UNVAN DEĞİŞİKLİĞİ SINAVI

BİLGİSAYAR TEKNİKERLİĞİ

DERS NOTLARI

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

- Yazılım Geliştirme Şube Müdürlüğü talep edilen projeleri inceleyerek etkin, doğru ve fonksiyonel proje geliştirme planlarının oluşturulması
- Tüm yazılım geliştirme süreçlerine ait standartların tarif edildiği teknik dokümanların hazırlanması ve uygulanması,
- Geliştirilecek veya değişiklik yapılacak projeler için; Analiz, tasarım, kodlama, test ve uygulamaya verme planlarının hazırlanması ve uygulanması,
- Kullanıcılardan gelen hatalar, istekler ve mevzuat değişikliklerini tetkik ederek uygulamalar üzerinde gerekli düzenlemelerin yapılması/yaptırılması,

- Yeni teknolojilerin sürekli takip edilmesi ve uygun olanların sisteme entegre edilmesi,
- Yazılımların; test, eğitim ve uygulama ortamına kurulması, yürütülen projelerle ilgili güvenlik ve performans testlerinin yapılması veya yaptırılması,
- Dış kurum/kuruluşlarla yapılacak bilgi alışverişi için gerekli uygulamaların yazılması/yazdırılması ve sisteme entegre edilmesi,
- Kuruluşumuz ve Havalimanları Web sitelerinin ve Portalinin yapılması/yaptırılması ve güncel olarak tutulmasına yönelik takip hizmetlerinin yürütülmesi,
- e-Devlet projelerinin takip edilmesi,
- Kuruluşumuz projeleri ile entegrasyon ve web servis imkanlarının araştırılması ve gerçekleştirilmesi,
- Çalışan veri tabanı sistemlerinde performans sorununun yaşanmaması için sürekli olarak izlenmesi ve gerekli müdahalelerin yapılması işlerini yürütmektedir.

Sistem Yönetimi Şube Müdürlüğü

- DHMİ Merkez ve Taşra Birimleri ile bu birimlerde çalışan yaklaşık 10.000 kullanıcının Bilgi Teknolojileri Dairesi Sistem Merkezine bağlantısının sağlanması, bu bağlantılarda şifreleme ve güvenlik tedbirlerinin sürekli ayakta tutulması, Kurumsal hizmetlerinin verilebilmesi için gerekli sunucu/Ağ alt yapısı ve işletim sistemlerinin yönetilmesi, gelişen teknolojilerinin takip edilmesi ve uygun olanlarının Kuruluşumuza kazandırılması konularında iş ve işlemleri yapar.

Sunucu Yönetimi

- BT hizmetlerinin verilebilmesi için gerekli sunucu alt yapısının ve işletim sistemlerinin yönetilmesi,
- Sistemlerin devamlılığının sağlanması ve erişimlerin düzenlenmesi,
- Tüm çalışanların Kurumsal kullanıcı ve e-posta hesaplarının oluşturulması, düzenlenmesi ve bakımının yapılması.

Kurumsal Veri Depolama ve Yedekleme Sistemleri Yönetimi

- Sunucu ve veri alt yapımıza uygun merkezi veri depolama ve yedekleme ünitelerine ait hizmetlerin planlanması ve yürütülmesi
- Bilgi Teknolojileri Dairesi Başkanlığı sorumluluğundaki verilerin tutulduğu depolama sistemlerinin(EXADATA, 3PAR, SUN storage) kesintisiz kullanımının sağlanması ,
- Kurumsal verilerimiz için kapasite planlamasının yapılması,

Bilgi Sistemleri Destek Şube Müdürlüğü

- Bilgisayar Sistemleri ve Çevre donanımları alımı için teknik şartnamelerinin hazırlanması, temini kabul ve tahsis işlemleri,
- Bilgi Teknolojileri sistem/cihaz ve yazılımların teknik kurulumlarının yapılması/yaptırılmasının sağlanması,
- Kullanıcıların karşılaştığı teknik altyapı ile ilgili sorunlara destek sağlanması, meydana gelen arızalara müdahale edilmesi, bakım/onarımlarının yapılması
- Uçuş Bilgi Sistemi donanımlarının temini,
- İlgili Havalimanı ve Başkanlığın talebi üzerine CUTE/BRS Sistemlerinin teminini koordine etmek.
- Bilgi Teknolojileri cihazlarının Envanter kayıtları, Sigorta, garanti vb. hizmetlerinin yürütülmesi, Başkanlığın Yatırım bütçesinin takibi, Bilgi Sistemleri Destek Şube Müdürlüğünce yapılmaktadır.

Bilgi ve İletişim Güvenliği Şube Müdürlüğü

Bilgi Güvenliği Yönetimi

- Kuruluşumuzun, Sistem ve Ağ Güvenliği Yönetim Sisteminin düzenlenmesi, yönetilmesi ve buna ilişkin standartların takip edilmesi. Yetkisiz erişimlerin, İç ve dış saldırıların önlenmesi.
- Bilgi Teknolojileri kaynaklarının kullanım politikalarının belirlenmesi ve güncellenmesi.
- DHMİ Genel Müdürlüğü ağında çalışan mevcut merkezi yönetimli “Uç kullanıcı güvenlik yazılımları, Ağ geçidi güvenlik yazılımları, e-posta güvenlik yazılımları ve veri yedekleme yazılımları” güncellenmesi ve aktif olarak tüm cihazlarda kullanımının sağlanması,
- Kurumsal SOME’ nin çalışmalarının planlanması ve yürütülmesi.

Ağ Yönetimi

- Kuruluşumuzdaki kablolu ve kablosuz Bilgisayar ağlarının altyapısının düzenlenmesi ve yönetilmesi,
- Kurum dışı network bağlantılarının düzenlenmesi ve yönetilmesi
- Kuruluşumuzdaki yerel ve geniş alan ağlarında bant genişliğinin yönetilmesi
- Gelişen bilgisayar ağları teknolojilerinin yakından takip edilmesi ve uygun olanlarının kuruluşumuza kazandırılması
- Kuruluşumuzda VOIP IP Telefon Santrali /Çağrı Yönetim Sisteminin kesintisiz kullanımının sağlanması

Sistem Log Yönetimi

- Yasal Mevzuat(5651 sayılı kanun) ve Standartlar doğrultusunda Kuruluşumuzun Log Yönetim Sisteminin düzenlenmesi ve yürütülmesi

Bilgi Güvenliği Risk Yönetimi Şube Müdürlüğü

- 2019/12 sayılı Cumhurbaşkanlığı Genelgesi ve Dijital Dönüşüm Ofisi tarafından yayınlanan "Bilgi ve İletişim Güvenliği Rehberi" talimatlarına uymak/uyulmasını sağlamak,
- 6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK) kapsamında kişisel verilerin korunmasına yönelik iş ve işlemleri yürütmek,
- Bilgi teknolojileri sistemleri üzerindeki kurumsal bilgi güvenliği politikalarının oluşturulması ve buna ilişkin planlama, işletim, yönetim, denetleme ve sertifikasyon çalışmalarını yapma/yaptırma,
- ISO 20000-1 (ITIL-Bilgi Teknolojisi Altyapı Kütüphanesi Uyumluluğu) standardına uyum
- ISO 22301 standardı düzeyinde iş sürekliliğinin oluşturulması, uygulanması, izlenmesi, gözden geçirilmesi, sürekliliğinin sağlanması ve iyileştirilmesi için risk yaklaşımını esas alan bir yönetim sistemi kurulmasını sağlama,
- Yazılım Süreç İyileştirme ve Yetenek Belirleme çalışmalarında ISO 15504 SPICE uyum ve sertifikasyon çalışmalarını yürütme, bağımsız bir şekilde takip ve denetim görevini yerine getirme,
- Uluslararası standartların takibi, süreçlere dahil edilmesi konularında çalışmalar yaparak süreç yönetim sistemlerinin güncelliğini sağlama,
- Kurumsal amaç ve hedeflerin gerçekleşmesini ve hedeflere ilişkin faaliyetlerin sürdürülmesini engelleyebilecek bilgi teknolojileri risklerinin; belirlenmesi, analiz edilmesi ve yönetilmesi amacıyla, risk yönetiminin etkin bir yönetim aracı olarak uygulanmasını sağlama,
- Uluslararası standardizasyon konularında teknolojinin getirdiği yenilikler doğrultusunda Ulusal ve/veya uluslararası projelerin araştırılarak geliştirilmesi ve üst makamlara sunulması, uygulamaya alınmasına karar verilen projelerin hayata geçirilmesine yönelik süreçlerin yürütülmesi ve takibi,
- 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.

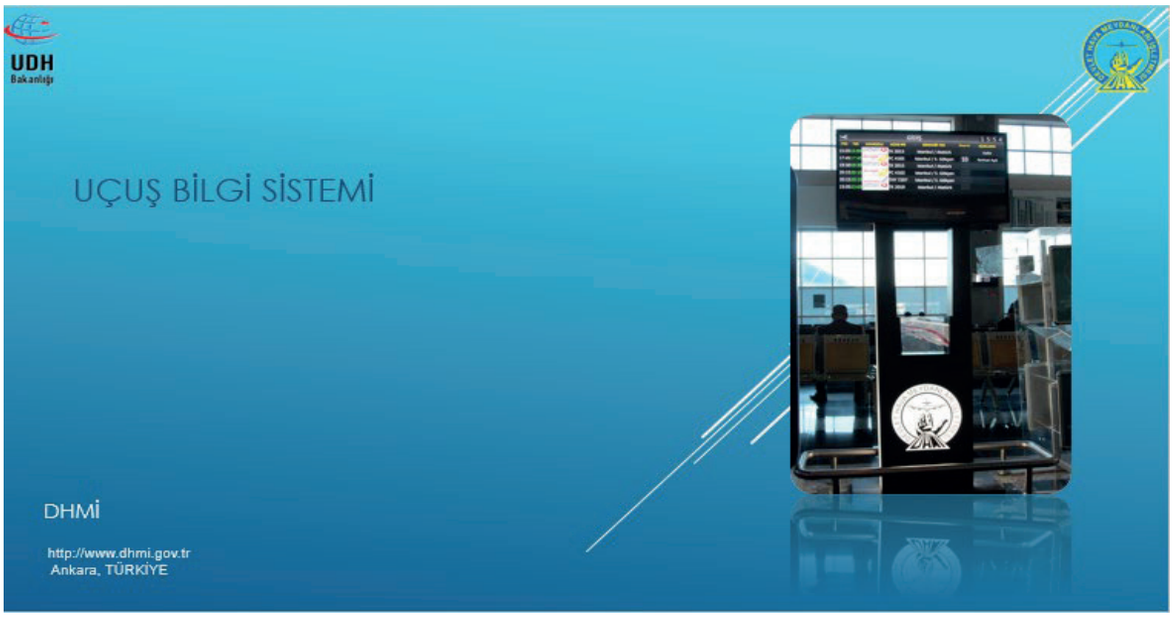
Bilgi Teknolojileri Dairesi Başkanlığının Destek Verdiği ve Geliştirdiği Projeler

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.

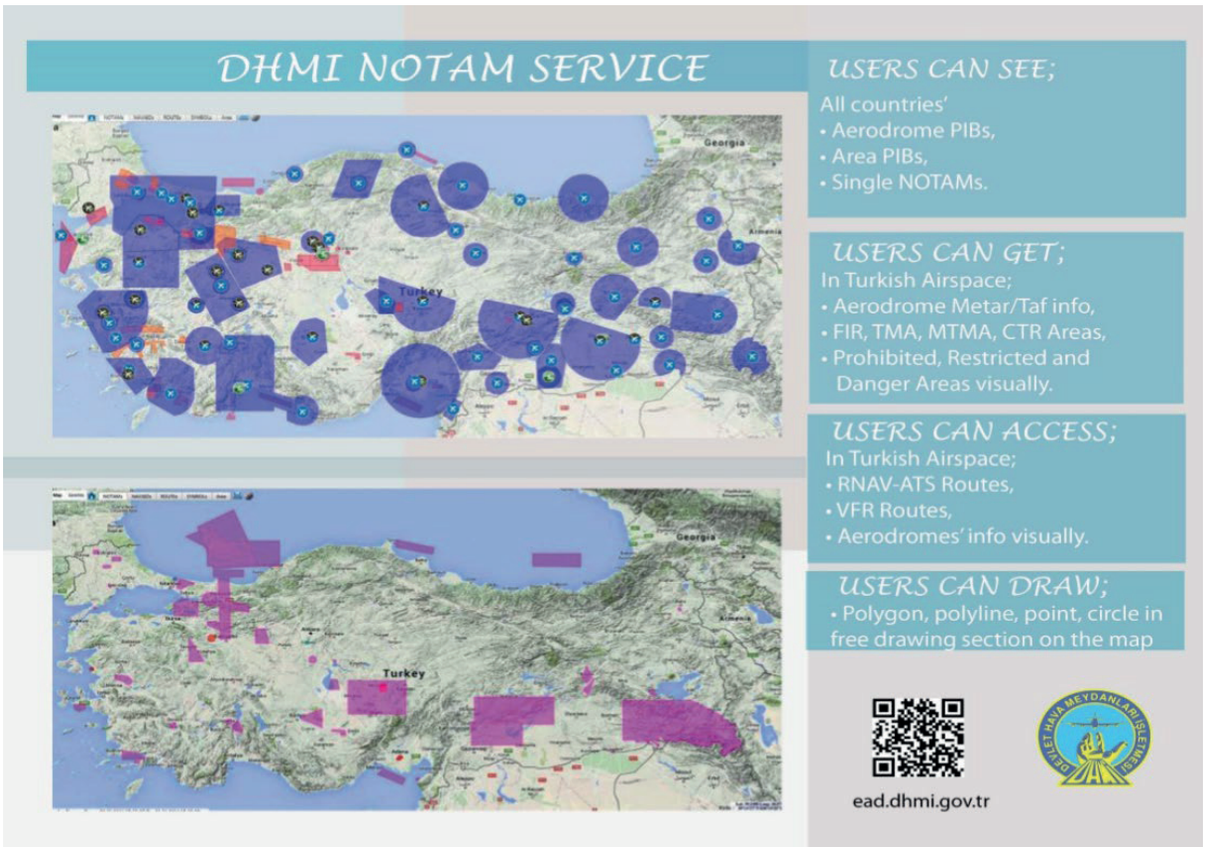
- **Check-in Banko Monitörleri:** Tipik olarak 32 inç boyutunda ve check-in bankosun yer alan firmanın check-in işlemi yapılan uçuşuna ait bilgiler yer almaktadır.
- **Giden Yolcu Salonu Monitörleri:** Tipik olarak 40 ve 46 inç boyutlarında yatay ve dikey olarak konumlandırılan İç veya Dış Hat yakın 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 2023 yılı Ocak ayı itibarı ile 41 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.

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 sağlanmıştır.

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,

Kurumsal Uygulama (Dhmionline)

Kuruluşumuzda işlemlerin büyük bir bölümü **"dhmionline"** olarak adlandırılan uygulama üzerinden online yapılmaktadır.

Birimlere özgü işler dışında standart işlemler için de (izin işlemleri, hastane işlemleri, e-imza başvuruları, evrak yazma, cihaz arıza bildirme, araç talep etme, bazı kişisel bilgilerinizi güncelleme, maaş bordroları ve eğitim bilgilerini görmek ve yetkiniz ölçüsünde güncellemek) bu sistemi kullanmanız gerekmektedir. Bu sebeple işe başlayan bütün personele sistemi kullanabilmesi için kullanıcı oluşturulmaktadır.

Web tabanlı olan uygulamaya **https://dhmionline.dhmi.gov.tr** adresi üzerinden Internet Explorer, Chrome vs. herhangi bir tarayıcı ile erişilmektedir.

Sistemde bulunan bazı modüller;

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

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.

Bilgisayar Kasası

Bilgisayarı oluşturan parçaların içine takıldığı ve parçalan bir arada tutan metal ve/veya plastik bir kutudur. Önceleri Desktop, slim ve mini tower kasa adı verilen kasalar kullanılırken son yıllarda Ekran ve Kasanın bir bütün olarak yer aldığı All-in-One(Tümleşik) kasalar yaygınlaşmaya başlamıştır. Server(sunucu) olarak kullanılmak üzere tasarlanan bilgisayarlarda genişleme olanakları fazla olan kasalar kullanılmaktadır. Kasanın en önemli bileşeni güç kaynağıdır. Güç kaynağı(Power Supply), normal şehir elektriğini bilgisayarın kullanabileceği elektrik enerjisine dönüştürür. Bilgisayar parçalarının fazla ısınmasını engellemek üzere güç kaynağının içinde bir soğutucu fan bulunur. Genellikle mikroişlemcilerin üzerinde de ayrıca bir soğutucu fan bulunmaktadır. PC'lerde (Personal Computer) güç kaynağının kapasitesi ortalama 200-250 watt'tır.

2.1 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.

2.1.1 Anakart'ın Yapısı ve Çalışması

Anakartlar özel alaşımlı bir blok üzerine yerleştirilmiş ve üzerinde RAM yuvaları genişleme kartı slotları, devreler ve yongalar bulunan ve bütün bu donanım birimlerinin mikroişlemci ile

iletişimini sağlayan elektronik devredir. Anakart, üzerindeki yonga setleri sayesinde sistem çalışmasını organize eder. Bir nevi tüm birimlerin bir arada ve uyumlu çalışmasını sağlayan bir köprü vazifesi görür.

Anakart bütün donanımları veya bağlantı noktalarını üzerinde bulundurur. Üzerinde mikroişlemci soketi, RAM slotu, genişleme yuvaları (ISA, PCI, AGP ve PCI-e), BIOS, donanım kartları (dâhilî), veri yolları ve bağlantı noktalarını bulundurur.

Anakart, bilgisayara hangi sistem bileşenlerinin eklenebileceğini ve hızlarının ne olacağını belirleyen temel unsurdur.

Anakartlarda dikkat edilmesi gereken hususların başında, kullanılmak istenen CPU (işlemci) ile uyumlu bir yonga seti kullanan bir anakart sahibi olmanız gerekliliği gelir.

