5.3.1.19	İz Kayıtlarının Merkezi Kayıt Sistemine Gönderilmesi	Mülakat, Gözden Geçirme	Web sunucularından alınan iz kayıtları merkezi bir kayıt sistemine gönderiliyor mudur?
5.3.1.20	Sunucuya IP Adresi Üzerinden Erişimlerin Engellenmesi	Mülakat, Güvenlik Denetimi, Sızma Testi	Sunucuya IP adresi üzerinden erişimler engellenmiş midir?

5.3.2. Sanallaştırma Sunucusu Sıkılaştırma Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.3.2.1	1	Güncel Sanallaştırma Yazılımının Kullanılması	Sanallaştırma sunucusunda kullanılan sanallaştırma yazılımı güncel olmalı ve mevcut güvenlik yamaları yüklü olmalıdır.
5.3.2.2	1	Konteynerların /Sanal Makinelerin Çalıştığı Ana Makine Üzerinde Sıkılaştırmaların Yapılması	Konteynerların/sanal makinelerin çalıştığı ana makine üzerinde sıkılaştırmalar yapılmalıdır. Bk. Bölüm 5.1
5.3.2.3	1	Sanal Makineler Arasında Zaman Senkronizasyonunun Sağlanması	Bk. Tedbir No: 5.1.1.11
5.3.2.4	1	Sanallaştırma Yazılımı Güvenlik Duvarının Aktif Olması	Sanallaştırma yazılımı ile beraber gelen güvenlik duvarı aktif olmalı ve sadece ihtiyaç duyulan portlar üzerinden ihtiyaç duyulan IP adreslerine erişime izin vermelidir.
5.3.2.5	1	Mantıksal Birim Numarası (LUN) Maskelemesi Yapılması	Depolama alanı ağı (SAN) etkinliğini ayırmak için imar ve mantıksal birim numarası (LUN) maskeleme kullanılmalıdır.
5.3.2.6	1	Sanallaştırma Ünitesi Üzerinden Konsol Erişimlerinin Kısıtlanması	Sanallaştırma ünitelerine erişim sağlayabilen kullanıcıların, sanal makinelerin sahibi olan kullanıcıların ekranlarını yetkisiz olarak görüntülemesi engellenmelidir. Ayrıca yetkisiz konsol erişimleri de engellenmelidir. Her kullanıcı kimlik doğrulaması sonrasında erişim sağlamalıdır.
5.3.2.7	1	Sanallaştırma Ünitesinde Kullanıcı Yetkilendirme	Sanallaştırma ünitesinde kullanıcılar en az yetki prensibine uygun şekilde ilgili kullanıcı rollerine atanmalıdır.
5.3.2.8	1	Gereksiz Hizmetlerin ve Kullanılmayan Donanımların Kaldırılması	Ana bilgisayardan ve sanal makinelerden gerekli olmayan tüm hizmetler/donanımlar kaldırılmalıdır. Örneğin, kullanılmayan sanal donanımlar (sürücüler, ağ adaptörleri vb.) devre dışı bırakılmalıdır. Ayrıca gereksiz hipervizör hizmetleri (pano paylaşımı, dosya paylaşımı vb.) devre dışı bırakılmalıdır.
5.3.2.9	1	Sanal Makineler Üzerindeki Diskler için Disk Küçültme Konfigürasyonuna Erişimin Kısıtlanması	Sanal disk küçültme (disk shrinking) işleminin sürekli olarak yapılması, sanal diskin kullanılamamasına ve veri kaybına sebebiyet verebileceği için bu ayarı yönetebilecek kullanıcılar belirlenerek, sadece bu kullanıcıların erişimine izin verilmelidir.
5.3.2.10	2	Sanallaştırma Yazılımının Merkezi Olarak Güncellenmesi	Sanallaştırma yazılımı çalıştığı tüm sunucularda merkezi olarak eş zamanlı güncellenmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.3.2.11	2	Sanal Makineler için İz Kayıtlarının Yönetilmesi	Sanallaştırma ortamında çalışan sanal makineler için alınan iz kayıtları kalıcı bir şekilde saklanmalıdır. Ayrıca bu iz kayıtları merkezi bir kayıt sistemine gönderilmelidir. Bk. Tedbir No: 3.1.8.1 Bk. Tedbir No: 3.1.8.6
5.3.2.12	2	Sanal Makinelerin Güvenli İmhası	Sanal makineler silinmeden önce, sanal makineye ait disk dosyalarına sıfır yazılmalı ve daha sonrasında kalıcı silme işlemi yapılmalıdır.
5.3.2.13	2	Hipervizörler Tarafından Sunulan Bellek Paylaşımı Özelliklerinin Kullanımı	Bellek paylaşımı (memory sharing) kullanılmıyor ise devre dışı bırakılmalıdır. Eğer bellek paylaşımı özelliği kullanılacak ise sanal makineler arasında gruplandırma gibi gerekli güvenlik önlemleri alınmalıdır.
5.3.2.14	2	Sunucu Yedeklerinin Alınması	Düzenli olarak sunucu sistem yedekleri alınmalıdır. Yedekler yetkisiz erişime karşı güvenli ortamlarda muhafaza edilmelidir. Belirli aralıklarla yedekten geri dönme testleri gerçekleştirilmelidir.
5.3.2.15	3	Disk ve İmajların Şifreli Olarak Saklanması	Sanal makineye ait imajlar ve anlık görüntüler şifreli olarak muhafaza edilmelidir. Ayrıca, sanal makinelerde disk seviyesinde şifreleme yapılmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
5.3.2.1	Güncel Sanallaştırma Yazılımının Kullanılması	Mülakat, Güvenlik Denetimi	Sanallaştırma sunucusu için kullanılan sanallaştırma yazılımı güncel midir?
5.3.2.2	Konteynerların /Sanal Makinelerin Çalıştığı Ana Makine Üzerinde Sıkılaştırmaların Yapılması	Mülakat, Güvenlik Denetimi	İşletim sistemi sıkılaştırmaları en iyi çözüm önerilerine uygun mudur? Bk. Bölüm 5.1
5.3.2.3	Sanal Makineler Arasında Zaman Senkronizasyonunun Sağlanması	Mülakat, Güvenlik Denetimi	Sanal makineler arasında zaman senkronizasyonunun sağlanması için gerekli yapılandırma sağlanmış mıdır?
5.3.2.4	Sanallaştırma Yazılımı Güvenlik Duvarının Aktif Olması	Mülakat, Güvenlik Denetimi	Sanallaştırma yazılımı güvenlik duvarı aktif midir?
5.3.2.5	Mantıksal Birim Numarası (LUN) Maskelemesi Yapılması	Mülakat, Güvenlik Denetimi	SAN etkinliğini ayırmak için LUN maskeleme yapılmış mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
5.3.2.6	Sanallaştırma Ünitesi Üzerinden Konsol Erişimlerinin Kısıtlanması	Mülakat, Güvenlik Denetimi	Sanallaştırma ünitesi üzerinde konsol kısıtlaması için gerekli yapılandırma var mıdır?
5.3.2.7	Sanallaştırma Ünitesinde Kullanıcı Yetkilendirme	Mülakat, Güvenlik Denetimi	Sanal makinelere ait imajlar ve anlık görüntülere erişim yetkisi kimlere verilmektedir? Erişim yetkileri en az yetki prensibine uygun olarak mı verilmektedir?
5.3.2.8	Gereksiz Hizmetlerin ve Kullanılmayan Donanımların Kaldırılması	Mülakat, Güvenlik Denetimi	Ana makine ile sanal makine arasında dosya paylaşımında gerekli kısıtlamalar uygulanmış mıdır? Sanal makine üzerinde kullanılan/çalışmakta olan gereksiz donanım/hizmet mevcut mudur?
5.3.2.9	Sanal Makineler Üzerindeki Diskler için Disk Küçültme Konfigürasyonuna Erişimin Kısıtlanması	Mülakat, Güvenlik Denetimi	Disk kapasite küçültme işlemi için kullanıcı bazlı izin tanımlaması mevcut mudur?
5.3.2.10	Sanallaştırma Yazılımının Merkezi Olarak Güncellenmesi	Mülakat	Sanallaştırma yazılımı merkezi olarak güncellenmekte midir?
5.3.2.11	Sanal Makineler için İz Kayıtlarının Yönetilmesi	Mülakat, Gözden Geçirme	Sanal makineler için iz kayıtları tutulmakta mıdır? Tutulan bu kayıtlar merkezi bir kayıt sistemine gönderilmekte midir?
5.3.2.12	Sanal Makinelerin Güvenli İmhası	Mülakat, Gözden Geçirme	Sanal makinelerin güvenli imhası için belirli bir politika bulunmakta mıdır?
5.3.2.13	Hipervizörler Tarafından Sunulan Bellek Paylaşımı Özelliklerinin Kullanımı	Mülakat, Güvenlik Denetimi	Hipervizörler tarafından sunulan bellek paylaşımı özellikleri kullanılmakta mıdır? Sanal makineler arasında bellek paylaşımı ile ilgili bir gruplandırma yapılmış mıdır?
5.3.2.14	Sunucu Yedeklerinin Alınması	Mülakat, Gözden Geçirme	Sanallaştırma sisteminin yedeklemesi yapılmakta mıdır?
5.3.2.15	Disk ve İmajların Şifreli Olarak Saklanması	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Sanal makinelere ait diskler şifreli olarak korunmaktadır? Anlık görüntüler şifreli olarak korunmakta mıdır?

KAYNAKÇA

1. Bilişim Terimleri Sözlüğü, TSE (2006)
2. CIS (Center for Internet Security) Controls v7.1 (2019)
3. Cloud Controls Matrix 3.0.1 (2016)
4. NIST (National Institute of Standards and Technology) Framework for Improving Critical Infrastructure Cybersecurity (2018)
5. NIST IR (National Institute of Standards and Technology Internal Report) 8228 (2019)
6. OWASP (Open Web Application Security Project) Application Security Verification Standard 4.0 (2019)
7. OWASP (Open Web Application Security Project) IoT (Internet of Things) Security Guidance (2018)
8. OWASP (Open Web Application Security Project) Mobile Application Security Verification 1.1.4 (2019)
9. PCI DSS (Payment Card Industry Data Security Standard) Requirements and Security Assessment Procedures 3.2.1 (2018)
10. TS ISO/IEC 27001:2017 Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler Standardı (2017)
11. 24.03.2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu
12. 28.10.2017 tarihli Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik
13. 30.12.2017 tarihli Veri Sorumluları Sicili Hakkında Yönetmelik
14. 10.03.2018 tarihli Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ
15. 10.03.2018 tarihli Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ
16. 04.05.2017 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
17. TÜBİTAK BİLGEM Güvenli Yazılım Geliştirme Kılavuzu 1.1 (2018)
18. Kurumsal SOME Kurulum ve Yönetim Rehberi (2014)

EKLER

EK-A: GENELGE MADDELERİ EŞLEŞTİRME TABLOSU

06.07.2019 Tarihli ve 30823 Sayılı Resmi Gazete'de yayımlanan 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi'nde yer alan 21 adet tedbirin ilgili rehber başlıklarıyla eşleşmesi aşağıdaki tabloda yer almaktadır. Söz konusu maddelerin tabloya ilaveten farklı başlıklarla da ilişkilendirilmesi mümkündür. Genelge Maddesi doğrudan Rehber başlığıyla ilişkiliyse tablodaki ilgili hücreye A (Asıl) yazılmıştır. Genelge Maddesi ile Rehber başlığı arasında dolaylı bir ilişki varsa tablodaki ilgili hücreye D (Dolaylı / Destekleyici) yazılmıştır.