2.1.2 Anakart'ın Bileşenleri

2.1.2.1 Yonga Seti (Chipset)

Anakart üzerinde yer alan bir dizi işlem denetçileridir. Bu denetçiler anakartın üzerindeki bilgi akış trafiğini denetler. Bilgisayarın kalitesi, özellikleri ve hızı üzerinde en önemli etkiye sahip birkaç bileşenden biridir. Bir yonga seti "North Bridge" (kuzey köprüsü) ve "South Bridge" (güney köprüsü) denen iki yongadan oluşur. Esasen bir anakart üzerinde birden fazla yonga mevcuttur. Ancak kuzey ve güney köprüleri yönetici yongalardır.

Tipik bir kuzey köprüsü yongası temel olarak işlemciden, bellekten, AGP veya PCI ekspres veri yollarından sorumludur ve bunların kontrolüyle bunlar arasındaki veri aktarımını sağlar. Ancak kuzey köprüsü ve güney köprüsü özellikleri üreticiye ve yonga setine göre farklılık gösterebilir ve bu genellemenin dışına çıkabilir. Kuzey köprüsü yongası fonksiyonlarından dolayı işlemciye, bellek ve AGP slotlarına yakın olmalıdır (Sinyalin geçtiği fiziksel yollar ne kadar kısa olursa sinyal o kadar temiz ve hatasız olur.) ve bu yüzden de anakartın üst kısmına yerleştirilir. Zaten adındaki "kuzey" kelimesi de buradan gelmektedir.

Güney köprüsü yongası ise giriş-çıkış birimlerinden, güç yönetiminden, PCI veriyolundan ve USB ile anakarta entegre özelliklerden (ses ve ethernet gibi) sorumludur. Adındaki "south" kelimesinin de yine anakarttaki pozisyonundan geldiği kolayca tahmin edilebilir.

Üreticilerin yonga setlerini iki parça hâlinde tasarlamaları anakart tasarımında esneklik sağlar. Örneğin USB 2.0 desteği olmayan bir yonga setine bu desteği eklemek için bütün yonga setini baştan tasarlamak yerine sadece güney köprüsü yongasında değişiklik yapmak

çok daha kolaydır. Ayrıca değişik özelliklerdeki güney köprüsü yongaları kullanılarak değişik kullanıcı gruplarına hitap etmek mümkün olur.

2.1.2.2 Veri Yolları (BUS)

Anakart üzerindeki bileşenlerin birbiriyle veri alışverişini sağlayan yollardır. Dışarıdan bağlanan donanımlarda ise veri yolları uçlarında bulunan slotlar sayesinde bilgi alışverişi sağlamaktadır.

Bant Genişliği: İletişim kanalının kapasitesini belirler. Birim zamanda aktarılabilecek veri miktarıdır. Bant genişliği ne kadar büyükse belli bir sürede aktarılabilecek veri miktarı da o kadar büyük olur.

2.1.2.3 Portlar ve Konnektörler

Anakart ile dış birimlerin iletişim kurmasına olanak sağlayan bağlantı noktalarıdır. Portların bir kısmı kasanın içindedir ve bu portlara harddisk gibi kasa içine monte edilen birimler bağlanır. Bazı portlarda kasa yüzeyinde anakarta monteli şekilde bulunur. Bu portlara kasa dışından ulaşılır ve mikrofon gibi kasa dışında bulunması gereken cihazlar bağlanır.

2.1.2.3.1 PS/2 Portu: Yeşil ve mor renklerde iki ayrı PS/2 portu vardır. Bunlardan yeşiline fare, mor olanına ise klavye takılır. Günümüzde USB klavye ve fareler daha çok kullanıldığından çoğu bilgisayarda bulunmamaktadır.

PS/2 Portları

2.1.2.3.2 USB (Universal Serial BUS) Portu: Günümüzde bilgisayarların hemen hepsinde birden fazla USB girişi bulunmaktadır. Bu USB konnektörler fareden yazıcıya birçok çevresel cihazın

bilgisayara hızlı ve kolayca bağlanmasını sağlar. İşletim sisteminin desteklemesine göre, cihaz sürücülerinin yüklenmesi de oldukça kolay ve hızlı bir şekilde yapılabilmektedir.

USB Hızları:

- USB 1.0 ve 1.1: Hız 12 Mbit/sn (1,5 MByte/sn)
- USB 2.0: Hız 480 Mbit/sn (60 MByte/sn)
- USB 3.0: Hız 4,80 Gbit/sn (600 MByte/sn)
- USB 3.1: Hız 10 Gbit/sn (1,22 GByte/sn)

USB Türleri:

Type A: Günümüzde en çok kullanılan Klavye, fare gibi birçok kablonun ucu, Type-A konektörüne sahiptir.

Type B: Kare şekline yakın bu konektör, yazıcı ve diğer güç gerektiren, bilgisayara bağlı bileşenler tarafından kullanılır.

Type C: İki yönde de takılabilen bu kablo, önceki USB türlerine göre daha çok güç ve veri taşıyabiliyor. Laptop'larda, bazı telefon ve tabletlerde kendine giderek daha çok yer buluyor.

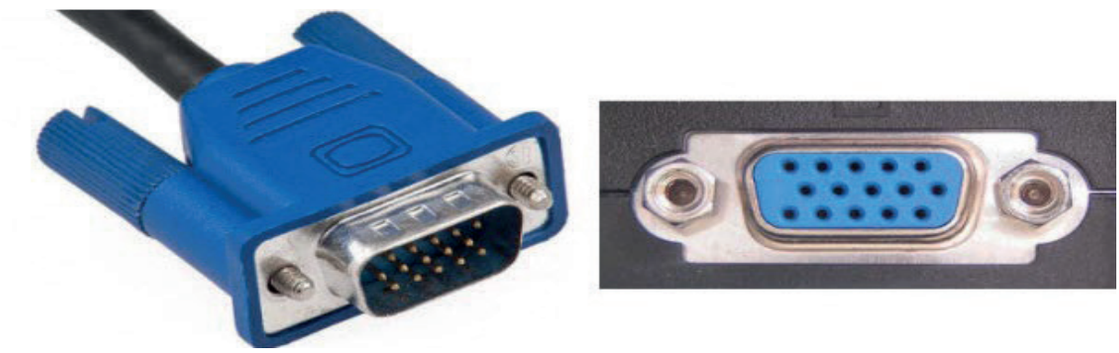
USB Türleri

2.1.2.3.3 Görüntü Portları:

2.1.2.3.3.1 VGA (Video Graphics Array - Video Grafikleri Dizilimi)

VGA, ilk olarak 1987'de ortaya çıktı. Biraz eski kalmış olsa da bugün hala birçok PC'de görebileceğiniz VGA girişi, analog sinyallerle çalışır. VGA, kullandığı yüksek frekanslar sayesinde nispeten yüksek çözünürlüklere ulaşabilmektedir. Ancak videonun kalitesi, kablonun kalitesine bağlı kalacaktır. Bir VGA konnektörü, 3 sıraya ayrılmış 15 pin içerir ve

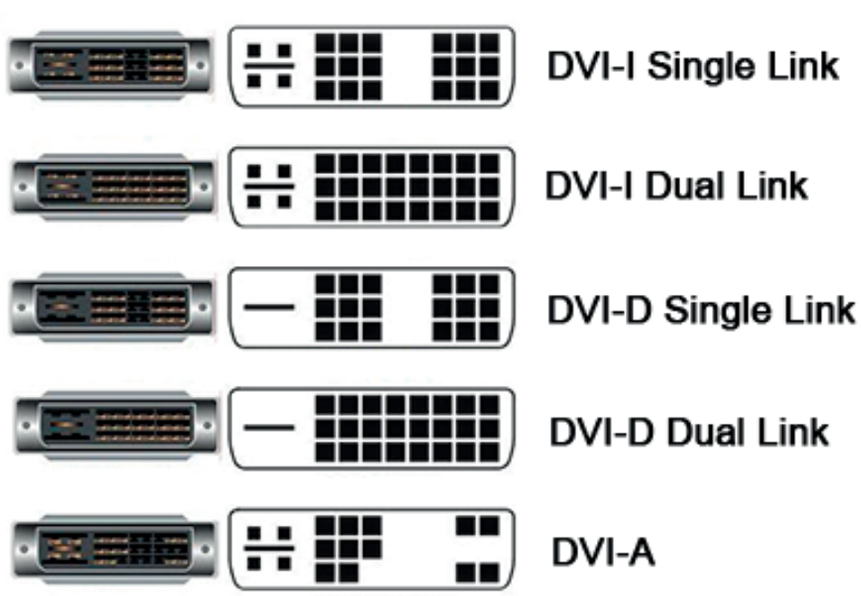
bir yamuk şekline sahiptir. VGA konnektörlerinde genellikle mavi renk kullanılmaktadır.



VGA Kablo ve VGA Portu

2.1.2.3.3.2 DVI (Digital Video Interface – Dijital Görüntü Arabirimi)

VGA'nın haleflerinden biri olarak görülen DVI, Bilgisayar, LCD ekranı, Projeksiyon veya dijital televizyon gibi harici bir çıkış aygıtını bağlamak üzere tasarlanmış eski bir bağlantı türüdür. DVI standardı hem masaüstü bilgisayarlarda hem de monitörlerde olmak üzere bilgisayar endüstrisinde yaygın olarak kabul görmüştür. Günümüzde perakende olarak satılan çoğu bilgisayar ve LCD monitörde bir DVI arabirimi bulunmaktadır; projektörler ve tüketici televizyonları gibi birçok aygıttaysa DVI bir başka video arabirimi standardı olan HDMI aracılığıyla dolaylı olarak desteklenmektedir. Çoğu Dizüstü bilgisayarda eski VGA bağlantı noktası, bazı modellerde de HDMI bağlantı noktası vardır. Az sayıda Dizüstü bilgisayarda DVI bağlantı noktası görülmektedir.



DVI Kablo Türleri

2.1.2.3.3.3 HDMI (High Definition Multimedia Interface – Yüksek Çözünürlüklü Çoklu Ortam Arayüzü)

2003 yılında ses (audio) ve görüntü (video) verilerini sıkıştırılmadan dijital olarak aktarmak için geliştirilmiş bir arabirimdir. HDMI; blu-ray disk çalar, HD-DVD disk çalar, bilgisayar, oyun konsolu, dijital uydu alıcısı gibi cihazları uyumlu ses ve görüntü cihazlarına (ör. "HD Ready" LCD televizyon) bağlar.

HDMI için Her biri farklı alanlara hitap eden 5 farklı konnektör tanımlanmıştır.

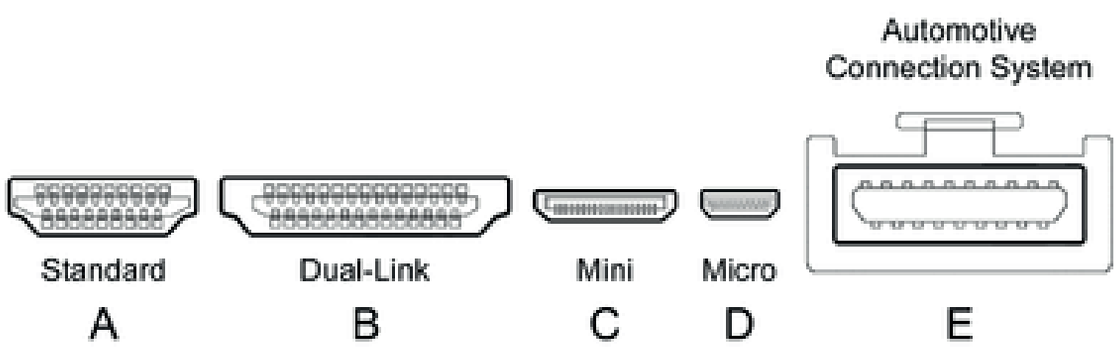
Tip-A konnektör 19 pin'lidir. 13.9mm genişliğinde ve 4.45mm yüksekliğindedir. Elektriksel olarak tek-hatlı DVI-D ile uyumludur.

Tip-B daha yüksek çözünürlükleri (ör. WQSXGA (3200x2048)) destekler ve 29 pin'lidir. Çift-hatlı DVI-D ile elektriksel olarak uyumludur. 21.2mm genişliğe sahiptir.

Tip-C taşınabilir cihazlar için tasarlanmıştır. Tip-A gibi 19 pin'lidir ama boyutları daha küçüktür.

Oldukça küçük yapıda olmalarıyla Tip D konnektör akıllı telefonlara uyumludur.

Tip E ise otomotiv donanımlarında kullanılan bir HDMI çeşididir.



HDMI Tipleri

2.1.2.3.3.4 DISPLAYPORT

DisplayPort, VESA (Video Electronics Standards Assosiation - Video Elektronik Standartları Kurumu) tarafından oluşturulan herkesin kullanımına açık, görüntü ve sesi aynı kablo üzerinden gönderilmesine imkân tanıyan dijital bir arabirim. DisplayPort, aynı zamanda panel giriş / çıkışları ve mikrofon gibi bağlantıları destekleyen ayrı bir hatta da sahip. DisplayPort'un en fazla öne çıkan özelliklerinden birisi ise, tek kablo üzerinden çoklu monitöre aktarım imkânı

tanıyor olmasıdır. HDMI, tüketici elektroniği için geliştirilen bir bağlantı arabirimi iken, DisplayPort sadece bilgisayar sistemleri düşünülerek geliştirilen bir bağlantı arabirimidir.

DISPLAYPORT Özellikleri:

10.2 Gbit/s ileri bağlantı, tek kablo ile 2560×1600 çözünürlük desteği

8B/10B veri iletişimi

Açık ve genişleyebilen standart.

6, 8, 10, 12 ve 16 bit renk derinliği desteği.

3 metre kabloda tam bant veri iletimi

15 metre kabloda düşük bant veri iletimi ile 1080p transferi

Displayport

2.2 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.

Bilgisayarın, bir toplama işlemini yapabilmesi için bir dizi devreyi açıp kapatması gerekir. Bu işlemleri çok kısa sürede ve eş zamanlı olarak yapar. Bu eş zaman işlemi gerçekleştiren CPU ya bağlı bir saattir (Kuarts Kristal). Saatin her vuruşunda bilgisayar birçok elektriksel işlemi gerçekleştirir. Bu saatin ürettiği darbeler Mega Hertz (Mhz) olarak adlandırılan birimle ölçülür. 33 Mhz hıza sahip bir bilgisayarın sistem saati 1 saniyede 33.000.000 kez çalışıyor demektir. Mhz değeri büyüdükçe, bilgisayarın çalışması da hızlanacaktır.

Bir kişisel bilgisayarın hızı, mikro işlemcisinin hızına ve birim zamanda işlediği sözcük boyuna bağlıdır. Mikro işlemcisinin hızı ise, bir saniyede yapılan işlem sayısı ile ölçülür. Sözcük boyu ise, bilgisayarın birim zamanda işleyebildiği bit sayısıdır. Bu değer 8, 16 ve 32 olabilmektedir. Mikro işlemciler belirli numaralarla ifade edilirler.

2.2.1 İşlemcinin Yapısında Bulunan Birimler

- Çekirdek (Core)
- Kontrol Birimi
- Ön Bellek (Cache)

2.2.1.1 Çekirdek (Core)

Komut çalıştırma işlemlerini yapan bölümdür. Çalıştırma birimi (execution unit) olarak da bilinir. Bu ünite komutları çalıştırır ve pipeline (iş hattı) denen yollarla beslenip tamsayıları kullanarak okuma, değiştirme ve komut çalıştırma işlemlerini yapar. Çekirdek içerisinde ALU, Genel amaçlı register, Durum registeri (Status Register-SR) ve Program sayacı (Program counter –PC) bulunmaktadır.

2.2.1.2 Kontrol Birimi

İşlemciye gönderilen komutların çözülüp (komutun ne anlama geldiğinin tanımlanması) işletilmesini sağlar. İşlemci içindeki birimlerin ve dışındaki birimlerin eş zamanlı olarak çalışmasını sağlayan kontrol sinyalleri bu birim tarafından üretilir. Kontrol Ünitesinde Komut kaydedici (Instruction Register-IR) ve Komut çözücü (Instruction Decoder –ID) bulunur.

2.2.1.3 Ön Bellek (Cache Memory)

Sistem belleğinden gelen veriler, çoğunlukla CPU'nun hızına yetişemez. Bu problemi çözmek için CPU içinde yüksek hızlı hafızalar bulunur, buna ön bellek denir. Ön bellek çalışmakta olan programa ait komutların, verilerin geçici olarak saklandığı yüksek hızlı hafızalardır.

L1 Ön Bellek (Cache) : Önemli kodlar ve veriler bellekten buraya kopyalanır ve işlemci bunlara daha hızlı ulaşabilir. Kodlar için olan Code cache ve veriler için olan Data cache olmak üzere ikiye ayrılır. Kapasitesi 2 KB ile 256 KB arasında değişir.
L2 Ön Bellek (Cache) : L1 belleklerine göre kapasiteleri 256 KB ile 2 MB arasında değişir. Başlangıçta L2 önbellek anakart üzerinde işlemciye yakın bir yerde yer almaktaydı. Daha sonra slot işlemciler ortaya çıkınca işlemci çekirdeğinin üzerinde kartuş şeklindeki paketlerde yer aldı. Bununla beraber çekirdeğin dışında ve işlemciyle aynı yapıda kullanılmaya başlandı. Bu kısa geçiş döneminden sonraysa L2 önbellek işlemci çekirdeklerine entegre edildi.
L3 Ön Bellek (Cache): L3 ön belleklerinin kapasiteleri 2MB ile 256 MB arasında değişir. Yeni bir teknolojidir. Çok çekirdekli işlemcilerde bütün çekirdeklere tek bir bellekle hizmet vermek akıllıca bir yaklaşım olacağı düşüncesiyle geliştirilmiştir.

2.2.2 İşlemcilerde Kullanılan Ölçü Birimleri

Birim	Kısaltma	Anlamı
Hertz	Hz	1Hz =Saniyede 1 işlem yapabilme yeteneği
KiloHertz	KHz	1KHz=1024Hz
MegaHertz	Mhz	1MHz=1024KHz
GigaHertz	GHz	1GHz=1024MHz

2.2.3 İletişim Yolları

İşlemciler, bilgisayarı yönetmek ve kontrol etmek için iletişim yollarını kullanır. Hem işlemci içerisinde hem de işlemciyle diğer birimler arasında iletişim hatları bulunmaktadır. İletişim hatları, üzerinden elektrik sinyali geçebilecek iletken hatlardır. Bu hatların sayısı işlemci modeline göre değişir.