Madde No	Genelge Maddesi	Varlık Gruplarına Yönelik Güvenlik Tedbirleri						Uygulama ve Teknoloji Alanlarına Yönelik Güvenlik Tedbirleri					
		Ağ ve Sistem Güvenliği	Uygulama ve Veri Güvenliği	Taşınabilir Cihaz ve Ortam Güvenliği	Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği	Personel Güvenliği	Fiziksel Mekânların Güvenliği	Kişisel Verilerin Güvenliği	Anlık Mesajlaşma Güvenliği	Bulut Bilişim Güvenliği	Kripto Uygulamaları Güvenliği	Kritik Altyapılar Güvenliği	Yeni Geliştirmeler ve Tedarik
1	Nüfus, sağlık ve iletişim kayıt bilgileri ile genetik ve biyometrik veriler gibi kritik bilgi ve veriler yurtiçinde güvenli bir şekilde depolanacaktır.	A	A	D			D	A		A	A		
2	Kamu kurum ve kuruluşlarında yer alan kritik veriler, internete kapalı ve fiziksel güvenliği sağlanmış bir ortamda bulunan güvenli bir ağda tutulacak, bu ağda kullanılacak cihazlara erişim kontrollü olarak sağlanacak ve log kayıtları değiştirilmeye karşı önlem alınarak saklanacaktır.	A	D				A					A	
3	Kamu kurum ve kuruluşlarına ait veriler, kurumların kendi özel sistemleri veya kurum kontrolündeki yerli hizmet sağlayıcılar hariç bulut depolama hizmetlerinde saklanmayacaktır.	A	A				D			A			
4	Mevzuatta kodlu veya kriptolu haberleşmeye yetkilendirilmiş kurumlar tarafından geliştirilen yerli mobil uygulamalar hariç olmak üzere, mobil uygulamalar üzerinden, gizlilik dereceli veri paylaşımı ve haberleşme yapılmayacaktır.		A						A		D		

Madde No	Genelge Maddesi	Varlık Gruplarına Yönelik Güvenlik Tedbirleri						Uygulama ve Teknoloji Alanlarına Yönelik Güvenlik Tedbirleri					
		Ağ ve Sistem Güvenliği	Uygulama ve Veri Güvenliği	Taşınabilir Cihaz ve Ortam Güvenliği	Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği	Personel Güvenliği	Fiziksel Mekânların Güvenliği	Kişisel Verilerin Güvenliği	Anlık Mesajlaşma Güvenliği	Bulut Bilişim Güvenliği	Kripto Uygulamaları Güvenliği	Kritik Altyapılar Güvenliği	Yeni Geliştirmeler ve Tedarik
5	Sosyal medya üzerinden gizlilik dereceli veri paylaşımı ve haberleşme yapılmayacaktır.					A							
6	Sosyal medya ve haberleşme uygulamalarına ait yerli uygulamaların kullanımı tercih edilecektir.								A				
7	Kamu kurum ve kuruluşlarınca gizlilik dereceli bilgilerin işlendiği yerlerde yayma güvenliği (TEMPEST) veya benzeri güvenlik önlemleri alınacaktır.						A						
8	Kritik veri, doküman ve belgelerin bulunduğu ve/veya görüşmelerin gerçekleştirildiği çalışma odalarında/ortamlarında mobil cihazlar ve veri transferi özelliğine sahip cihazlar bulundurulmayacaktır.				D		A						
9	Gizlilik dereceli veya kurumsal mahremiyet içeren veri, doküman ve belgeler kurumsal olarak yetkilendirilmemiş veya kişisel olarak kullanılan cihazlarda (dizüstü bilgisayar, mobil cihaz, harici bellek vb.) bulundurulmayacaktır.	D		A	D	D							
10	Kişisel olarak kullanılanlar da dâhil olmak üzere kaynağından emin olunmayan taşınabilir cihazlar (dizüstü bilgisayar, mobil cihazlar, harici bellek/disk, CD/DVD vb.) kurum sistemlerine bağlanmayacaktır. Gizlilik dereceli verilerin saklandığı cihazlar, ancak içerisinde yer alan veriler donanımsal ve/veya yazılımsal olarak kriptolanmak suretiyle kurum dışına çıkarılabilecek; bu amaçla kullanılan cihazlar kayıt altına alınacaktır.	A		D								D	
11	Yerli ve milli kripto sistemlerinin geliştirilmesi teşvik edilerek, kurumlara ait gizlilik dereceli haberleşmenin bu sistemler üzerinden gerçekleştirilmesi sağlanacaktır.										A		

Madde No	Genelge Maddesi	Varlık Gruplarına Yönelik Güvenlik Tedbirleri						Uygulama ve Teknoloji Alanlarına Yönelik Güvenlik Tedbirleri					
		Ağ ve Sistem Güvenliği	Uygulama ve Veri Güvenliği	Taşınabilir Cihaz ve Ortam Güvenliği	Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği	Personel Güvenliği	Fiziksel Mekânların Güvenliği	Kişisel Verilerin Güvenliği	Anlık Mesajlaşma Güvenliği	Bulut Bilişim Güvenliği	Kripto Uygulamaları Güvenliği	Kritik Altyapılar Güvenliği	Yeni Geliştirmeler ve Tedarik
12	Kamu kurum ve kuruluşlarınca temin edilecek yazılım veya donanımların kullanım amacına uygun olmayan bir özellik ve arka kapı (kullanıcıların bilgisi/izni olmaksızın sistemlere erişim imkânı sağlayan güvenlik zafiyeti) açıklığı içermediğine dair üretici ve/veya tedarikçilerden imkânlar ölçüsünde taahhütname alınacaktır.		A			D							D
13	Yazılımların güvenli olarak geliştirilmesi ile ilgili tedbirler alınacaktır. Temin edilen veya geliştirilen yazılımlar kullanılmadan önce güvenlik testlerinden geçirilerek kullanılacaktır.	D	A						D				D
14	Kurum ve kuruluşlar, siber tehdit bildirimleri ile ilgili gerekli tedbirleri alacaktır.	A										A	
15	Üst düzey yöneticiler de dâhil olmak üzere, personelin sistemlere erişim yetkilendirmelerinin, fiilen yürütülen işler ve ihtiyaçlar nazara alınarak yapılması sağlanacaktır.	A	A			A	A	A					
16	Endüstriyel kontrol sistemlerinin, internete kapalı konumda tutulması sağlanacak, söz konusu sistemlerin internete açık olmasının zorunlu olduğu durumlarda ise gerekli güvenlik önlemleri (güvenlik duvarı, uçtan uca tünelleme yöntemleri, yetkilendirme ve kimliklendirme mekanizmaları vb.) alınacaktır.	D	D									A	
17	Milli güvenliği doğrudan etkileyen stratejik önemi haiz kurum ve kuruluşların üst yöneticileri ile kritik altyapı, tesis ve projelerde görev alacak kritik önemi haiz personel hakkında ilgili mevzuat çerçevesinde güvenlik soruşturması veya arşiv araştırması yaptırılacaktır.					A							