2.2.3.1 BUS Interface (Yol arayüzü): İşlemciye veri–kod karışımı olan bilgileri getirir. Bunları ayırarak işlemcinin ünitelerini kullanmasını sağlar ve sonuçları tekrar birleştirerek dışarı yollar. Bu ara yüzün genişliği işlemcinin adresleyebileceği hafızayı belirler. Örneğin 32 bitlik hafıza genişliğine sahip bir işlemci 4 GB hafızayı adresleyebilir ve bu hafızadan aynı anda 32 bit üzerinde işlem yapabilir. Günümüzde masaüstü pazarına 32 bitlik işlemciler hâkimken sunucu uygulamaları ve bilimsel çalışmalar için de 64 bitlik işlemciler yaygın olarak kullanılır.

İletişim hatları üç grup hâlinde incelenebilir:

2.2.3.2 Adres yolu (Address Buses)

İşlemcinin bilgi yazacağı veya okuyacağı her hafıza hücresinin ve çevre birimlerinin bir adresi vardır. İşlemci, bu adresleri bu birimlere ulaşmak için kullanır. Adresler, ikilik sayı gruplarından oluşur. Bir işlemcinin ulaşabileceği maksimum adres sayısı, adres yolundaki hat sayısı ile ilişkilidir. Adres yolunu çoğunlukla işlemci kullanır. Bu yüzden adres yolunun tek yönlü olduğu söylenebilir ama yeni teknolojilerde çift yönlüdür.

Adres yolundaki hat sayısı işlemcinin kullanabileceği maksimum RAM'ı belirler

$2^{\text{Adres hattı sayısı}}$ = Maksimum hafıza kapasitesi

Bir mikroişlemci 16 adres hattına sahipse adresleyebileceği maksimum hafıza kapasitesi,

2^{16} = 65536 bayt = 64 KB olacaktır.

Yeni işlemciler 36 bit adres yoluna sahiptir. Buda 2^{36} dan 64 GB bellek adresleye bilmesini sağlar

2.2.3.3 Veri yolu (Data Buses)

İşlemci, hafıza elemanları ve çevresel birimlerle çift yönlü veri akışını sağlar. Birbirine paralel iletken hat sayısı veri yolunun kaç bitlik olduğunu gösterir. Örneğin, iletken hat sayısı 64 olan veri yolu 64 bitliktir. Yüksek bit sayısına sahip veri yolları olması sistemin daha hızlı çalışması anlamına gelir.

2.2.3.4 Kontrol yolu (Control Buses)

İşlemcinin diğer birimleri yönetmek ve senkronizasyon(eş zamanlama) sağlamak amacı ile kullandığı sinyallerin gönderildiği yoldur. Burada bellek okuma-yazma sinyalleri, kesme sinyalleri ve clock(saat) sinyalleri iletilir.

2.3 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. Buradaki "rastgele erişim" ifadesi bilgisayarın bellek içerisindeki herhangi bir adrese doğrudan gidip bilgileri okuyabileceği veya yazabileceği anlamında kullanılmaktadır. Ana bellekte veriler geçici olarak tutulur; başka bir deyişle bilgisayar kapatıldığında bu veriler silinir. Çok kullanıcılı sistemlerde bilgisayar bir kullanıcı için herhangi bir işi yapmayı bitirdiğinde, ana bellekteki aynı kısma diğer kullanıcılar için işlenmesi

gereken veri ve programlar yerleşir. Ana bellek diğer bilgi saklama araçlarına oranla biraz daha pahalıdır.

Ana belleğin temel görevleri şöyle özetlenebilir.

1. Hali hazırda çalışan programların program deyimleri ve bu programların ihtiyaç duyduğu verileri tutmak.
2. İşletim sistemi yüklendikten sonra ana bellekte sürekli olarak kalması gereken işletim sistemi bileşenlerini tutmak.
3. Programlar tarafından üretilen sonuçlan tutmak.
4. Sabit disklere veya harici bir cihaza gönderilmeye hazır olan çıkış bilgilerini tutmak.

2.3.1 Ana Bellek(RAM) Türleri

DRAM: Bu bellek, bilgi alışverişi sağlayabilmek için elektrik sinyallerini, verileri barındırmak için de kapasitörleri kullanır. Bu nedenle de sürekli yenilenme ihtiyacı duyar, bir saniye içerisinde binlerce kez yenilense de SRAM'e göre daha yavaş kalır.

SRAM: Bu bellek, DRAM'de olduğu gibi bilgileri tutabilmek için kapasitörler yerine açma-kapama anahtarları (transistör) kullanır ve yenilenmeye ihtiyaç duymaz. Bu yüzden DRAM'e oranla daha hızlı ve pahalıdır. Ayrıca daha fazla bilgi tutabilir.

SDRAM: Bu bellek, işlemci ile eş zamanlı olarak çalışan bir RAM bellek türüdür. Girişdeki değişiklik algılanıp hızlı bir şekilde yanıtlandığı ve işlemciyi daha az beklettiği için daha sık tercih edilir.

DDRRAM: Bu bellek içerisinde kullanılan saat sinyali SDRAM belleklerden yaklaşık iki kat daha hızlıdır. 100 Mhz DDR RAM'in veri aktarım hızı 1.600 MB/sn'dir. Bu bellekler grafik ağırlıklı işlemlerde çok başarılılardır. 64 bitlik veri yolu kullanırlar ve daha az enerji harcarlar. DDR2, DDR3, DDR4, DDR5 şeklinde geliştirilmektedir.

DRDRAM: Rambus isimli bir firma tarafından üretilen bu bellekler, 16 bitlik bir veri yolu kullanılarak yüksek hızlar üretilmiştir. Günümüzde kullanılan en son teknolojidir. 1.6 GB/sn hızındadır.

PSRAM: DRAM'in yüksek yoğunluğu ve SRAM'in kullanım kolaylığı gibi faydalarını ortak sunan bellek, SRAM'e çok benzer yenileme ve adres kontrol devresine sahiptir. Apple ürünleri gibi birçok gömülü sistemlerde kullanılır.

RLDRAM: Ağ oluşturma ve önbelleğe alma uygulamalarında kullanılan bellek türünden yüksek okuma-yazma oranı içeren uygulamalar için faydalanılır.

SGRAM: Grafik bağdaştırıcılarında kullanılır ve bir seferde iki bellek sayfası açabilir. Ayrıca bit maskeleme ve blok yazma özelliği de sunan bu bellek türü, özellikle ekran kartlarında kullanılan yüksek performans hızlandırma amaçları için tasarlanmıştır.

2.4 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. Not: BIOS bugün üretilen ana kartların çoğunda, Flash ROM üzerine kayıtlıdır. Bu türdeki belleğin içeriği bilgisayarı kapadığınızda silinmez ama gerektiğinde özel bir program çalıştırılarak değiştirilebilir. Böylelikle BIOS un içerdiği hatalar giderilebilir.

BIOS' un ilk görevi, bilgisayarın açılışı sırasında bellek gibi çeşitli parçalan kontrol ederek, bir problem varsa kullanıcıyı uyarmaktır. Bilgisayarın açılışı sırasında özel bir tuşa (genellikle DEL tuşu) basarsanız, karşınıza BIOS setup ekranı gelir. Bu ekranda gerekiyorsa, sabit disk sürücülerinin tipi gibi çeşitli bilgileri ve ayarlan değiştirebilirsiniz.

2.5 Grafik Kartı (Ekran Kartı)

Bilgisayarda genel olarak oyun oynamak, çizim veya resim yapmak, mimari çizimlerin yapılması amacıyla kullanılan karttır. Piyasada bulunan bazı grafik kartlarının isimleri şunlardır:

MDA (Monochrome Display Adaptör) (Tek renk-720x320 Pixel)

CGA (Color Graphic Adaptör) (4 Renk - 400x200 Pixel) EGA

(Enhanced Graphic Array) (16 Renk - 600x400 Pixel) VGA

(Video Graphic Adaptör) (256 Renk - 800x600 Pixel) SVGA

(Süper Video Graphic Adaptör) (256 Renk - 1024x768 Pixel)

Ekran, grafik özelliğinde çalışırken satır ve sütun sayısı yerine, her biri ayrı ayrı duyarlı noktalardan oluşur. Bu noktaların her birine Pixel adı verilir. Nokta (Pixel) sayısı ne kadar fazla olursa ekrandaki görüntü daha net olur.

Grafik Kartında Etkin Rol Alan Temel Bileşenler Şunlardır:

VGA BIOS: Ekran kartının çalışmasını sağlayan komutlar içermektedir. Yani ekran kartının ne zaman ne iş yapacağını bu bileşen belirlemektedir.

Grafik İşlemci (GPU): Ekran kartının beyni gibidir. Görüntü hesaplamalarını ve görüntü işlemlerini mikroişlemciye (CPU) yansıtmadan ekran kartında gerçekleştiren bir yongadır.

Video RAM: Grafik işlemci görüntüyü oluştururken hafıza olarak ekran kartı üzerindeki hafızayı kullanmaktadır. Bu da ana belleğin sadece CPU tarafından kullanılarak performansın artmasına sebep olmaktadır.

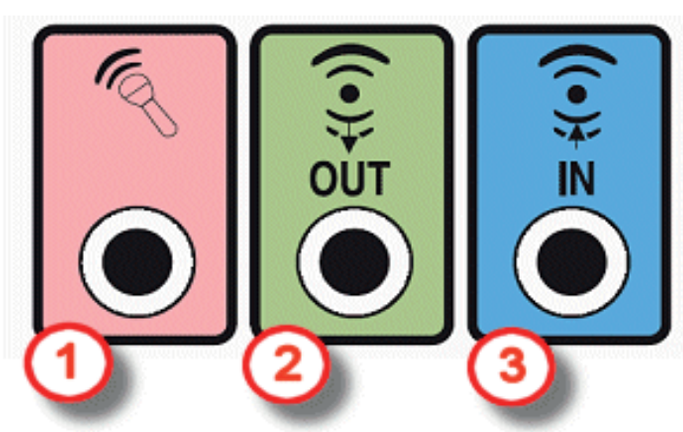
RAMDAC (dijital-analog çevirici): Ekran kartının görüntü belleğindeki dijital (sayısal) verileri monitörde görüntülenecek analog sinyallere dönüştürerek ekran kartının monitör çıkışına gönderir. RAMDAC'in verileri dönüştürme ve aktarma hızı, ekran tazelenme hızını belirler. Bu hız Hz cinsinden ölçülür. Örneğin monitörün ekran tazeleme hızı 70 Hz olarak ayarlanmışsa görüntü saniyede 70 defa yenilenir.

Ekran Kartı Çeşitleri

Fiziksel yapısına göre ekran kartları onboard (tümleşik) ve haricî (genişleme yuvalarına takılan) ekran kartları olmak üzere ikiye ayrılır. Günümüzde çeşitli üreticiler tarafından her türlü kullanıma uygun olarak ekran kartları üretilmektedir. Veriyolu standardına göre ekran kartları; ISA, PCI, AGP, PCI-X ve PCI-e şeklinde gruplandırılabilir.

2.6 Ses Kartı

Bilgisayardan seslerin daha kaliteli olarak elde edilmesini sağlayan elektronik devredir.



1 numaralı giriş: Mikrofon giriş portu – Dış ortamdaki sesleri bilgisayara aktarır.

2 numaralı giriş: Ses çıkış portu – Hoparlörün ya da kulaklığın kullanılmasını sağlar.

3 numaralı giriş: Ses giriş portu – Medya cihazlarındaki sesleri bilgisayara aktarır.

2.7 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). Bilgisayarınızda birden fazla sabit disk sürücü bulunabilir veya bir sabit disk iki ya da daha fazla bölüme ayrılabilir. Günümüzde RAM belleklerle aynı mantıkta çalışan mekanik harddisklere oranla daha hızlı olan SSD(Solid State Disk) disklerin kullanımı hızla artmaktadır. İlk sabit disk, C sürücüsü diye adlandırılır. Daha sonra takılan hard diskler sırasıyla D,E,F... harflerini alır. Bir sabit diskin saklayabileceği bilgilerin miktarı, MB(Mega Bbyte), GB(Giga Byte) veya TB(Terabayt) ile ifade edilir. Bilgisayardaki Disk, CD, DVD, Manyetik bant, Flash Hafıza kartları gibi depolama ünitelerinde kapasite belirtmek amacı ile kullanılan bazı ölçü birimleri aşağıda verilmiştir.

Kapasite	Sembol	Değer
Bit	**b**	**0 veya 1**
Byte	**B**	**8 bit**
Kilobyte	**KB**	**1024 Byte**
Megabyte	**MB**	**1024 KB**
Gigabyte	**GB**	**1024 MB**
Terabyte	**TB**	**1024 GB**
Petabyte	**PB**	**1024 TB**
Exabyte	**EB**	**1024 PB**
Yottabyte	**YB**	**1024 EB**

2.7.1 Sabit Disk(Harddisk)'in Çalışması

Sabit diskler özel bir motor tarafından kontrol edilen kolların üzerinde yer alan okuma/yazma başlıkları ve manyetik malzeme ile kaplı alüminyumdan yapılmış plaklardan oluşur. Kolların ucundaki iki küçük okuma/yazma kafası, bu plakalar üzerinde okuma ve yazma işlemleri gerçekleştirir.

Plakalar dakikada 3.500 ile 15.000 devirle dönerler ve devir hızı RPM olarak ifade edilir. Plakalar ile kafalar arasındaki boşluk uçuş yüksekliği olarak ifade edilir ve bu yükseklik, bir

parmak izinin kalınlığından bile daha azdır. Okuma/yazma başlıkları diske ne kadar yaklaşırsa bilgi sürücüye o kadar yoğun depolanır.

2.7.2 Sabit Disk(Harddisk)'te Bad Sector

Harddiskler sektör adı verilen ve üstüne bilgilerin yazıldığı birçok birimden oluşur. Bu birimler zamanla bazı nedenlerle kullanılamaz hale gelir, bu da ya sadece veri kaybına ya da diskin tamamen iş göremez duruma gelmesine neden olur. Harddisklerde oluşan ve diskin zarar gören biriminin kalıcı olarak kullanılamaz hale gelmesine neden olan bozuk disk bölümüne "bad sector" denir. Bad Sector'ler donanımsal hatalardır ve bilinenin aksine herhangi bir yazılım tarafından düzeltilemezler (ama devre dışı bırakılabilirler). Hard diskte bad sector oluşmasına neden olan faktörleri şöyle sıralayabiliriz;

Hard disk çalışma sıcaklığının aşırı yüksek olması (+55 C) veya nemli ortam

Hard disklerde yaşlanmaya bağlı yıpranma ve korozyonlar

Diski çalışır durumdayken yere düşürmek, bir yere çarpmak

2.7.3 SSD (Solid State Drive – Katı Hal Sürücü)

Veri depolamak için geliştirilmiş sabit disklerin yerini alan veri depolama aygıtıdır. Mekanik bir sabit diskin maksimum yazma hızı ortalama 150mb/sn iken SSD'lerde bu hız 560mb/sn'dir. En büyük avantajları; Isı, ses, düşük enerji sarfiyatı ve mekanikliğin ortadan kalkması. SSD'lerin çalışma mantığı RAM'ler ile aynıdır. Veri yolları her mikroçipe paralel bağlanarak istenilen bilgiye eş zamanlı olarak erişilebilir. Bu nedenle SSD'ler çok yüksek hızlara erişebilir.

HDD SSD

Özellikler	SSD	HDD
Hazırlık Süresi	Yok	Birkaç saniye
Rasgele Erişim	0.1 ms	5-10 ms
Okuma Gecikmesi	Genelde düşük	Genelde yüksek
Okuma Performansı	Değişmez	Parçalı dosyalarda performans düşmektedir.
Disk Birleştirme	Gerekmez	Gerekli
Ses	Yok	Var
Güç Gereksinimi(Aynı Tip)	Az	Çok(>15 Watt)
Mekanik Süreklilik	Söz konusu değil	Gerekli
Sıcaklık, Darbe Dayanımı	Çok	Az
Manyetik Hassasiyet	Yok	Çok
Ağırlık Hacim	Az	Çok
Paralel Çalışma	Bazılar aynı anda farklı çipleri okuma/yazma yapabilir.	Aynı silindir üzerinde mümkün
Yazma Ömrü	Flash tanlılar sınırlı , fakat DRAM tabanlılar sınırsızdır.	Sınırsız
Kapasite	Şu an HDD den daha az	SDD den daha çok
Okuma/Yazma süreleri	Bazılarında farklı	Aynı

2.8 DVD (Digital Versatile Disc ya da Digital Video Disc)

DVD ilk önceleri "Dijital Video Disk" anlamına geliyordu. Bunun temel nedeni, ilk uygulamaların video alanında ortaya çıkmış olmasıdır. Fakat bir süre sonra, veri saklama uygulamalarının da önemli olduğu anlaşılmış ve DVD "Dijital Versatile Disk (Çok-yönlü Sayısal Disk)" anlamında kullanılmaya başlanmıştır.

Görüntü, ses ve bilgiyi aynı ortamda saklamaya yarar. DVD-ROM'lar CD-ROM'ların daha gelişmiş bir tipi olarak düşünülen CD'lerdir. DVD Videolar ise televizyona takılan DVD Player'larda izlenen, ses ve görüntü içeren disklerdir. DVD-ROM sürücüler 4,7 GB kapasitede üretiliyorlar. Günümüzde DVD-ROM'ların yerini her bir katmanda 25 - 35 GB veri tutabilen 200 GB'a kadar kapasite üretebilen BLU-RAY Disc'ler almaya başlamıştır.

CD / DVD / BLU-RAY DISC

2.9 Monitör (Ekran)

Monitör (veya ekran) bilgisayarın mikroişlemcisinden gönderilen sinyalleri gözün görebileceği şekilde görüntüye dönüştüren cihazdır. Yani CPU tarafından istenilen bilgilerin kullanıcıya iletildiği ortamdır; bir çıkış birimidir. Monitörlerin en önemli özelliklerinden birisi ekrandaki görüntülerin netliği veya çözünürlüğüdür. Çözünürlük (resulation), yatay ve dikey olarak ekrandaki nokta sayısıyla ölçülür. Çözünürlük yükseldikçe ekrana daha fazla bilgi sığar, ama ekrandaki görüntüler küçülür. Multisync monitörler, değişik çözünürlüklerde çalışabilirler (640x480, 800x600, 1024x768, 1280x1024 gibi). Böylece ekrandaki görüntüleri amaca göre genişletip daraltılabilir.