Madde No	Genelge Maddesi	Varlık Gruplarına Yönelik Güvenlik Tedbirleri						Uygulama ve Teknoloji Alanlarına Yönelik Güvenlik Tedbirleri					
		Ağ ve Sistem Güvenliği	Uygulama ve Veri Güvenliği	Taşınabilir Cihaz ve Ortam Güvenliği	Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği	Personel Güvenliği	Fiziksel Mekânların Güvenliği	Kişisel Verilerin Güvenliği	Anlık Mesajlaşma Güvenliği	Bulut Bilişim Güvenliği	Kripto Uygulamaları Güvenliği	Kritik Altyapılar Güvenliği	Yeni Geliştirmeler ve Tedarik
18	Kamu e-posta sistemlerinin ayarları güvenli olacak biçimde yapılandırılacak, e-posta sunucuları, ülkemizde ve kurumun kontrolünde bulundurulacak ve sunucular arasındaki iletişimin şifreli olarak yapılması sağlanacaktır.	A							A	D			
19	Kurumsal olmayan şahsi e-posta adreslerinden kurumsal iletişim yapılmayacak, kurumsal e-postalar şahsi amaçlarla (özel iletişim, kişisel sosyal medya hesapları vb.) kullanılmayacaktır.					A			D				
20	Haberleşme hizmeti sağlamak üzere yetkilendirilmiş işletmeciler Türkiye'de internet değişim noktası kurmakla yükümlüdür. Yurtiçinde değiştirilmesi gereken yurtiçi iletişim trafiğinin yurtdışına çıkarılmamasına yönelik tedbirler alınacaktır.											A	
21	İşletmeciler tarafından, kritik kurumların bulunduğu bölgelerdeki veriler, radyolink ve benzeri yöntemlerle taşınmayacak, fiber optik kablolar üzerinden taşınacaktır. Kritik veri iletişiminde, radyolink haberleşmesi kullanılmayacak; ancak kullanımın zorunlu olduğu durumlarda veriler milli kripto sistemlerine sahip cihazlar kullanılarak kriptolanacaktır.										A	A	

EK-B: ULUSLARARASI STANDARTLAR VE YAYIMLI KILAVUZLAR EŞLEŞTİRME TABLOSU

Rehber Ana Başlıkları	Standart/Yayımlı Doküman																		
	CMMC v1.0	ISO 27001:2017	CIS Controls v7.1	Cloud Controls Matrix 3.0.1	NIST 800-53	OWASP Application Security Verification Standard 4.0	OWASP Mobile Application Security Verification 1.1.4	TÜBİTAK BİLGEM Güvenli Yazılım Geliştirme Kılavuzu 1.1	Mobile Application Security Checklist 1.1	OWASP IoT Security Guidance	NIST 800-82	CIS Benchmark	ENISA Security Aspects of Virtualization	NIST 800-125	Ubuntu Server Guide - Security	Oracle Linux 7 Security Guide	DISA STIG - Canonical Ubuntu 16.04 LTS Security Technical Implementation Guide	DISA STIG - Red Hat Enterprise Linux 7 Security Technical Implementation Guide	Red Hat Enterprise Linux 8 Security Hardening
3.1 Ağ ve Sistem Güvenliği	+	+	+	+	+														
3.2 Uygulama ve Veri Güvenliği		+				+	+	+											
3.3 Taşınabilir Cihaz ve Ortam Güvenliği	+	+	+	+	+				+										
3.4 Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği		+							+	+									
3.5 Personel Güvenliği	+	+	+	+															
3.6 Fiziksel Mekânların Güvenliği	+	+		+															
4.1 Kişisel Verilerin Güvenliği		+																	
4.2 Anlık Mesajlaşma Güvenliği		+		+															

Rehber Ana Başlıkları	Standart/Yayımlı Doküman																		
	CMMC v1.0	ISO 27001:2017	CIS Controls v7.1	Cloud Controls Matrix 3.0.1	NIST 800-53	OWASP Application Security Verification Standard 4.0	OWASP Mobile Application Security Verification 1.1.4	TÜBİTAK BİLGEM Güvenli Yazılım Geliştirme Kılavuzu 1.1	Mobile Application Security Checklist 1.1	OWASP IoT Security Guidance	NIST 800-82	CIS Benchmark	ENISA Security Aspects of Virtualization	NIST 800-125	Ubuntu Server Guide - Security	Oracle Linux 7 Security Guide	DISA STIG - Canonical Ubuntu 16.04 LTS Security Technical Implementation Guide	DISA STIG - Red Hat Enterprise Linux 7 Security Technical Implementation Guide	Red Hat Enterprise Linux 8 Security Hardening
4.3 Bulut Bilişim Güvenliği		+		+															
4.4 Kripto Uygulamaları Güvenliği	+	+	+																
4.5 Kritik Altyapılar Güvenliği	+	+	+	+	+	+	+	+	+	+	+								
4.6 Yeni Geliştirmeler ve Tedarik	+	+	+	+															
5.1 İşletim Sistemi Sıkılaştırma												+			+	+	+	+	+
5.2 Veri Tabanı Sıkılaştırma												+							
5.3 Sunucu Sıkılaştırma												+	+	+					

EK-C: BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ UYGULAMA SÜRECİ KAPSAMINDA KULLANILACAK FORMLAR, ŞABLONLAR VE ÖRNEK DOKÜMANLAR

EK-C.1: VARLIK GRUBU KRİTİKLİK DERECELENDİRME ANKETİ

Bu anket, Rehber'de yer alan varlık grubu ana başlıkları altında yer alan ve Kurum tarafından belirlenen tüm varlık grupları için tek tek doldurulmalıdır.