Büyüklük: Monitör büyüklüğü, ekranın köşegen uzunluğuyla ölçülür.

Nokta aralığı: Görüntü netliği, ekran yüzeyindeki noktaların arasındaki uzaklığa bağlıdır. Nokta aralığı ne kadar küçükse görüntü o kadar net olur. Eski monitörlerde bu 0.39 mm iken şimdiki monitörlerde genellikle 0.28 veya daha küçüktür.

Ekran tazeleme: Ekrandaki görüntü saniyede en az 60 kez tazelenmelidir. Ekran tazeleme frekansı yükseldikçe daha sabit bir görüntü elde edilir. "Non-interlaced" (titreşimsiz) denilen monitörler ekranı tek seferde tarayabildiği için gözü daha az yorar.

Monitör ve görüntü kartı, ekranda görüntülerin sergilenebilmesi için birlikte çalışırlar.

Monitörde görüntülenebilen renklerin sayısı görüntü kartındaki bellek miktarıyla sınırlanır.

Görüntü kartındaki bellek yongaları, bilgileri monitöre göndermeden önce geçici olarak saklar.

Renk sayısı, ekrandaki görüntülerin kalitesini doğrudan doğruya etkiler. Daha fazla renk, gerçeğe daha yakın ve daha iyi görüntü demektir.

2.10 Monitörlerde Kullanılan Ölçü Birimleri

Ölçü Birimi	Anlamı
Genişlik(inch)	Monitörlerde genişlikleri inç ile ölçülür. 1 inç yaklaşık 2,54 santimetredir. 15" lik bir monitör (15 x 2.54 = 38,1 cm) yaklaşık
Yineleme(Tazeleme) Hızı(Hz)	Monitörün bir saniyede ekranı yatay ve dikey olarak kaç kez tazelediğini belirtir. Örneğin 60 Hz tazeleme hızına sahip bir monitör ekranı saniyede 60 kez tazelemektedir.
Çözünürlük	Çözünürlük Ekrandaki dikey ve yatay nokta sayısını belirtir. Bu rakamlar sabittir. İlk olarak 640x480 (480p) ile başlayıp 1280x720 (720p) ve 1920x1080 (1080p- Full HD) yükselmiş 3840x2160 (4K – Ultra HD) ile zirveye

2.11 Klavye (Keyboard)

Klavye, üzerinde harf, rakam, özel karakterler ve özel fonksiyon tuşlarının bulunduğu bir bilgisayar giriş birimidir. Bilgisayar temelde klavye aracılığıyla yönlendirilir ve kumanda edilir. Klavyenin tuşlarına basıldığında, basılan tuşun kodu bilgisayarın CPU'su tarafından değerlendirilmek üzere belleğe aktarılır ve yankısı ya da neticesi ekrana gelir. Klavyeler üzerindeki harf tuşlarının diziliş şekline göre F veya Q tipi olurlar. Farklı firmaların ürettiği klavyelerde bazı farklı tuşlar bulunabilir. Q klavye: İngiliz klavyesi olarak da adlandırılır. Q harfi, klavyenin sol başında yer alır. F klavye: Türkçe klavye olarak da adlandırılır. Bu klavyede harf dizilişi, daktilolardaki gibidir. Q Türkçe klavye: Q klavyede Türkçe Ö, Ç, Ş, I, Ğ, Ü harfleri, sağ tarafa yerleştirilmiştir.

Klavyenin üzerinde bulunan bazı tuşlar, ekrana bir karakterin yazılmasına neden olmazlar. Çünkü bu tuşlar bir görüntüden öte bir etki oluştururlar. Ancak bu tuşların işlevleri programdan programa değişiklik gösterebilir. Örneğin birçok programda F1 tuşuna basıldığı zaman o sırada çalışan program veya yapılan işleme bağlı olarak ekrana yardımcı bilgi getirilmektedir. Bu tuşlardan bazıları;

Enter tuşu: Bilgisayara bir işi yapmasını söylemek, bir komutu çalıştırmak için kullanılır. Kelime işlemcilerde ise yeni bir paragrafa geçmeyi sağlar.

Esc (Escape) tuşu: O sırada yapılan işi yanda kesmek, vazgeçmek veya geriye dönmek amacıyla kullanılır. Windows uyumlu programlarda Esc tuşu genellikle iptal düğmesini temsil eder.

Fonksiyon tuşları (F1, F2, … F12) : Bu tuşlar belirli bir işlemi çabucak yapmak için kullanılır. Örneğin F1 tuşu çoğu programda yardım bilgilerini ekrana getirir.

Tab tuşu: Kelime işlem programlarına paragraf girintisi için, Windows'ta iletişim kutusu pencerelerinde ise düğmeler arası geçişte kullanılır.

Caps Lock tuşu: Bu tuşa bir kez basınca (klavyenin sağ üst köşesinde ilgili ışık yanar ve) klavyeden hep büyük harf girebilirsiniz. Bir kez daha basarsanız, yine küçük harf moduna geçilir.

Shift tuşu: Bu tuşa bir harf tuşu ile birlikte basıldığında, o harfi büyük yazmakta veya bir rakam tuşu ile birlikte basıldığında ise o rakam tuşunun üst kısmında belirtilen özel karakteri yazmaktadır.

Ctrl ve Alt Tuşları: Başka tuşlarla birlikte aynı anda bastığınızda, belirli işlemleri yapmaya yarar.

Alt Gr tuşu: Q dizilişine sahip klavyelerde Türkçe 'ye özgü ç,ş,ü ve ö gibi harflere yer bulabilmek için bazı tuşlara 3. bir görev verilmektedir. Bu 3. görevi kullanabilmek Alt Gr tuşu basılı iken söz konusudur.

Sağ fare tuşu: Windows'ta sağ fare tuşu ile aynı görevi görür. Klavyedeki yeri boşluk tuşunun sağındaki Ctrl tuşunun solundadır. Bu arada Ctrl, Shift ve Enter tuşları kullanım kolaylığı düşünülerek klavye üzerinde ikişer adettir.

Back Space (Geriye Silme) tuşu: Klavyede rakamların bulunduğu sırada en sağda olan bu tuş, ışıklı göstergenin(imlecin) solunda bulunan karakteri silmek için kullanılır. İmlecin solundaki karakter silindiği için sağında bulunan bütün karakterler bir karakter genişliği kadar sola kayarlar.

Del (Delete) tuşu: Del tuşu ise imlecin sağındaki karakteri siler.

İns (İnsert) tuşu: İnsert tuşu açık/kapalı mantığıyla çalışır. İnsert açıkken yazılan karakterler sağdaki karakteri ileri doğru iterek araya yerleşir. İnsert kapalı iken ise yazdığımız karakterler daha önceki karakterlerin üstüne yazılır.

Home tuşu: Bu tuş satırın başına gitmemizi sağlar.

End tuşu: Bu tuş satırın sonuna gitmemizi sağlar.

Page Up tuşu: Bu tuş bir sayfa yukarı çıkmamızı sağlar.

Page Down tuşu: Bu tuş bir sayfa (bir ekran görüntüsü kadar) aşağı inmemizi sağlar.

Pause tuşu: Bu tuş yapılan işlemin bir tuşa basana kadar durdurulmasını sağlar. Bir tuşa basınca işlem kaldığı yerden devam eder.

Print Screen tuşu: Windows ortamında bu tuşa bastığınızda ekranın resmi çekilir. Ancak ekranın resmi yazıcı yerine, geçici bilgi saklama ortamı olan ve Pano adı verilen ortama

aktarılır. Daha sonra panoda saklanan resmi Paint gibi bir boyama programına aktarıp istediğiniz gibi kullanabilirsiniz.

İmleç tuşları: Bu tuşlarla imleci ekranda istediğiniz yere götürebilirsiniz.

Nümerik klavye: Num Lock ışığına bağlı olarak, buradan rakamları girebilir veya imleci kontrol edebilirsiniz. Num Lock ışığını "Num Lock" tuşu yakar veya söndürür. Bunlardan başka yeni tip klavyelerde Sleep(Stand-by/Bekleme uyuma modu), Power (açmakapama) gibituşlar da vardır.

2.12 Mouse (Fare)

Mouse (fare), klavyeden farklı olarak sadece komut girişinde kullanılır. Bilgisayar ortamında kullanılabilmesi için çalışan programın, Mouse kullanımına uygun şekilde yazılmış olması gerekir.

Mouse altında yer alan bilye, optik ya da lazer düzenek, mouse göstergesinin ekranda istenilen yere hareket etmesini sağlar. Mouse, üzerinde yer alan tuşlarla seçme, açma vb. işlemler yapılır. Mouse, avuç içinde tutularak bilekten hareket ettirilerek kullanılır.

2.13 Yazıcı (Printer)

Bilgisayarda yer alan bilgilerin kâğıda yazdırılmasını sağlayan elektronik ve mekanik parçalardan oluşmuş yan ünitedir. Piyasada birçok tür ve marka yazıcı bulunmaktadır.

Karakterleri yazış şekillerine göre aşağıdaki şekilde gruplandırılabilir.

Nokta Vuruşlu (Dot Matrix)Yazıcılar: Nokta vuruşlu yazıcılar, bir satıra yazdıkları karakter sayısına göre iki gruba ayrılırlar. 80 sütunluk yazıcılar, bir satıra normalde 80 karakter yazarlar. Sıkıştırılmış olarak 132 karakter yazabilirler. 136 sütunluk yazıcılar ise bir satıra normalde 132 karakter yazarlar. Sıkıştırılmış olarak 236 karakter yazabilirler. Bu yazıcılarda, yazma kafasında yer alan iğne (pin) sayısına göre yazım kalitesi değişir. İğne sayısına göre 9 ve 24 olmak üzere iki çeşittir. Nokta vuruşlu yazıcıların hız birimi CPS (Character Per aSeconds) ile ifade edilir. Hız birimi saniyede bastığı karakter sayısı ile belirtilir.

Mürekkep Püskürtmeli Yazıcılar (İnkjet Printer): Karakterleri mürekkep püskürterek yazarlar. Renkli ve grafik basımında diğer yazıcılara göre daha iyi olduğu söylenebilir.

Lazer Yazıcılar (Laser Printer): Nokta vuruşlu yazıcılara göre bu yazıcıların yazım kalitesi ve hızı mükemmeldir. Fotokopi makineleri gibi çalışırlar. Nokta vuruşlu yazıcılar satır satır, lazer yazıcılar ise sayfa sayfa basım yapar. Lazer yazıcıların hız birimi PPM (Page Per Minute) ile ifade edilir. Hız birimi dakikada bastığı sayfa sayısı ile belirtilir.

2.13.1 Yazıcılarda Kullanılan Ölçü Birimleri

Çözünürlük (dpi - dots per inch) Bir yazıcının kâğıt üzerindeki her inç başına (2.52 cm2) basabileceği nokta sayısını belirtir. Örneğin 300 dpi'lık bir yazıcı, 2.54 cm2'lik bir alana 300 nokta basabilir.

Hız (PPM - Pages Per Minute) Yazıcının hızı dakikada basabildiği kâğıt adedi ile ölçülür. Örneğin 5 ppm hızındaki bir yazıcı dakikada 5 sayfa yazı basabiliyor demektir.

2.14 Çizici (Plotter)

Çiziciler özellikle grafik çıktıların alınmasında kullanılan aygıtlardır. Renkli kalemler kullanılmak suretiyle renkli çıktılar alınabilir. Çiziciler genellikle mimarlık ve mühendislik uygulamalarında kullanılır.

2.15 Tarayıcı (Scanner)

Tarayıcılar fotoğraf, grafik ve düz yazılan okuyup bilgisayara aktaran aygıtlardır. Bilgisayara aktarılan resim ve grafikler üzerinde değişiklik yapılabilmektedir. Düz yazılar ise kelime işlem programlan(OCR optik karakter tanıma programı) ile değiştirilebilmektedir.

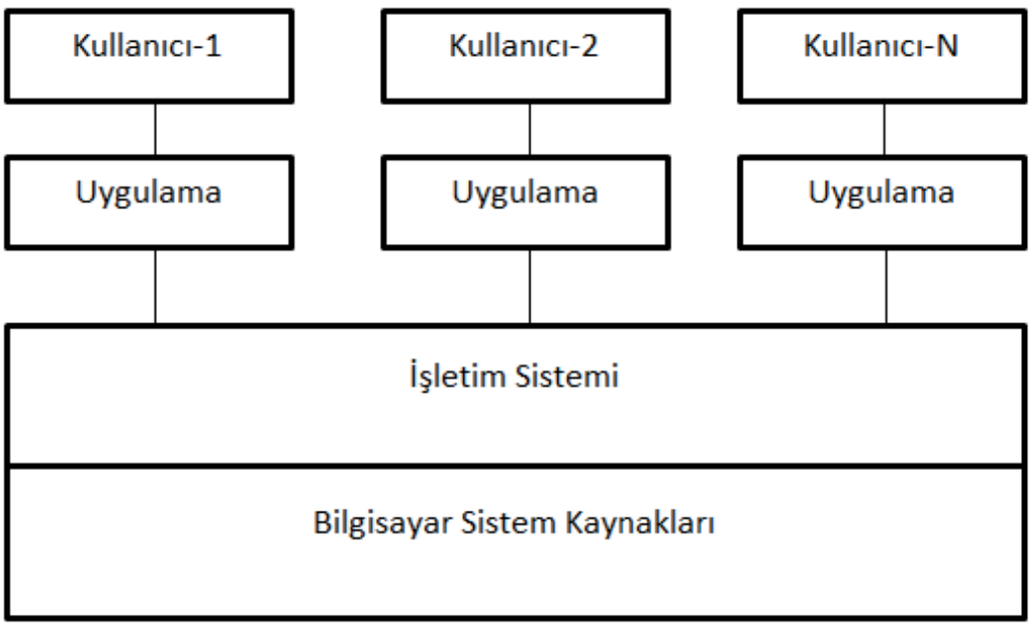
2.16 Modem

Modem, tanım olarak "Modülator" ve "Demodülator" kelimelerinin birleşiminden üretilmiştir. Modem, bilgisayarların genel ağa bağlantısını sağlayan ve bir bilgisayarı uzak yerlerdeki bilgisayarlara bağlayan aygıttır.

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
- Windows Server 2019
- Windows Server 2022

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.

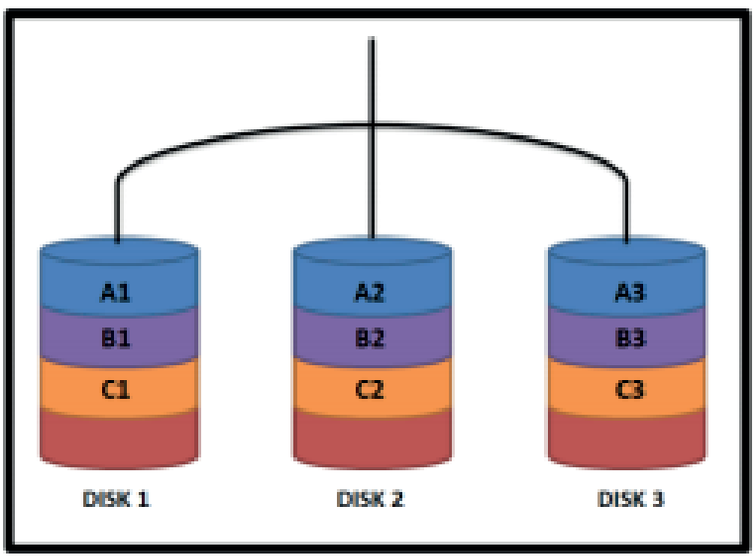
RAID ile ilgili olarak bilinmesi gereken bazı hususlar;

* 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.

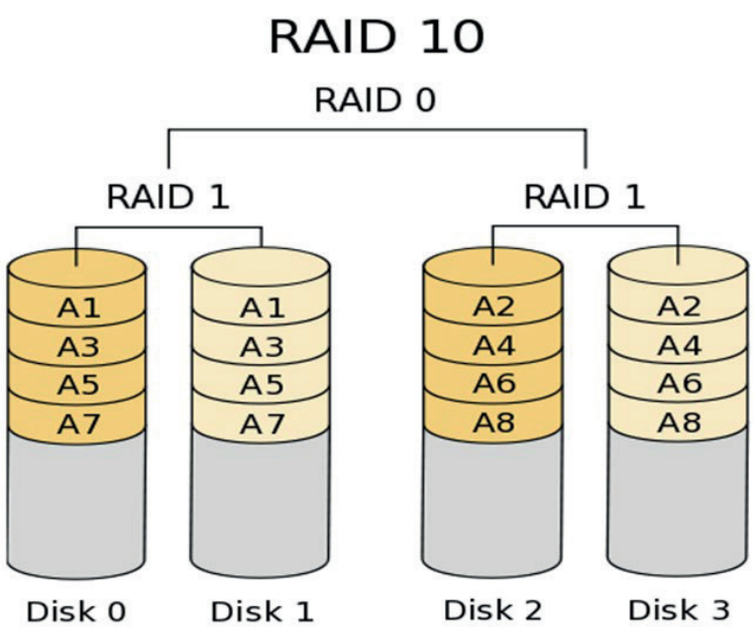
Bir algoritma ile bilgiler disklere sırası ile yazılırken, her defasında bir diske yazılan bilgilerin algoritması kaydedilir. Bu şekilde devam eden veri yazma işlemi ile RAID 5 sistemindeki herhangi bir diskin arızalanması durumunda sistemin çalışmaya devam etmesi, arızalı diskin sistem kapanmadan değiştirilmesi 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.

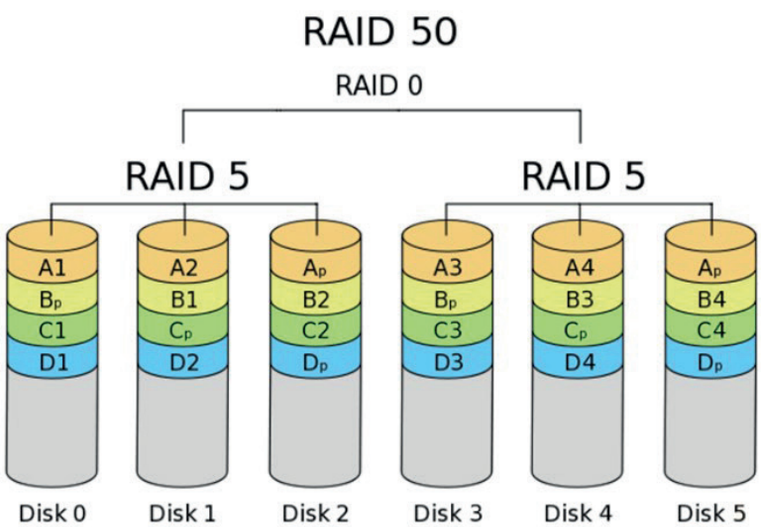
RAID 10

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 , Windows Server 2019 , Windows Server 2022 ve Linux işletim sistemleri kullanılmaktadır.

Kişisel bilgisayarlarda ise; Windows XP, Windows 7, Windows 8, Windows 10 ve Windows 11 işletim sistemleri kullanılmaktadır.

3. KORUYUCU BAKIM

Herhangi bir koruyucu bakım programının amacı, pahalı bilgisayar onarımlarının önüne geçmektir. Bu bölümde, koruyucu bakımın önemi vurgulanmakta ve bunu gerçekleştirmek için gereken araç-gereçler tanımlanmaktadır. Uygun bakım, donanımın ömrünü uzatmaya yardımcı olabilir. Yardımcı yazılımlar, bir bilgisayar sistemini daha hızlı ve daha verimli hale getirebilir. Bu bölümde ayrıca, bir bilgisayar üzerinde çalışmak ve bileşenlerden kurtulmak için önemli güvenlik talimatları da ele alınmaktadır.

3.1 Genel Bilgiler

Bilgisayar teknisyeni/teknikeri, kendi başına ve belirli bir süre içerisinde, bilgisayar montajını ve kuruluşunu yapma, bilgisayarın sorunsuz çalışmasına engel olan faktörleri tespit edip çözüm getirme, bakım ve onarım yapma bilgi ve becerisine sahip nitelikli kişidir.

3.1.1 Bilgisayar Teknikeri/Teknisyeni:

1. Bilgisayar montajı yapar ve işletim sistemi ile çevre birimleri sürücülerini yükler.
2. Bilgisayara klavye, fare, monitör ve çevre birimlerinin bağlantısını yapar ve çalışmasını test eder, network bağlantılarını kurar.
3. Arızalı bilgisayarın bildirim formlarını ve önceki arıza kayıtlarını inceler.
4. Kullanılan araç ve gereçleri hazırlar ve gerekli onarımları yapar.
5. Donanımların güvenli şekilde taşınmasını sağlayıcı ve bilgi kaybını önleyici önlemler alır.
6. Virüs olup olmadığına bakar ve hata mesajlarını değerlendirir.
7. Sistem dosyalarının silinmiş ve/veya zarar görmüş olup olmadığına bakar.
8. Yüklenen programların işletim sistemi ile uyumluluğunu kontrol eder.
9. Donanım test programlarını çalıştırır.
10. Çevre birimleri sürücüleri, kasa içindeki kablo bağlantıları ve kartları, setup (Kurulum) ayarları ve güç kaynağını kontrol eder.
11. Setup (Kurulum) ayarlarını yapar ve virüsleri temizler.
12. Hard diski formatlar, disket ve/veya CD/ROM sürücülerini temizler.
13. Disket sürücüsünü, güç kaynağını, klavye ve fareyi onarır veya değiştirir.
14. Hard diski, bellek kartını, CD/ROM sürücüsünü, ekran, multimedya, çevre birimlerini, network kartlarını, enerji ve veri kablolarını, bilgisayar pilini, işlemciyi ve anakartı değiştirir.
15. Bilgisayarın periyodik bakımını yapar.

Bu hususları grafik olarak aşağıdaki gibi özetleyebiliriz:

3.1.2 Bir Koruyucu Bakım Programının Öğeleri

Her koruyucu bakım programının ana hedefi, sistemi gelecekte oluşabilecek sorunlara karşı korumaktır. Bir koruyucu bakım ilkesi geliştirirken aşağıdaki 2 sorunun cevaplandırılması gerekir.

1) Koruyucu bakım ne zaman planlanmalıdır?

Kesin zamanlar özel taleplere bağlıdır. Önemli olan bir zaman çizelgenizin olmasıdır. Bir koruyucu bakım ilkesi geliştirirken otomatikleştirilmiş görevlerin gece yapılıp yapılamayacağını ve gece veya hafta sonları ne gibi yükseltmelerin yapılması gerektiğini belirleyiniz. Belirli görevlerin, günün, haftanın ve ayın belirli zamanlarında tamamlanması için bir zaman çizelgesi hazırlanmalıdır. Bu zaman çizelgesinde sunucu odası ve bilgisayar

laboratuvarının belirlenen zamanlarda bakım ve kontrolünü içeren bilgiler yer alır. Bilgisayar teknisyeni bu zamanlarda, önceden tespit edilen bakım ile ilgili hususları yapar.

2) Ne tür bakıma ihtiyaç vardır?

Uygulanan bakım türü kişisel koşullara bağlıdır. Örneğin, sürekli güncellenen sistemlerin daha sık desteklenmesi gerekir. Internet erişimi olan sistemler sürekli virüs taramasından

geçirilmelidir. Büyük sorunların oluşmasını beklemek yerine küçük sorunlara eğilmek daha kolay olduğundan, bu belirlemeleri, koruyucu bakım ilkesinin bir parçası olarak yapınız.

3.1.3 Önlem

Sunucu odası ve bilgisayar laboratuvarından sorumlu teknisyen her şeyden önce bilgisayar sistemleri donanım ve yazılım olarak zarar görmeden önce gerekli tedbir ve önlemleri almalıdır. Önceden alınacak küçük bir güvenlik önlemi, daha sonra ortaya çıkabilecek büyük arızaların önüne geçebileceğini hiçbir zaman akıldan çıkarılmamalıdır. Zaten, koruyucu bakım, sistemler zarar görmeden önce alınacak önlemleri içerir. Bu önlem ve tedbirleri aşağıdaki gibi sıralayabiliriz:

1. Teknisyen/Tekniker, sunucu odası ve bilgisayar laboratuvarının fiziksel olarak güvenlik önlemlerini almalıdır.
2. Yetkisiz ve sorumlu olmayan kişilerin girişine izin vermemelidir.
3. Ortamı sürekli temiz ve bakımlı tutmalıdır.
4. Çevresel yönergeler, anlatılacak olan ortam ile ilgili hususlara dikkat etmelidir.
5. Bakım zaman çizelgesinde belirlenen zamanlarda donanımların ve yazılımların bakımını yapmalıdır.
6. Bilgisayar çevre birimlerinin bakım ve kontrolünü yapmalıdır.
7. Sistemlerde bulunan aygıtların kendi sürücülerini yüklemeli ve güncel tutmalıdır.
8. Sistemlere gereksiz yazılımların yüklenmemesi için tedbirler almalıdır.
9. Lisansız yazılımlar kullanılmamasını sağlamalıdır.
10. Güncel olmayan yazılımları sistemden kaldırmalıdır.
11. Sistemleri sürekli virüs taramasından geçirmelidir.
12. Virüs programını güncel tutmalıdır.
13. Sistemde bulunan önemli verilerin yedeğini periyodik olarak almalıdır.

3.1.4 Araç-Gereçler

3.1.4.1 Araç-Gereç Çantaları

Bir teknisyenin, şekilde gösterildiği gibi temel araç-gereci içeren bir alet çantası olmalıdır.

Tipik teknisyenin araç -gereç takımı

Buna ek olarak, bir araç takımında bulunması gerekenler aşağıdaki gibidir:

- Anti statik bilek bandı ya da diğer anti statik aygıtlar
- Düz kafalı tornavida
- Yıldız kafalı tornavida
- Somun ağızlı tornavida
- İğne burunlu pense
- Köşegenler veya enine kesimli penseler
- Dar bölgelerde görmeyi kolaylaştırmak için bir ayna
- Sayısal /Analog avometre
- Cep feneri

Bir teknisyenin araç takımında çeşitli düz kafalı ve yıldız kafalı tornavidalar bulunmalıdır. Teknisyenler çok farklı vida ve somun türleriyle karşılaşabilir. Bazı vidalar, teknisyenin onlara ulaşabilmesi için farklı uzunlukta tornavidalar gerektirebilir. Manyetik araçlar, kullanışlı olmalarına rağmen iç bileşenlere zarar verebileceklerinden, bilgisayarın içinde kullanılmamalıdır. Yeterince güçlü bir mıknatıs, diske, anakarta veya diğer iç bileşenlere zarar vermeye yetecek akım üretebilir.

Teknisyenler telleme ve kablolama üzerinde çalışarak çok zaman geçirirler. Bazen, bir telin veya kablonun kesilmesi gerekir. Köşegenler veya enine kesimli penseler, teknisyenin, telleri veya kabloları tam istedikleri gibi kesmelerini mümkün kılar.

Bir araç takımında bir soket set anahtar takımına da ihtiyaç vardır. Bilgisayar vidalarının çoğu altı köşeli başlığa sahiptir ve teknisyen altı köşeli vidaları gevşetmek veya sıkıştırmak için bir somun ağızlı tornavida kullanabilir. Dar denkleri ya da etraftaki köşeleri görmek için bir ayna kullanılabilir.

Ayrıca, bir anti statik vakumlu temizleyici, kutulanmış hava, çeşitli çözgenler ve tiftiksiz bezlerin de bulunması gerekir. Normal vakumlu temizleyiciler statik ürettiğinden, bilgisayar bileşenleri için anti statik vakumlu temizleyiciler kullanılmalıdır. Vakumlu temizleyicinin bir bilgisayarda kullanılmak üzere özel olarak onaylanmış olması gerekir. Tipik bir vakumlu temizleyici, lazer kartuşundan toner temizlemek için kullanılmamalıdır. Toner partiküllerinin tutarlılığı için yüksek süzme kapasitesine sahip bir vakumlu temizleyiciye ihtiyaç vardır.
Sıkıştırılmış kutuda hava, bilgisayar bileşenlerini temizlemek için en faydalı araçlardan biridir. Bir kutu hava, bilgisayarın içindeki tozu statik elektrik yaratmadan çıkarabilir. Tozun erişilemeyen bölgelere uçmasını engelleyiniz. Bilgisayar kasasının veya bileşenlerinin dışını temizlemek için biraz su ve yumuşak bir sabunla tiftiksiz bir bez kullanılabilir.

3.1.4.2 Kablo Test Cihazları

RJ11,Rj12,RJ45 ve BNC uçlu kabloları test etmekte kullanılan cihazlardır. Kablonun kısa devre veya kopuk olup olmadığını, yanlış uç bağlantılarını test etmekte de kullanılır. Mevcut bağlantı durumunu gösteren LED ile teçhiz edilmiştir. Cihazda mevcut bulunan ton jeneratörüne harici bir "tone tracer" bağlayarak döşenmiş kablolardaki kısa devre ve kopuklukları sınırlandırmak mümkündür.

3.2 Genel Bilgi

Bilgisayarlar ve diğer elektronik aygıtları belli bir süre sonra kullanılmaz hale gelir. Bu sorun, aşağıda sıralanan nedenlerden kaynaklanır:

- Makine eski olduğundan ve ekonomik olmadığından, parçalar veya bileşenler daha sık arızalanmaya başlar.
- Bilgisayar, başlangıçta planlandığı uygulamalar için artık yetersiz kalır.

- Önceki modellerin yerini, geliştirilmiş özelliklere sahip daha yeni makineler alır.
- Sonuç olarak, eski bilgisayarlardan veya parçalardan nasıl kurtulabileceğimizi sormaya başlarız.

Bilgisayarlar ve yan birimleri, çevre dostu olmayan bazı maddeler içerir. Bilgisayar bileşenlerinin çoğu, ya zararlıdır ya da belli bir düzeyde zararlı madde içerir. Atık maddeler zararlı olarak sınıflandırılır. Çünkü uygun olarak kullanılmadığında insan sağlığına ve çevreye zararlı oldukları bilinir. Zehirli atık olarak da bilinen zararlı maddeler genellikle, kadmiyum, kurşun veya cıva gibi ağır metal konsantrasyonları içerir. Bilgisayar baskılı devre kartları, plastik, kıymetli metaller, fiber cam, arsenik, silikon, galyum ve kurşundan oluşur. Katot ışınlı tüp - cathode ray tube- (CRT) monitörleri, cam, metal, plastik, kurşun, baryum ve seyrek toprak metalleri içerir. Taşınabilir sistemlerden gelen piller, kurşun, kadmiyum, lityum, alkalik manganez ve cıva içerebilir. Bilgisayar donatımında kullanılan temizlik maddelerin çoğu da zararlı maddeler olarak sınıflandırılabilir.

3.2.1 Ortam Güvenliği ve Sunucu Odası İçin Yönergeler

Sunucu odasında sıcaklık önemlidir. Sunucu kesinlikle sıcak boru geçişinin yakınına veya klimanın yanına yerleştirilmemelidir. Motorlar ve mikro dalgalar gibi öğeler elektromanyetik girişime (Manyetik alan etkisi) yol açabilir. Elektromanyetik girişim (EMI) de önlenmelidir. Yalnızca, yalıtılmış topraklama devreleri kullanılmalıdır.

Sunucunun etrafındaki alanın kullanılmayan malzemeler ve karışıklıktan uzak tutulması gerekir, ideal olan, sunucuyu, erişimi sınırlandırılmış ve hiçbir şekilde darbe almayacak, sarsılmayacak, doğrudan erişilemeyecek ya da yönetici olmayanlar tarafından rahatsız edilemeyecek biçimde bir dolaba kilitlemektir. Teknisyenin ve donatımın güvenliği için tüm kablo ve tellerin güvence altına alınması gerekir. Tavan ile binanın bir sonraki katının zemini arasında bulunan alçaltılmış tavanın üstündeki alan, ağ yöneticileri ve yangın denetçileri için çok önemlidir. Tesisat boşluğu denen bu alan, bir bina etrafındaki ağ kablolarını çalıştırmak için uygun bir yerdir. Tesisat boşluğu, genellikle, havanın içinde rahatça dolaşabildiği açık bir alandır. Bu nedenle, yangın denetçileri buna özel bir önem verir.

Bakır tabanlı kablolama için en yaygın dış kaplama, polivinil klorür PVC'dir. PVC kablolama, yandığında, zehirli dumanlar çıkarır. Yangın talimatları, zehirli dumanların bina içinde rahatça dolaşmasını engellemek için, tesisat boşluğunda PVC kablolamayı yasaklar. Tesisat boşluklarında, duvarlarda ve yangın kodlarının PVC kablolamayı yasakladığı diğer alanlarda,

tesisat boşluğuna uygun üretilmiş bakır tabanlı kablolama, kablo kanalı olmaksızın kullanım için tasarlanmıştır. Tesisat boşluğu seviyesinde kablolama, PVC kablolamadan daha zor ve daha pahalıdır, bu yüzden de birincil olarak, PVC kablolamanın kullanılamadığı yerlerde kullanılır.

3.2.2 Sıcaklık

İnsanlar gibi, bilgisayar sistemleri de belirli sıcaklıklar arasında işlevselliklerini sürdürebilir. Birçok bilgisayar sistemi için 10-30 C arası sıcaklıkların korunması uygun olacaktır. Eğer bilgisayar sistemlerinizin dışındaki sıcaklıklar çok yüksek ise sistemlerin havalandırma düzenekleri doğru biçimde çalışmayı sürdüremeyecek ve bilgisayarınızın bileşenleri zarar görebilecektir. Eğer sıcaklık çok düşerse, bilgisayar sistemleriniz açıldığında termal şoka uğrayarak elektronik devrelerinin çatlaması nedeniyle çalışmaz hale gelebilecektir.

Sıcaklık yönetimine ilişkin öneriler aşağıda sıralanmıştır:

a) Bilgisayar sistemlerinizin belgelemesinden faydalanarak uygun sıcaklık aralıklarını tespit ediniz.

b) Sistem odanıza bir sıcaklık alarmı yerleştirerek çok sıcak ve çok soğuk durumlarda Alarmların uyarı vermesini sağlayınız.

c) Bilgisayar sistemlerinizi duvarlara çok yakın yerleştirmemeye özen gösteriniz. Duvarlara çok yakın yerleştirdiğiniz takdirde, havalandırmayı engelleyerek bilgisayarlarınızın iç sıcaklıklarının yükselmesine neden olabilirsiniz. Birçok üretici, bilgisayarlarının her kenarının duvardan 15-20 santimetre açıkta olmasını önerir.

Tanımlanması en kolay çevresel konulardan biri, sıcaklıktır. Sıcak bir bilgisayar odası, bir soruna işarettir. Ağ teknisyenlerinin, bilgisayar donatımı için işletim sıcaklıklarından haberdar olması gerekir. Tipik bir sunucu aşağıdaki aralıklarda işlem görecektir:

- İşletim sıcaklığı: 5 0°F ile 95 °F (10-3 5 °C)
- Bellek sıcaklığı: 40°F ile 95°F (4,4-35°C)

3.2.3 Nem

Nem, bilgisayar sistemlerinin çalışabilmesi için gereklidir. Ancak havadaki nem oranının aşırı yükselmesi sistemlerinize zarar verebilir. Nem, sistem odanızda statik elektrik yüklenmesini azaltacak yönde etkisini gösterir. Nemin çok az olması, statik elektrik yüklenme ve aktarımlarını arttırarak manyetik teyp ve benzeri bileşenlerde sorunlara yol açar. Nem

oranının çok yükselmesi ise bilgisayar sistemlerinizin devrelerinde kısa devrelere kadar uzanan sorunlara neden olabilir.

3.2.4 Nem düzeyinin korunmasına ilişkin alınabilecek önlemler aşağıda sıralanmıştır:

a) Nem düzeyini %20 ile %50 arasında tutmalısınız.

b) Yüksek güvenilirlik gerektiren ortamlar için nem düzeyinin belirlenen sınırlar dışına çıkması durumunda devreye girecek alarm sistemleri kullanmalısınız.

c) Bilgisayar sistemlerinin ya da çevre birimlerinin bir grubunun nem duyarlılığı diğerlerinden daha yüksek olabilir. Uygun nem düzeyinin tespiti için cihazlarınızın kullanım kılavuzlarına göz atmalısınız.