Varlık Grupları Tanımlanırken Dikkat Edilecek Hususlar:

Kurum bilgi güvenliği yönetim sistemi kapsamında yer alan varlıkların, aşağıda listelenen altı varlık grubu ana başlığı altında gruplandırılması gerekmektedir.

1. Ağ ve Sistemler
2. Uygulamalar
3. Taşınabilir Cihaz ve Ortamlar
4. IoT Cihazları
5. Personel
6. Fiziksel Mekânlar

Aşağıda varlık grubu ana başlıkları altında bulunabilecek varlıklara örnekler verilmektedir. Varlık grubu ana başlıkları altında yer alan varlıklar gruplandırılarak bir veya daha fazla sayıda varlık grupları tanımlanmalıdır. Bu kapsamda varlık grubunda yer alan varlıkların envanteri yönetilmelidir. Tüm varlıkların en az bir varlık grubunda yer alması sağlanmalıdır.

- Ağ ve Sistemler:
    - Ağ: Yönlendirici, modem, gateway, kablosuz erişim noktası, ağ erişim kontrol cihazı, 3G haberleşme cihazları, sanal ağ, iç ağ, internet ağı vb.
    - BT Sistemleri: Kullanıcı bilgisayarları, sunucular, güvenlik duvarları, saldırı tespit/önleme sistemleri vb.
    - OT Sistemleri: SCADA sistemleri, RTU (Uzak Terminal Birimi) ve PLC (Programlanabilir Mantıksal Kontrolör) vb.
- Uygulamalar: Personel yazılımı, EBYS, kurum içi portal, e-Devlet uygulaması, ana hizmet uygulaması vb.
- Taşınabilir Cihaz ve Ortamlar: Kurum bilgisine erişebilen akıllı telefon, tablet, dizüstü bilgisayar, USB bellek, taşınabilir sabit disk, CD/DVD vb.
- Nesnelerin İnterneti (IoT) Cihazları: Kamera, sensör (nem, gaz, sıcaklık) vb.
- Personel: Üst yöneticiler, idari yöneticiler, sistem yöneticileri, yazılım geliştiriciler, son kullanıcılar, altyüklenici personeli vb.
- Fiziksel Mekânlar: Merkez veri merkezi, felaket kurtarma merkezi, taşra veri merkezi, personel odası, yönetici odası, kat anahtarlarının (switch) bulunduğu odalar vb.

Anket Doldurulurken Dikkat Edilecek Hususlar

Anket, ilgili varlık grubuyla alakalı paydaşların, Kurumun sahip olduğu en yetkin personelin ve yöneticilerin katılımı ile doldurulur. Anket doldurma çalışmasında delfi metodunun kullanılması önerilir.

Ankette her bir soru için sadece bir şık işaretlenebilir. Sorular, varlık grubu içerisinde yer alan en kritik ve en etkili varlık dikkate alınarak yanıtlanmalıdır. Soruların Kurumunuzla ilişkili birden fazla doğru cevabı varsa en yüksek puanlı olan şık seçilmelidir. Cevaplandırdığınız her seçeneğin gerekçesi de ayrıntılı olarak yazılmalıdır.

Varlık Grubu No / Adı:

Varlık Grubu için Anket Soruları

A) Varlık Grubunun İşlediği Veri Açısından Değerlendirilmesi

Gizlilik Boyutu:

1. Varlık grubunuzun işlediği en kritik bilginin açığa çıkması veya yetkisiz kişiler tarafından ele geçirilmesi durumunda;
    a. Herhangi bir zarar oluşmaz, Kurum ve kişiler işlerine devam edebilir.
    b. Kurumun ya da ilgili kişilerin işlerini ve çıkarlarını etkileyecek zararlar gelir.
    c. Milli güvenlik ve ulusal çıkarlara saygınlık anlamında zararlar gelir. Söz konusu zararın telafisi mümkündür.
    d. Milli güvenlik ve ulusal çıkarlara yaşamsal zararlar gelir. Söz konusu zararın telafisi mümkün olamaz.

Bütünlük Boyutu:

2. Varlık grubunuzun işlediği en kritik bilginin içeriğinin yetkisiz kişiler tarafından değiştirilmesi durumunda;
    a. Herhangi bir zarar oluşmaz. Kurum ve kişiler işlerine devam edebilir.
    b. Kurumun ya da ilgili kişilerin işlerini ve çıkarlarını etkileyecek zararlar gelir.
    c. Milli güvenlik ve ulusal çıkarlara saygınlık anlamında zararlar gelir. Söz konusu zararın telafisi mümkündür.
    d. Milli güvenlik ve ulusal çıkarlara yaşamsal zararlar gelir. Söz konusu zararın telafisi mümkün olamaz.

Erişilebilirlik Boyutu:

3. Varlık grubunuzdaki varlıklara bağımlılığı bulunan hizmetlerde, hizmetin en yoğun olarak kullanıldığı periyodu göz önünde bulundurduğunuzda en fazla tolere edebildiğiniz devre dışı kalma süresi nedir?
    a. 24 (yirmi dört) saatten fazla
    b. 8 (sekiz) – 24 (yirmi dört) saat arası
    c. 1 (bir) – 8 (sekiz) saat arası
    d. 1 (bir) saatten az

B) Varlık Grubunun Etki Alanı Açısından Değerlendirilmesi

Etkilenen Kişi Sayısı:

4. Varlık grubunuzda yer alan varlıklar üzerinde gizlilik, bütünlük ve erişilebilirlik boyutlarının tamamını etkileyecek, olası en kötü senaryoya sahip bir bilgi güvenliği ihlal olayı meydana geldiğinde doğrudan etkilenebilecek kişi sayısı;
    a. Binden azdır.
    b. Binden fazla, 10 binden azdır.
    c. 10 binden fazla, 100 binden azdır.
    d. 100 binden fazla, 1 milyondan azdır.
    e. 1 milyondan fazladır.