3.2.5 Hava Özellikleri

Sunucu işletim ortamına ilişkin hiçbir tartışma, hava niteliğini hesaba katmadan tamamlanmış sayılmaz. Bu genellikle, veri merkezi ortamlarına ilişkin bir konu olmasa da sunucular çok tozlu ve kullanılmayan malzemeli alanlara yerleştirildiğinde göz önünde bulundurulması gereken bir konudur. Bir sunucunun üzerindeki fanlar, havadaki tüm tozun sistemin içinden geçerek çekilmesine ve bileşenlerin üzerinde birikmesine yol açabilir. Bileşenler tozla kaplanırsa, aşırı ısınabilir ve arızalanabilir. Donatım, hava niteliğinin şüpheli olduğu bir alanda bulunuyorsa, ağ teknisyeninin, bir vakumlu bilgisayar temizleyicisi veya kutulanmış hava kullanarak sistemi temizlemek için haftalık veya aylık bakım planlaması gerekir.

3.2.6 Duman

Duman, bilgisayar sistemlerine derinden zarar verir. Bilgisayar disklerinin kafalarına, optik disklere ve teyp sürücülerine etki eder. Bilgisayar sistemleri ve monitörler de belli durumlar altında duman üretebilir, birbirlerine zarar verebilir. Ancak duman konusunda en tehlikeli kaynak sigaradır. Duman, klavyelerin çok daha hızlı bozulmalarına neden olacaktır.

Duman konusunda önerilen önlemler aşağıda sıralanmıştır:

a) Sistem odasında ve sistem odasını kullanan yetkili kişilerin yanında sigara içilmesine izin vermeyiniz.

b) Sistem odasına mutlaka duman detektörleri yerleştiriniz.

c) Yükseltilmiş zeminin olduğu odalarda zeminin altına, alçaltılmış tavanın olduğu odalarda tavanın üstüne duman detektörleri yerleştirmelisiniz. Uygun olduğu takdirde, hem zeminin altına hem de tavanın üzerine detektör yerleştirmekten kaçınmayınız.

3.2.7 Toz

Toz verilere zarar verir. Duman gibi, toz da disk kafalarında birikerek disklerinizi çalışmaz hale getirebilir. Uzun vadede hem kayıt kafasına hem de disk kayıt ortamına zarar vererek disklerinizi bir çöp haline dönüştürebilir. Havada uçuşan tozun büyük bölümü elektriksel olarak iletkendir. Birçok bilgisayar sisteminde tasarımları sebebiyle, soğutma vantilatörleri aracılığı ile toz sistem içinde çekilmekte ve uzun sürede tozun sistem kartlarının kapladığı görülmektedir. Kartlar üzerinde biriken bu toz parçacıkları, kısa devrelere neden olarak bilgisayarlara zarar vermekte, kimi durumlarda ise bilgisayar sistemlerinin iç sıcaklıklarının artmasında da bir etken olmaktadır.

Toz konusunda sunulan öneriler aşağıda sıralanmıştır:

Sistem odanızı olabildiğince tozdan arındırınız.

a) Eğer bilgisayarlarınızın hava filtreleri varsa, periyodik olarak değiştiriniz ya da temizlenebilir türde ise temizleyiniz.

b) Bilgisayar sistemlerinin temizliğinde kullanmak üzere bir kompresör edininiz ve periyodik olarak kullanılmasını sağlayınız. Bilgisayar kasalarının içerisinin de kompresör ile temizlenmesini sağlayınız.

c) Tozu kolayca engelleyemediğiniz ortamlarda, bilgisayar sistemlerinin tozdan daha az etkilenmesi için sıradan örtüler ile örtmeyi denemeyiniz. Isının hızla yükselmesine neden olarak bir yangına sebebiyet verebilirsiniz.

4. 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.

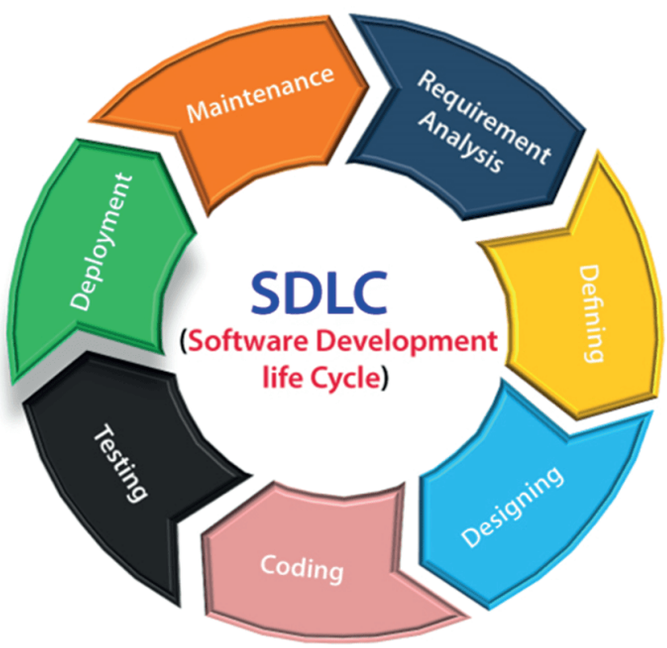
ELEKTRONİK YAZILIMLARI

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:

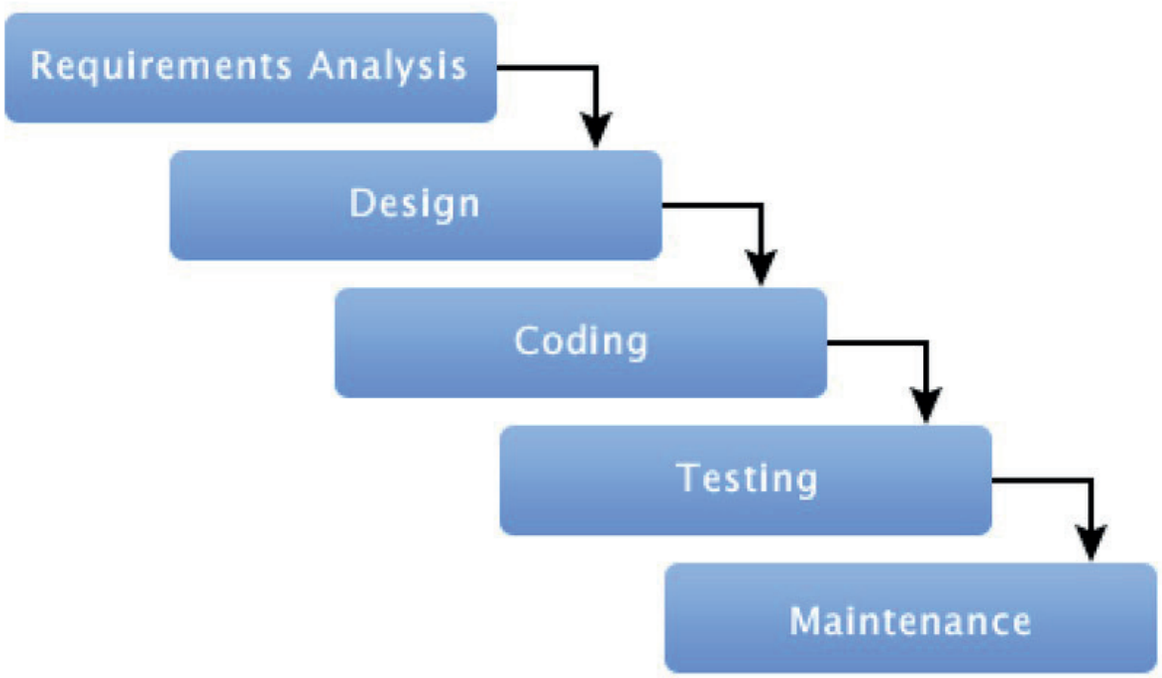
Gereksinim Tanımlama: Gerçekleştirilecek sistemin gereksinimlerinin belirlenmesi işidir. Müşteri ne istiyor? Ürün ne yapacak, ne işlevsellik gösterecek?

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.

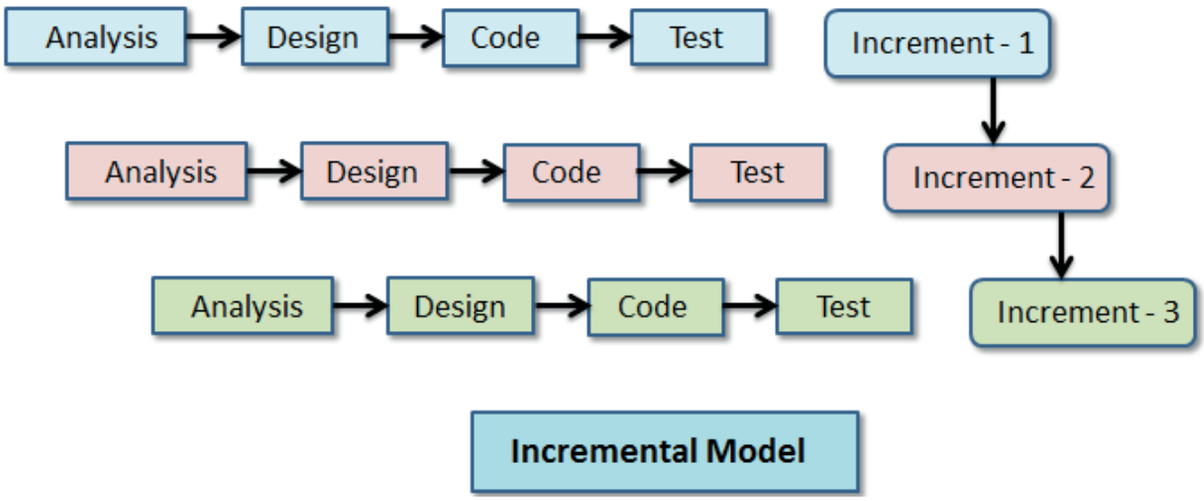
Kazançları:

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.

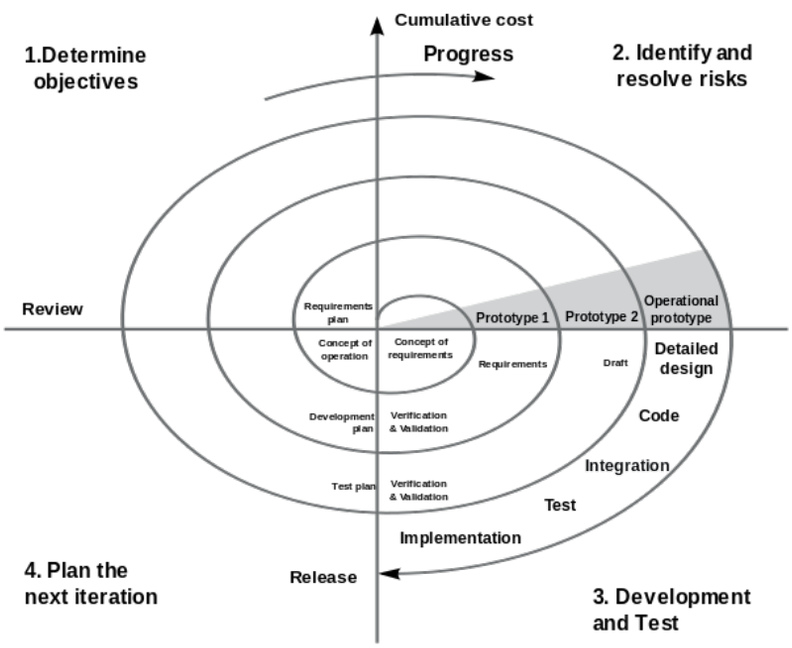
Her döngü süreçteki bir aşamayı ifade eder.

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.

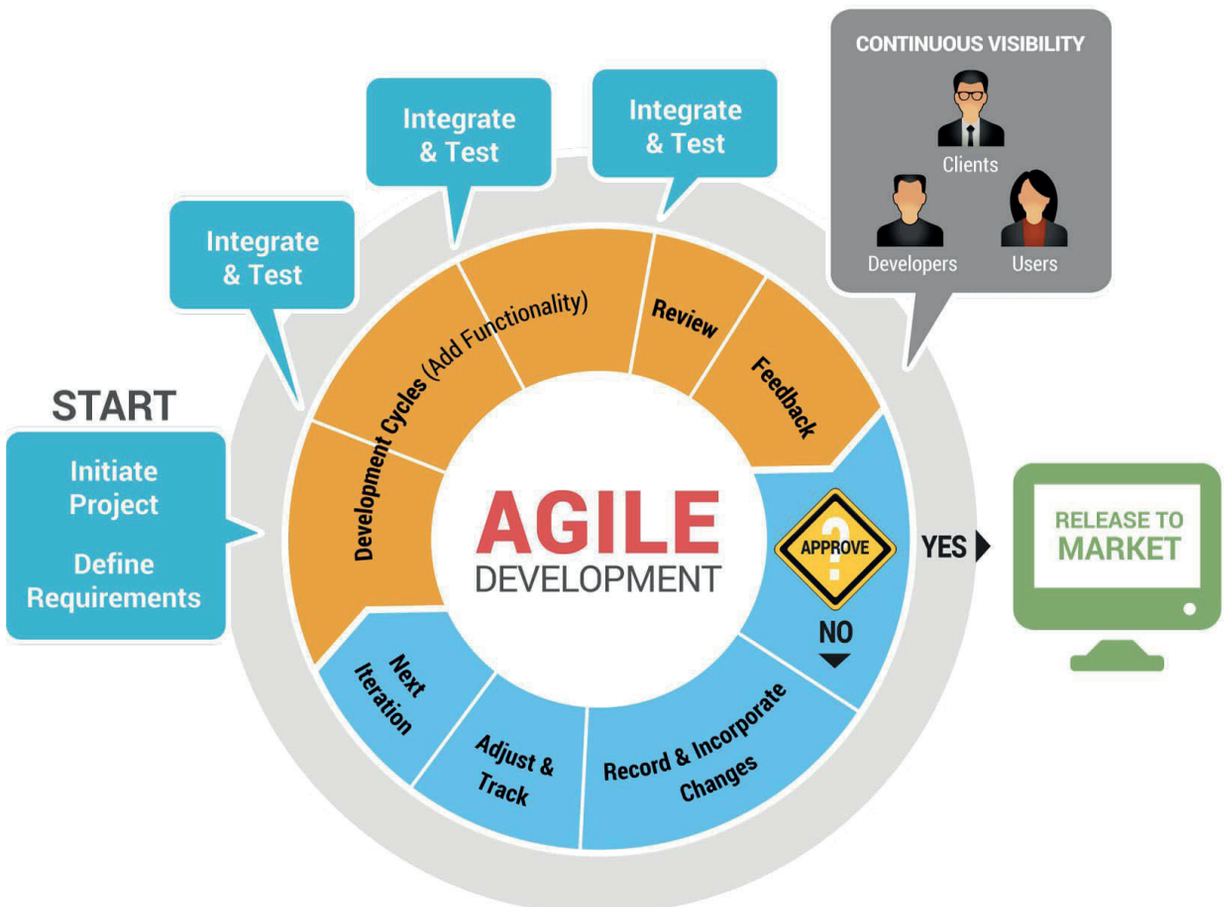
2001 yılında, dünyanın önde gelen çevik modellerinin temsilcileri, ortak bir zeminde buluşabilmek adına bir araya gelerek **"Çevik Yazılım Geliştirme Manifestosu"** nu yayınlamışlardır. Bu manifestoya göre:

- 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.

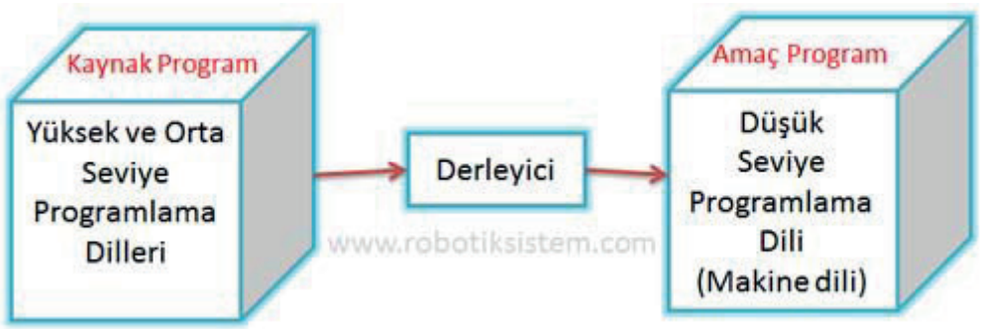
Programlama dilleri insanların algılamasına yakın olmasına göre 3 gruba ayrılır.

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 prog. 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.



<u>En Çok Kullanılan Programlama Dilleri:</u>

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

5. 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.

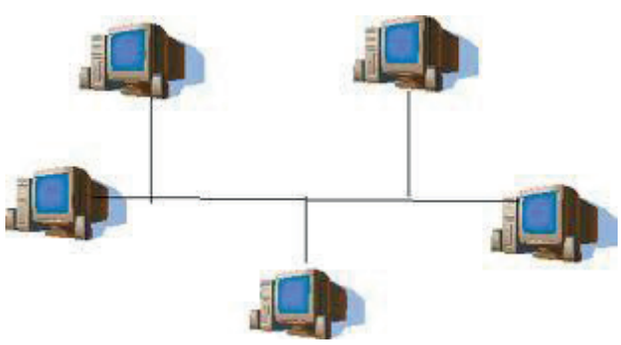
Yapılarına göre bilgisayar ağları 3 temel özellik gösterirler:

- 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.

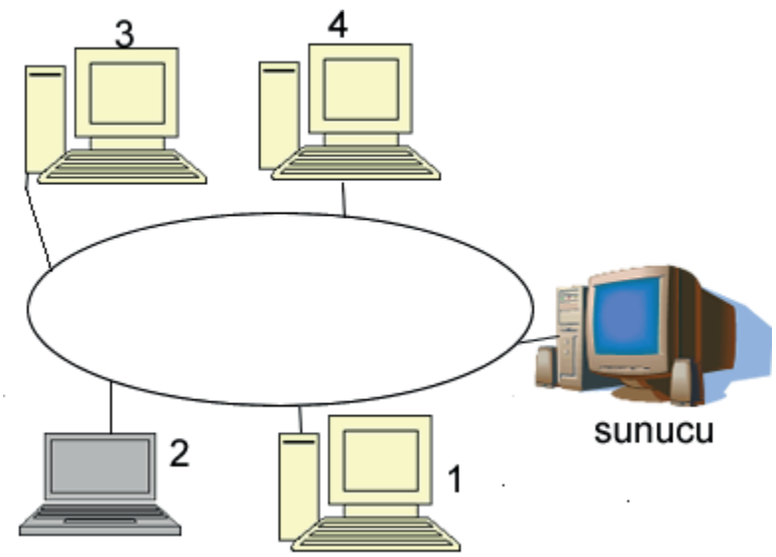
En büyük olumsuz yönü iletişim hattında bir arıza olduğu zaman çalışan hattın dışında kalanların çalışamaz olmasıdır. Bunu karşılık maliyeti düşük bir ağ yapısıdır.