Toplumsal Sonuçlar:

5. Varlık grubunuzda yer alan varlıklar üzerinde gizlilik, bütünlük ve erişilebilirlik boyutlarının tamamını etkileyecek, olası en kötü senaryoya sahip bir bilgi güvenliği ihlal olayı meydana geldiğinde karşılaşılan durum aşağıdaki sonuçlardan hangisine yol açar?
    a. Toplumsal kargaşa olmaz, yazılı görsel basına intikal etmez.
    b. Toplumsal kargaşa olmaz, fakat olay yazılı görsel basına intikal eder.
    c. Toplumsal kargaşa meydana gelir.
    d. Can kaybı meydana gelir.
    e. Diğer (a, b, c, d seçeneklerinden daha yüksek etkili bir sonuç doğurması durumu)

Kurumsal Sonuçlar:

6. Varlık grubunuzda yer alan varlıklar üzerinde gizlilik, bütünlük ve erişilebilirlik boyutlarının tamamını etkileyecek, olası en kötü senaryoya sahip herhangi bir bilgi güvenliği ihlal olayı olduğunda söz konusu olayın Kuruma etkisi ne olur?
    a. Kuruma etkisi olmaz, Kurum mevcut organizasyonu ve itibarını devam ettirir.
    b. Kurumun itibarı olumsuz etkilemez, fakat bilgi güvenliği organizasyon yapısını etkiler ya da personel değişikliğine gidilir.
    c. Kurumun itibarı olumsuz etkilenir.

Sektörel Etki:

7. Varlık grubunun hizmet verdiği sektöre etkisi nedir?
    a. Varlık grubu kurumun ana fonksiyonuna/sektöre doğrudan hizmet vermemektedir.
    b. Kamu kurum ve kuruluşları ana fonksiyonlarını yerine getirir ve sektöre doğrudan hizmet eder.
    c. Düzenleyici ve denetleyici kurum ve kuruluşlar, büyük ölçekli sanayi ve ticari kurumlar, AR-GE kurumlarının ana fonksiyonlarını yerine getirir ve sektöre doğrudan hizmet eder.
    d. Enerji, su yönetimi, bankacılık ve finans, ulaştırma, elektronik haberleşme, sağlık ve milli güvenlik/savunma sektörlerindeki ana fonksiyonlardan birini yerine getirir ve sektöre doğrudan hizmet eder.

Bağımlı Varlıklar:

8. Diğer varlıkların (entegre olan diğer yazılımlar, sunucular vb.) yönetiminizdeki varlığa olan bağımlılığı göz önünde bulundurulduğunda, varlığınızın işlediği verinin (uygulanabilir durumlarda) gizlilik, bütünlük veya erişilebilirliğine zarar gelmesi durumunda;
    a. Bağımlılığı olan varlıkların çalışması etkilenmez.
    b. Bağımlı varlıkların çalışmasını etkileyecek zararlar oluşur ancak ana faaliyet devam eder.
    c. Bağımlı varlıkların çalışmasını etkileyecek zararlar oluşur ve ana faaliyette aksamalar meydana gelir.
    d. Bağımlı varlıkların çalışmasını etkileyecek zararlar oluşur ve ana faaliyet durur.
    e. Diğer (a, b, c, d seçeneklerinden daha yüksek etkili bir sonuç doğurması durumu)

Anket Özeti

Varlık Grubu No / Adı:

a) Anket çalışmasına katılan ve anketi dolduran kişilerle ilgili bilgiyi aşağıdaki tabloya yazınız.

No.	Anket Katılımcısı	Görevi / Unvanı	Birimi / Kurumu	İrtibat	Tarih
1					
2					
3					
4					
5					
6					
7					
8					
9					

b) Her soru için anket cevaplarını aşağıdaki tabloya işaretleyerek anket puanını hesaplayınız.

Boyut	Soru No.	Şıkların Puanları					Soru Puanı
		a	b	c	d	e	
İşlenen Veri Açısından							
Gizlilik	1	1 puan	2 puan	3 puan	5 puan		
Bütünlük	2	1 puan	2 puan	3 puan	5 puan		
Erişilebilirlik	3	1 puan	2 puan	3 puan	5 puan		
Etki Alanı Açısından							
Etkilenen Kişi Sayısı	4	1 puan	2 puan	3 puan	4 puan	5 puan	
Toplumsal Sonuçlar	5	1 puan	2 puan	3 puan	5 puan	6 puan	
Kurumsal Sonuçlar	6	1 puan	2 puan	3 puan			
Sektörel Etki	7	1 puan	2 puan	3 puan	5 puan		
Bağımlı Varlıklar	8	1 puan	2 puan	3 puan	5 puan	6 puan	
Anket Puanı (Tüm soruların puanlarının toplamı)							

c) Her soru için işaretlediğiniz cevap şıkkını, olası senaryoyu da belirterek, gerekçelendiriniz.

Soru No.	Açıklama/Gerekçe
1	
2	
3	
4	
5	
6	
7	
8	

d) Anket puanına göre varlık grubunun kritiklik derecesini aşağıdaki tablodan faydalanarak belirleyiniz.

Anket Puanı	Varlık Grubu Kritiklik Derecesi
Anket puanı 18'den küçük ise	Derece 1
Anket puanı 18 (dâhil) ile 28 arasında ise	Derece 2
Anket puanı 28 ve daha yüksek ise	Derece 3

e) Varlık Grubu için Kritiklik Derecelendirme Anketi sonuçlarını aşağıdaki tabloda özetleyiniz.

Varlık Grubu No/Adı			
Anket Tamamlanma Tarihi			
Anket Çalışması Koordinatörü			
Anket Puanı (Tüm soruların puanlarının toplamı)			
Varlık Grubu Kritiklik Derecesi	Derece 1	Derece 2	Derece 3
	○	○	○

f) Anket sonuçlarını onaylayan yetkililerin bilgilerini yazınız.

Anket Sonucu Onay Tarihi	
Anket Sonuçlarını Onaylayan Yetkili	
Anket Sonuçlarını Onaylayan Yetkilinin İmzası	

EK-C.2: VARLIK GRUBU VE KRİTİKLİK DERECESİ TANIMLAMA FORMU

Varlık grubunda yer alan tüm varlıklar göz önünde bulundurularak, varlık grubu ile ilişkili uygulama ve teknoloji alanlarına yönelik uygulanması gereken güvenlik tedbirleri ile ilgili sıkılaştırma tedbirleri, varlık grubu kritiklik derecesi ile birlikte aşağıdaki tabloda kayıt altına alınmalıdır.