Doğrusal veya BUS Yapı

Halka Yapı (Ring Topology)

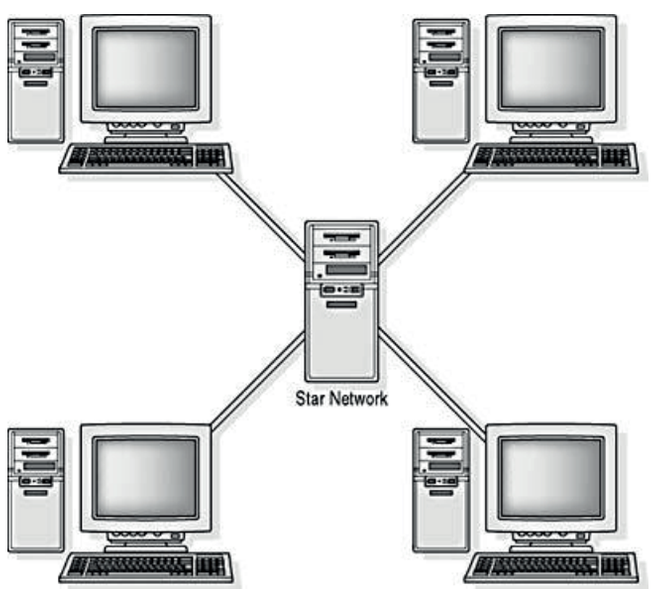
Halka yapıda ise sunucu ve diğer bağlantılı cihazlar bir dairenin kenarlarında yer alırlar. Bütün bilgi ve iletiler bu daire üzerinden gider.



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

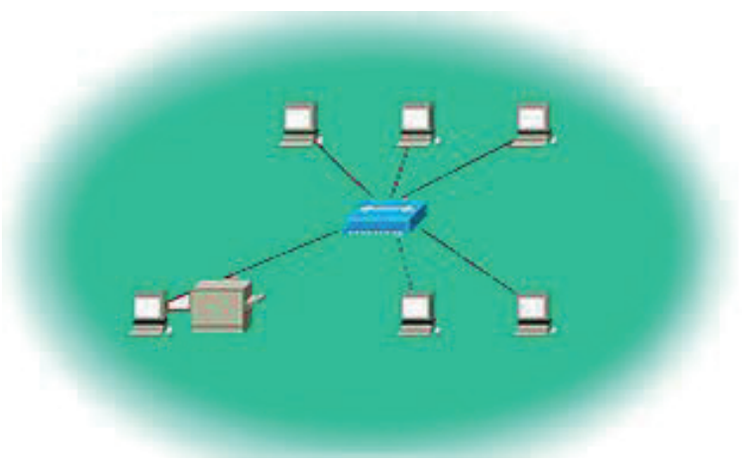
Bilgisayar ağ yapı çeşitlerini gördük. Bu ağ yapı çeşitlerine uyumlu olarak bilgisayar ağ çeşitleri bulunmaktadır. Bu ağlar:

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

Yerel Ağlar (Local Area Networks - LAN)

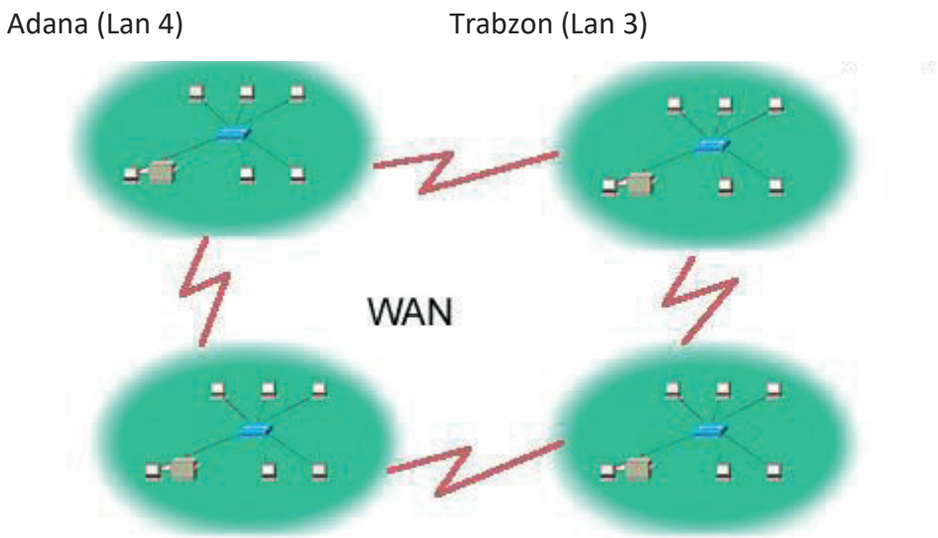
Bir sunucuya belirli bir uzaklıkla bağlanan gerek doğrusal, gerek halka ve gerekse yıldız yapıya sahip, mekân olarak küçük alanı kaplayan ağlara yerel ağlar denir.

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.



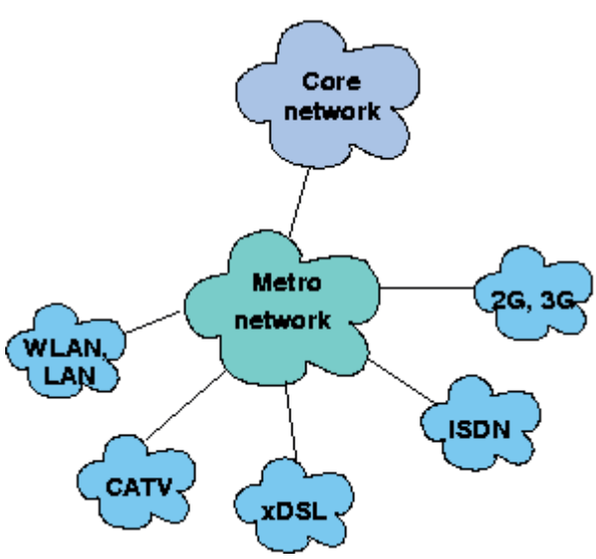
Geniş Alan Ağları (Wide Area Networks - WAN)

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

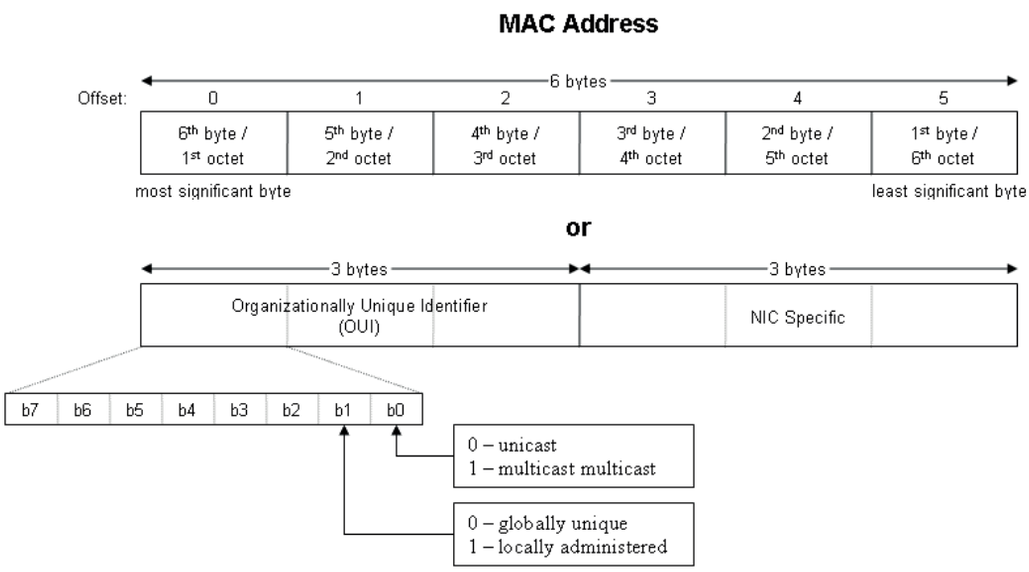
(straight) kablolama yapılır. Düz kablolamada kablonun her iki ucu da 568-A veya 568-B standardında göre bağlanır.

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:

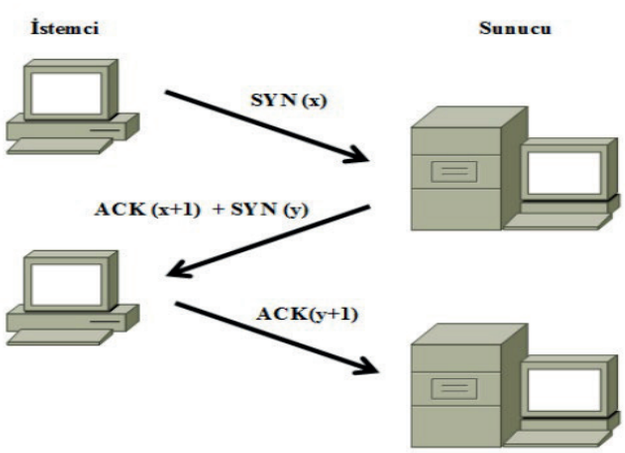
- Temel Veri Aktarımı(Basic Data Transfer)
- Güvenilirlik (Reliability)
- Uçtan uca Akış Kontrolü (End to end flow control)
- Çoğullama (Multiplexing)
- Bağlantılar (connections)
- Tam çift yönlü işlem (full duplex process)

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.

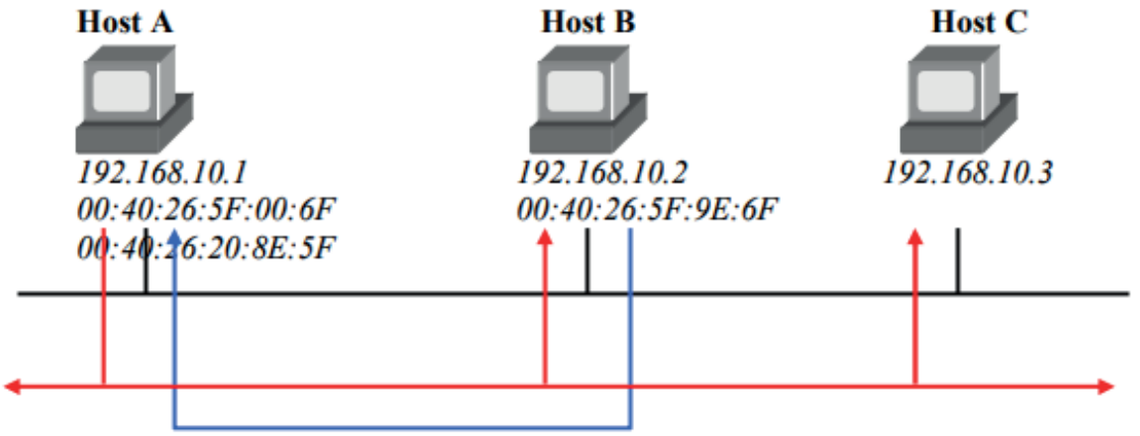
DHCP (Dynamic Host Configuration Protocol)

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

6. 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

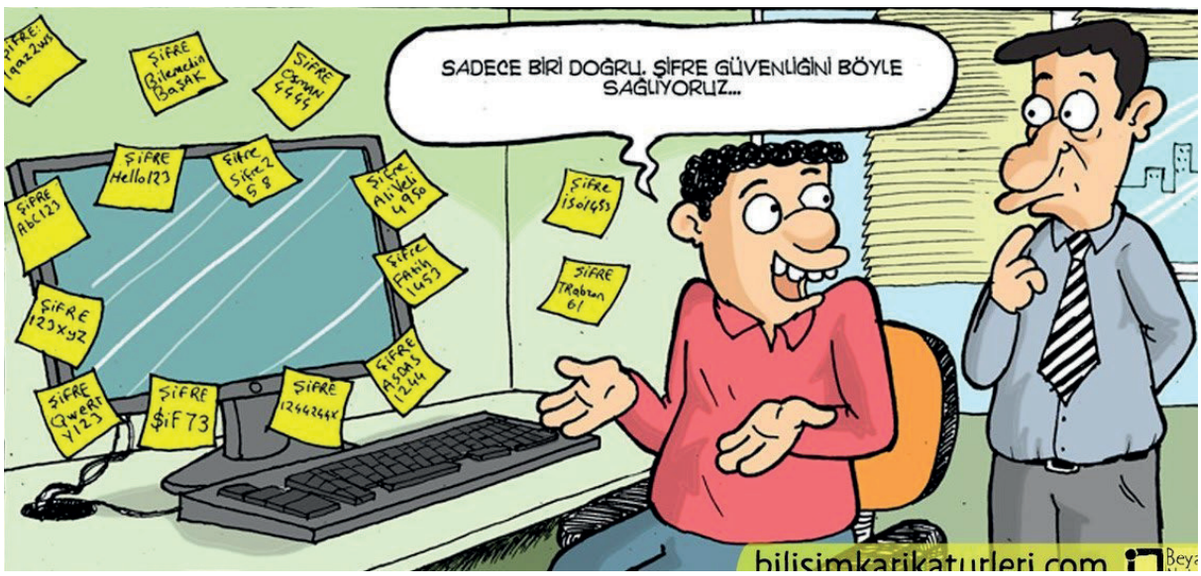
Siber tehditler denince akla ilk gelen tehdit aktörlerin dijitale dayalı olması, tehditlerin dış dünyada da var olduğu gerçeğinin göz ardı edilmesine yol açmaktadır.

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 e-mailin 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 çeşididir. 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.

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?

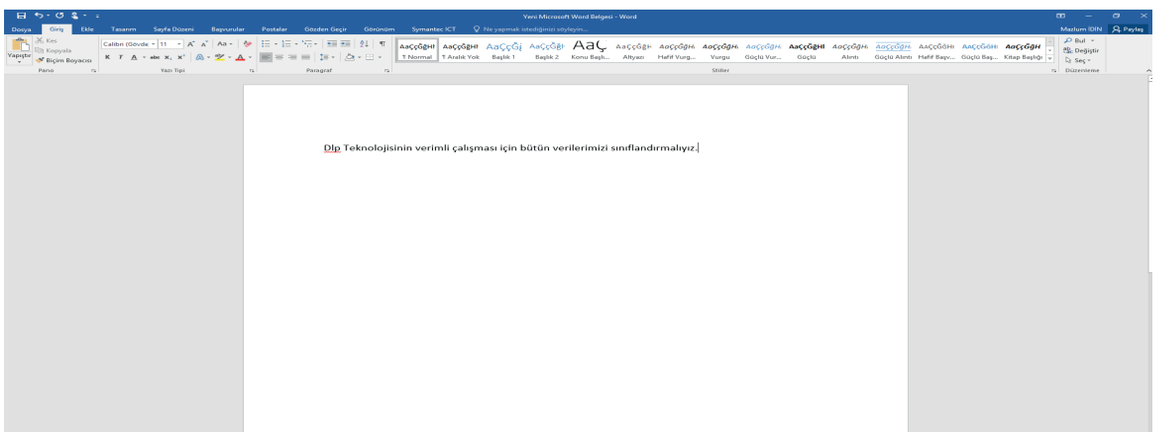
Güvenlik endüstrisindeki bakış farklılıklarına göre "veri sızıntısı önleme", "veri kaybı önleme", "veri kaçağı önleme", "veri sızıntısı engelleme", "veri kaybı engelleme" veya "veri kaçağı engelleme" olarak isimlendirilebilen **DLP (Data Loss Prevention)**, hassas verilerin bir ağ içinde yetkisiz olarak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

DLP KULLANIMI

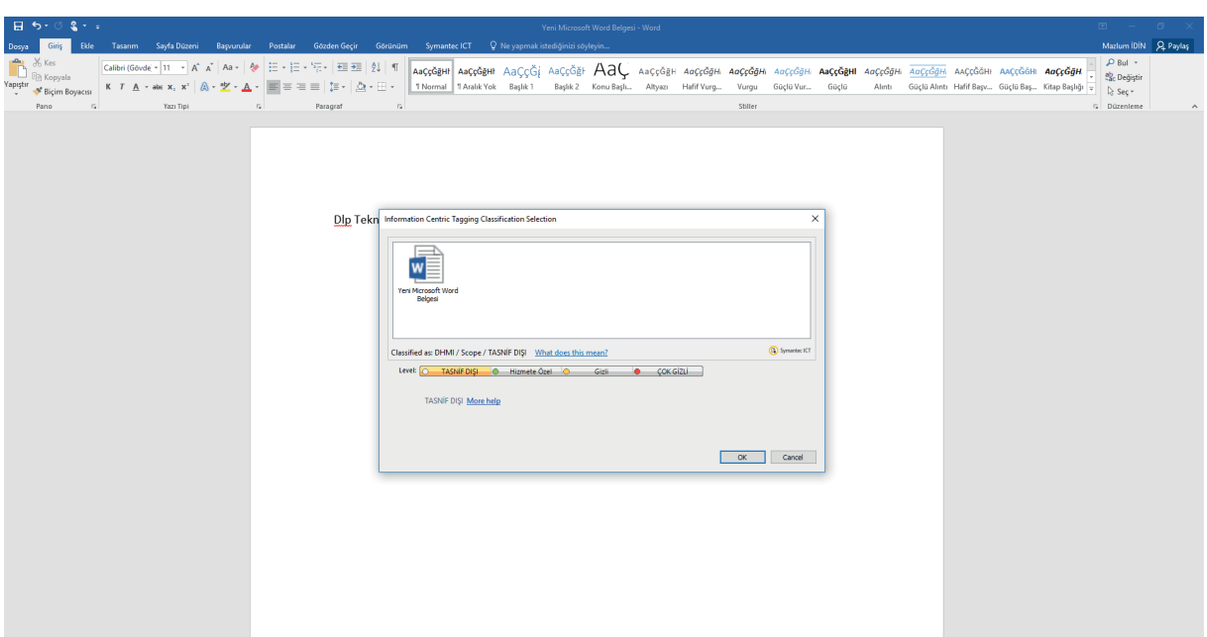
Kuruluşumuzda personelin DLP kullanımı ile yapması gerekenler:

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.