Varlık Grubu Ana Başlığı	**Varlık Grubu No**	**Varlık Grubu Adı**	**Uygulama ve Teknoloji Alanlarına Yönelik Güvenlik Tedbirleri** (Her varlık grubu için aşağıdaki başlıkların Uygulanabilir (U) / Uygulanabilir Değil (UD) olduğunu belirtiniz.)						**Sıkılaştırma Tedbirleri** (Her varlık grubu için aşağıdaki başlıkların Uygulanabilir (U) / Uygulanabilir Değil (UD) olduğunu belirtiniz.)			**Kritiklik Derecesi (Derece 1/ Derece 2/ Derece 3)**
			Kişisel Verilerin Güvenliği	**Anlık Mesajlaşma Güvenliği**	**Bulut Bilişim Güvenliği**	**Kripto Uygulamaları Güvenliği**	**Kritik Altyapılar Güvenliği**	**Yeni Geliştirmeler ve Tedarik**	**İşletim Sistemi Sıkılaştırma Tedbirleri**	**Veri Tabanı Sıkılaştırma Tedbirleri**	**Sunucu Sıkılaştırma Tedbirleri**	
Ağ ve Sistemler												
Uygulamalar												
Taşınabilir Cihaz ve Ortamlar												
Nesnelerin İnterneti (IoT) Cihazları												
Fiziksel Mekânlar												
Personel												

EK-C.3: MEVCUT DURUM VE BOŞLUK ANALİZ FORMU

Her bir varlık grubu için tedbir maddelerinin uygulanıp uygulanmadığı Uygulama Durumu açıklamaları dikkate alınarak belirlenmelidir. Mevcut duruma yönelik açıklamalar detaylı olarak belirtilmelidir. Ayrıca ilgili varlık grubu için hedeflenen duruma ulaşılması amacıyla yapılması gereken çalışmalar aşağıdaki tabloda kayıt altına alınmalıdır.

- Tedbir varlık grubunda yer alan tüm varlıklara uygulanmakta ise "tamamen"(T)
- Tedbir varlık grubunda yer alan varlıkların çoğuna uygulanmakta fakat bazı varlıklara kısmen uygulanmakta veya henüz uygulanmamakta ise "çoğunlukla" (Ç)
- Tedbir varlık grubunda yer alan bir kısım varlığa uygulanmakta veya tedbir kısmen uygulanmakta ise "kısmen"(K)
- Tedbir hiç uygulanmamakta ise "hiç" (H)
- Tedbirin teknik olarak uygulanma ihtimali bulunmuyorsa "uygulanamaz"(UD)

Varlık Grubu Adı / Kodu:	

Tedbir No	Uygulanma Durumu * (T/Ç/K/H/UD)	Mevcut Duruma Yönelik Açıklama	Hedeflenen Durum (T/Ç/K/H/UD)	Telafi Edici Kontrol ** (Tedbirin Birebir Uygulanamadığı Durumda)	Hedeflenen Durum İçin Yapılması Gereken Çalışmalar

* Varlık gruplarının mevcut durum ve boşluk analizi kapsamında belirlenen çalışmalar yazılmalıdır.

** Tedbir için telafi edici kontrol tanımlanması gerekiyorsa EK-C.5 formu doldurulur ve kontrol formunun numarası bu bölüme girilir.

EK-C.4: REHBER UYGULAMA YOL HARİTASI BELİRLEME FORMU

Mevcut durum ve boşluk analizi kapsamında yapılan çalışmalar göz önünde bulundurarak yapılması gereken iş paketleri ve bu kapsamda yapılacak 3 - 24 aylık çalışmalar aşağıdaki tabloda kayıt altına alınmalıdır.

İş Paketi No	İş Paketi Adı	İş Paketinin Kapsadığı Faaliyetler	İş Paketi Hedefleri	
			3.Ay	
			6.Ay	
			9.Ay	
			12.Ay	
			15.Ay	
			18.Ay	
			21.Ay	
			24.Ay	

EK-C.5: TELAFİ EDİCİ KONTROL KAYIT FORMU

Kurum, boşluk analizi sonucunda uygulanması gereken ilave tedbirler kapsamındaki herhangi bir gereksinimi; üst yönetim tarafından onaylanmış teknik kısıtlamalar ve iş gereksinimlerinden dolayı rehberde tanımlandığı şekli ile karşılayamaması durumunda telafi edici kontroller uygulamalıdır. Telafi edici kontroller, yerine uygulandıkları tedbir maddeleri ile aynı amaç ve etkiye sahip olmaları durumunda kullanılabilir olarak kabul edilecektir. Tedbir maddesi ile ilgili gereklilikleri karşılamak amacıyla kullanılan her bir telafi edici kontrolü tanımlamak için aşağıdaki form kullanılmalıdır.

TELAFİ EDİCİ KONTROLE YÖNELİK BİLGİ		AÇIKLAMA
Telafi Edici Kontrolün Numarası	Telafi edici kontrole ait numara bilgisi	
Telafi Edici Kontrolün Tanımı	Güvenlik tedbir maddesi yerine uygulanan telafi edici kontrolün tanımının yapıldığı alan	
Telafi Edici Kontrolün Niteliği (Geçici / Kalıcı)	Telafi edici kontrolün geçici ya da kalıcı nitelikte olduğunun tanımlandığı alan	
Telafi Edici Kontrolün Geçici Olması Durumunda Planlanan Uygulama Zaman Aralığı	Telafi edici kontrolün geçici nitelikte olması durumunda, kontrolün planlanan uygulama zaman aralığı	
İlişkili Güvenlik Tedbiri Madde Numarası	Telafi edici kontrolün hangi güvenlik tedbiri yerine uygulanacağının tanımlandığı alan	
İlişkili Güvenlik Tedbiri Gereklilikleri	Telafi edici kontrolün ilişkili olduğu güvenlik tedbir maddesinin gerekliliklerinin tanımlandığı alan	
İlişkili Güvenlik Tedbirinin Uygulanamamasından Kaynaklanan Riskler	Güvenlik tedbir maddesinin uygulanmaması durumunda ortaya çıkacak risklere yönelik açıklamaların yapıldığı alan	
İlişkili Güvenlik Tedbirinin Uygulanamamasının Gerekçeleri	Güvenlik tedbir maddesinin mevcut durumda uygulanamamasının nedenlerinin, uygulama kısıtlarının ve gerekçelerinin tanımlandığı alan	
Telafi Edici Kontrolün Doğrulama Yöntemi	Telafi edici kontrolün etkinliği ve yeterliliğine yönelik yapılan doğrulama ve test faaliyetlerinin açıklandığı alan	

EK-C.6: TAAHHÜTNAME ÖRNEĞİ

İşbu taahhütname, 06.07.2019 tarih ve 30823 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren 2019/12 sayılı Bilgi ve İletişim Güvenliği Tedbirleri konulu Cumhurbaşkanlığı Genelgesi'nin 12. maddesinde yer alan hükme dayanılarak hazırlanmıştır.

1. Tanımlar ve Kısaltmalar

İşbu taahhütnamede geçen;

1.1. "Arka kapı", Uygulama yazılımı, donanım ve işletim sistemleri veya bu bileşenlerin bir ya da birkaçını üzerinde barındıran cihaz/sistemlerde mevcut güvenlik önlemlerini aşarak erişim sağlamak üzere özel olarak tasarlanan ve/veya kasıtlı olarak dâhil edilmiş boşluklar veya güvenlik açıklarını,

1.2. "Dağıtıcı", Bir üreticiye ait olan ürünlerin belirli bölgelerde tanıtımı ve satışını sağlamakla yetkili tüzel kişiyi,

1.3. "Kurum", …… adresinde faaliyet göstermekte olan …….. Kurumu'nu,

1.4. "Tedarikçi", tedarik zincirinde yer alan, üretici ve dağıtıcı dışındaki tüzel kişiyi,

1.5. "Üretici", ürünü üreten, imal eden veya ürüne adını, ticari markasını veya ayırt edici işaretini koyan tüzel kişiyi,

1.6. "Ürün", Kurum tarafından tedarik edilmesi planlanan uygulama yazılımı, donanım, işletim sistemi veya bu bileşenlerin bir ya da birkaçını üzerinde barındıran cihaz/sistemi,

1.7. "Şirket", işbu taahhütnamede yer alan yükümlülüklerden sorumlu üretici, dağıtıcı veya tedarikçiyi

ifade etmektedir.

2. Ürün Özellikleri

Üretici	
Ürünün Markası	
Ürünün Adı	
Ürünün Modeli	
Ürün Üzerindeki Yazılımlara Ait Versiyon Bilgisi	
Ürünü Kapsayan Ulusal/Uluslararası Standartlar	

3. Yükümlülükler

3.1. İşbu taahhütnamenin 2. maddesinde özellikleri belirtilen ürünün, Kurum yetkililerinin bilgisi ve izni olmadan; ürünü veya ürün içerisindeki herhangi bir bileşeni devre dışı bırakmak, yetkisiz kod çalıştırmak, ürün içerisindeki verilere erişim sağlamak, verileri silmek ya da bütünlüğünü bozmak amacıyla tasarlanmış herhangi bir arka kapı bulunmadığını,

3.2. Ürüne bakım, onarım ve garanti süreci dâhil olmak üzere tüm yaşam döngüsü süresince şirket tarafından sunulan yama ve güncellemeler ile yeni versiyonların kurulum ve yönetim süreçlerinde işbu taahhütnamenin 3.1. maddesinde yer alan hükümlere herhangi bir uygunsuzluk olmayacağını,

3.3. Yukarıda beyan ve taahhüt edilen yükümlülüklere uyulmadığı ve/veya Kurum tarafından, verdiğimiz bilgilerde gerçeğe aykırı durumların saptanması halinde, Kurum tarafından bu konuda alınacak kararlara uyacağımızı ve uygulanacak yaptırımların tarafımıza doğrudan uygulanma kabiliyeti bulunduğunu kabul ve taahhüt ederiz.

4. Muhtelif Hükümler

4.1. İşbu taahhütnamede yer almayan hususlarda Türkiye Cumhuriyeti mevzuat hükümleri uygulanacaktır.

4.2. İşbu taahhütnameden kaynaklanan uyuşmazlıklarda yalnız …….. Mahkemeleri yetkili olacaktır.

4.3. İşbu taahhütnamenin hükümlerinden biri ya da birkaçının kısmen veya tamamen geçersiz addedilmesi, taahhütnamenin kalan hükümlerinin geçerliliğine etki etmeyecektir.

4.4. İşbu taahhütname kapsamında şirkete yapılacak bildirim, tebligat ve diğer haberleşme yöntemlerinde aşağıda şirket yetkilileri tarafından beyan edilen adres(ler) ve diğer iletişim bilgileri geçerlidir. Şirket adres değişikliklerini derhal noter yolu ile Kurum'a bildirmek zorundadır. Aksi halde taahhütnamede belirtilen adreslere yapılan tebligatlar geçerli olacaktır.

4.5. İşbu taahhütname şirketi temsil ve ilzama yetkili kişiler tarafından imzalanmış olup imza tarihi itibarıyla ……. (süresince) yürürlükte kalacaktır.

Taahhütte Bulunan Şirketin

Unvanı:

Adresi:

Telefon / Faks:

Vergi Dairesi:

Vergi Numarası:

Ticaret Sicil Numarası:

Tedarik Zincirindeki Rolü: ☐ Üretici ☐ Dağıtıcı ☐ Tedarikçi

Taahhütte Bulunan Şirketi Temsil ve İlzama Yetkili Kişi(ler)

İmza Tarihi:

Yetkili Kişi Ad – Soyad	Yetkili Kişi Ad – Soyad	Yetkili Kişi Ad – Soyad
Kaşe/İmza	Kaşe/İmza	Kaşe/İmza