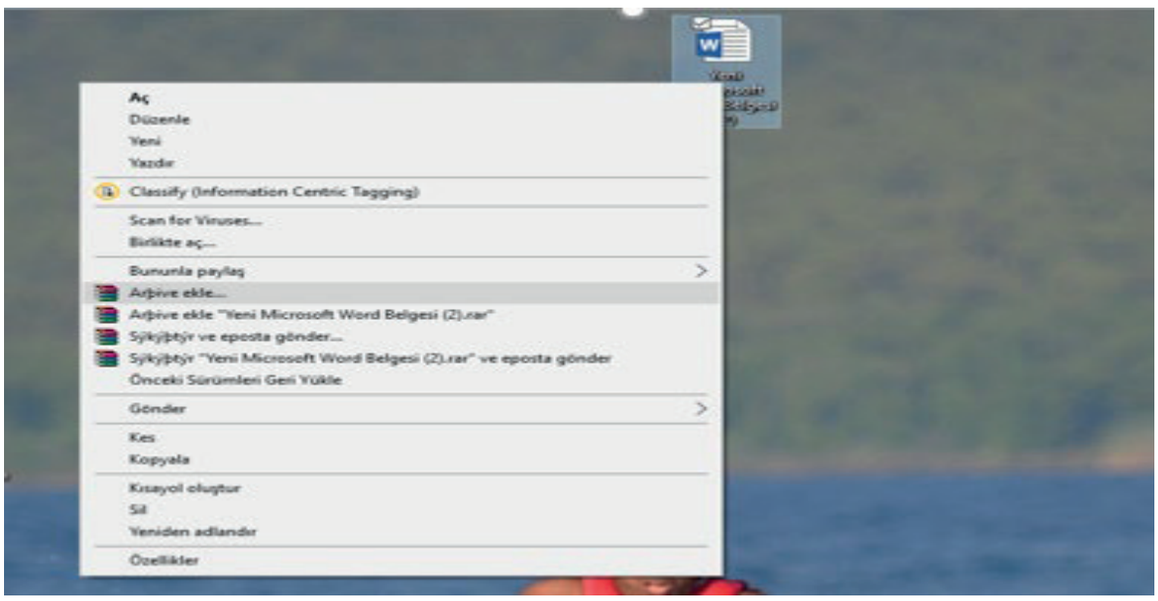
Örneğin yeni bir word dosyası oluşturalım.



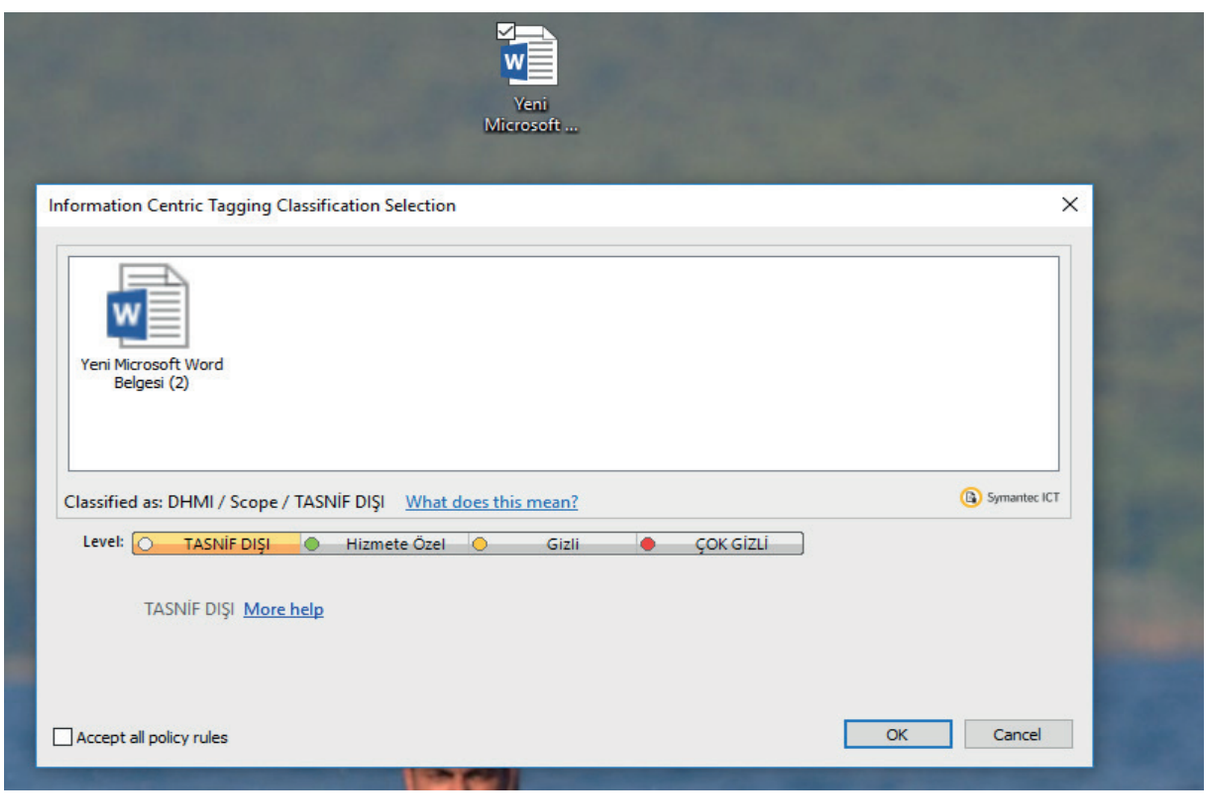
ICT programı yüklü olan bilgisayarlarda bu word belgesi kaydedilmeye çalışıldığında Aşağıdaki ekran görüntüsünde olduğu gibi bir mesaj ile sistem bu belgenin sınıflandırılmasını zorunlu tutacak ve Level kısmında bulunan Tasnif Dışı, Hizmete Özel, Gizli ve Çok Gizli olan kısımlardan biri seçilip belge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

7. BİLGİ GÜVENLİĞİ VE RİSK YÖNETİMİ

KURUMSAL VERİ GÜVENLİĞİ

Kişilerin bilgi güvenliği önem arz ederken, bundan daha önemlisi, kişilerin güvenliğini doğrudan etkileyen kurumsal bilgi güvenliğidir. Her birey bilgi sistemleri üzerinden hizmet alırken veya hizmet sunarken kurumsal bilgi varlıklarını doğrudan veya dolaylı olarak kullanmaktadır. Bu hizmetler kurumsal anlamda bir hizmet alımı olabileceği gibi, bankacılık işlemleri veya bir kurum içerisinde yapılan bireysel işlemler de olabilir. Kurumsal bilgi varlıklarının güvenliği sağlanmadıkça, kişisel güvenlikte sağlanamaz. Bilgiye sürekli olarak erişilebilirliğin sağlandığı bir ortamda, bilginin göndericisinden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlüğünün sağlanması ve güvenli bir şekilde iletilmesi süreci bilgi güvenliği olarak tanımlanabilir.

Kurumsal bilgi güvenliği ise, kurumların bilgi varlıklarının tespit edilerek zafiyetlerinin belirlenmesi ve istenmeyen tehdit ve tehlikelerden korunması amacıyla gerekli güvenlik analizlerinin yapılarak önlemlerinin alınması olarak düşünülebilir. Kurumsal bilgi güvenliği insan faktörü, eğitim, teknoloji gibi birçok faktörün etki ettiği tek bir çatı altında yönetilmesi zorunlu olan karmaşık süreçlerden oluşmaktadır. Bu süreçlerin yönetilmesi, güvenlik sistemlerinin uluslararası standartlarda yapılandırılması ve yüksek seviyede bilgi güvenliğinin sağlanması amacıyla tüm dünyada kurumsal bilgi güvenliğinin yönetiminde standartlaşma çalışmaları hızla sürmektedir. Standartlaşma konusuna önderlik eden İngiltere tarafından geliştirilen BS–7799 standardı, ISO tarafından kabul görerek önce ISO–17799 sonrasında ise ISO–27001:2005 adıyla dünya genelinde bilgi güvenliği standardı olarak kabul edilmiştir. (ISO/IEC 27001, 2007)

Ülkemizde Avrupa Birliği Uyum Kriterlerinde de adı geçen bu standartların uygulanması konusunda yapılan çalışmalar yetersiz olup bu standardı uygulayan kurum ve kuruluşların sayısı yok denecek kadar azdır. ISO–27001:2005 standardı ülkemizde Türk Standartları Enstitüsü (TSE) tarafından TS ISO/IEC 27001 “Bilgi Güvenliği Yönetim Sistemi” standardı adı altında yayınlanmış ve belgeleme çalışmaları başlatılmıştır. Bu standart kapsamında kurumsal bilgi varlıklarının güvenliğinin istenilen düzeyde sağlanabilmesi amacıyla; gizlilik, bütünlük ve erişilebilirlik gibi güvenlik unsurlarının kurumlar tarafından sağlanması gerekmektedir. Bilgi Güvenliği Yönetim Sistemleri (BGYS); insanları, süreçleri ve bilgi sistemlerini içine alan ve üst yönetim tarafından desteklenen bir yönetim sistemidir. Kurumlar açısından önemli bilgilerin

ve bilgi sistemlerinin korunabilmesi, risklerin en aza indirilmesi ve sürekliliğinin sağlanması, BGYS'nin kurumlarda hayata geçirilmesiyle mümkün olmaktadır. BGYS'nin kurulmasıyla; olası risk ve tehditlerin tespit edilmesi, güvenlik politikalarının oluşturulması, denetimlerin ve uygulamaların kontrolü, uygun yöntemlerin geliştirilmesi, örgütsel yapılar kurulması ve yazılım/donanım fonksiyonlarının sağlanması gibi bir dizi denetimin birbirini tamamlayacak şekilde gerçekleştirilmesi anlamına gelmektedir. Kurumsal bilgi güvenlik politikalarının oluşturulması, BGYS kapsamının belirlenmesi, risk yönetimi, denetim kontrollerinin seçilmesi, uygulanabilirlik beyannameleri BGYS kurulabilmesi için, yapılması gereken adımlardır.

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

BGYS'nin kapsamı kurumların sahip olduğu bilgi varlıkları ve ihtiyaçları doğrultusunda tespit edilir. Bu kapsam;

- Kurumun sahip olduğu bilgi varlıklarının tamamı,
- Bilgi sistemlerinin bir kısmı (Bilişim sistemleri, kâğıt ortamdaki bilgiler, elektronik bilgi varlıkları, vb.),
- Belli bir yerleşim birimindeki bilgi sistemleri (Merkez binalar, Genel Müdürlükler, vb.),
- Odaklanılmış bir bilgi sistemi (bilgisayarlar, ağ sistemi, sunucu bilgisayarlar, web sunucusu, vb.) olabilir.

Bir kuruluşta elektronik ortamlarda üretilen, dağıtılan ve saklanan bilgiler BGYS kapsamına örnek olarak verilebilir.

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. 2022 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

Bilgi güvenliği için yönetimin yönlendirilmesi ve desteğinin sağlanmasının yer aldığı bölümdür. 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.

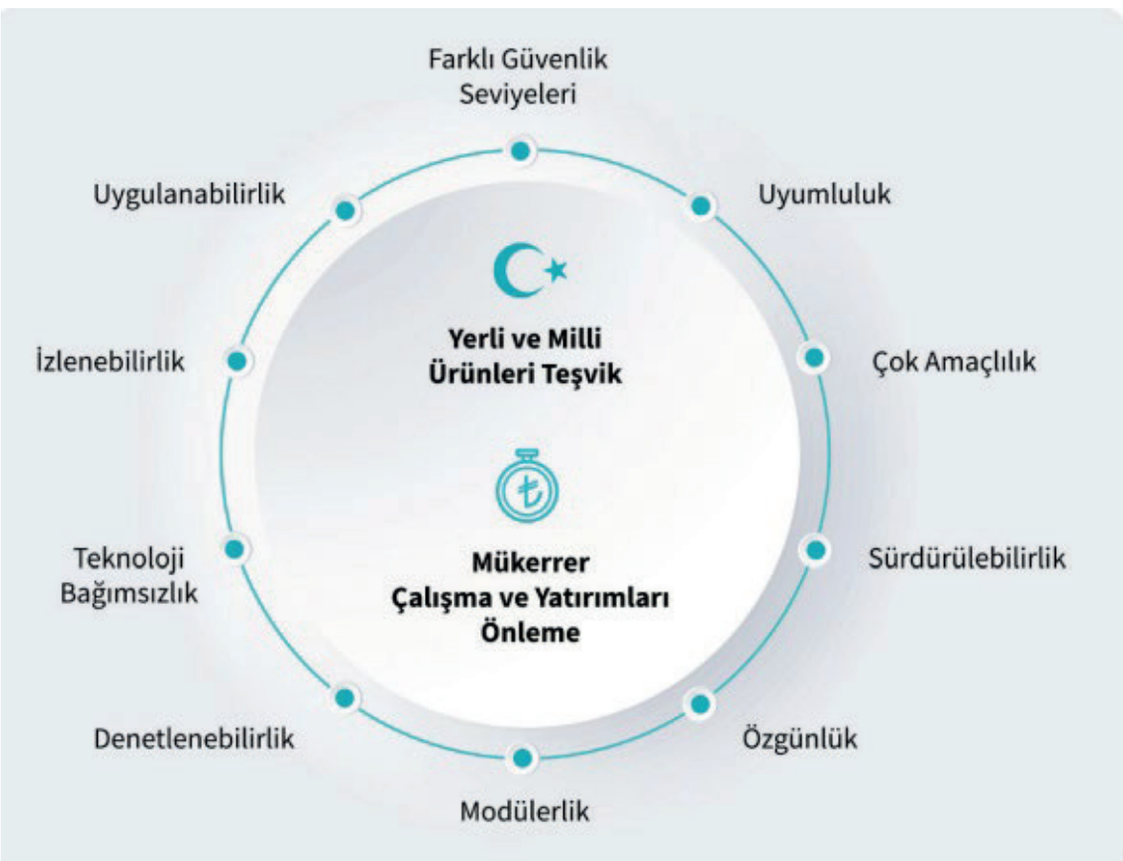
3.2. Örnek Risk Tablosu

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

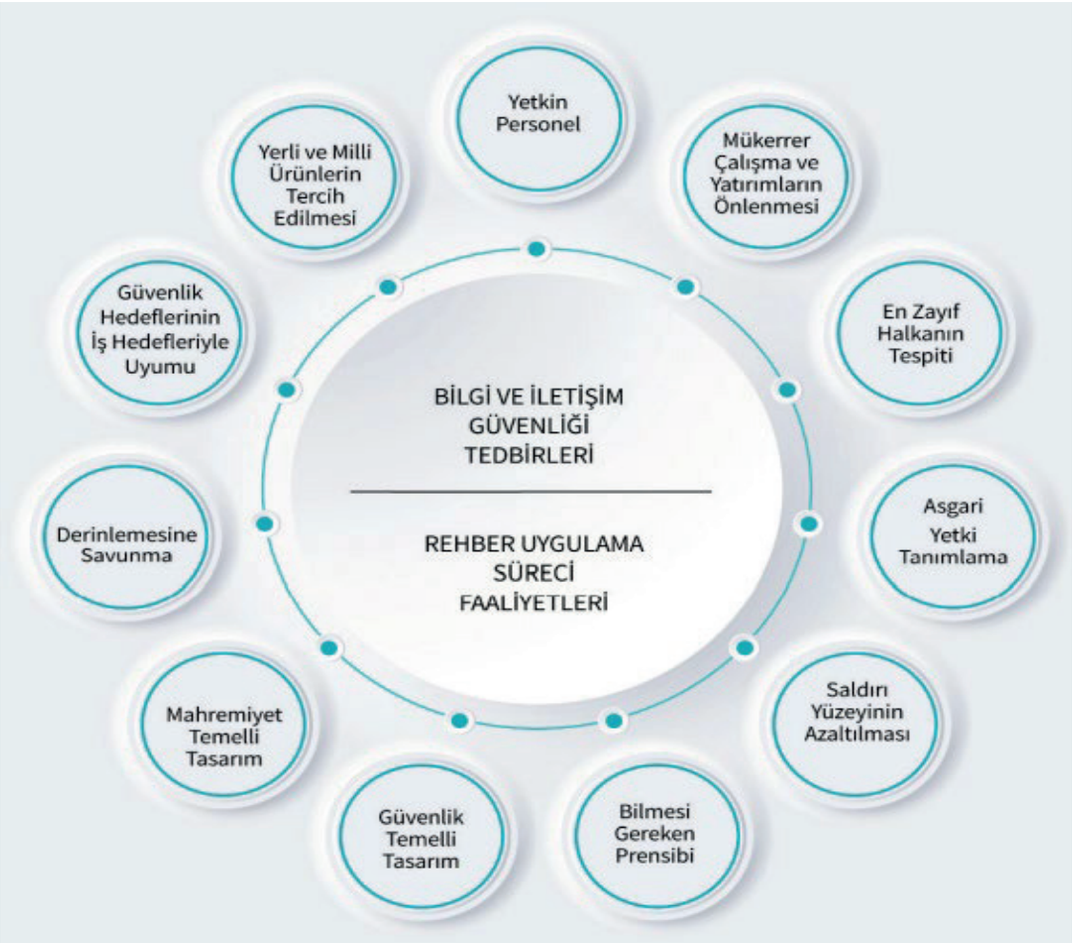
Kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmelerin bilgi ve iletişim güvenliği kapsamında genel olarak alması gereken tedbirleri belirlemek için 06.07.2019 tarih ve 30823 sayılı Resmi Gazete'de Bilgi ve İletişim Güvenliği Tedbirleri konulu 2019/12 sayılı Cumhurbaşkanlığı 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.

BGYS Süreçleri;

Aşama 1: ISO/IEC 27001:2017 standardının tüm gereklerinin yerine getirilmesi ve standartta belirtilen yönetim iskelet yapısının oluşturulması.

Aşama 2: Uyumluluk denetimleri için yetkilendirilmiş sertifikalandırma kurumuna ön başvuru yapılır. Bu başvuruya istinaden denetimi yapacak firma belgelendirme için maliyet ve zaman çizelgesi sunar.

Aşama 3: Maliyet ve zaman çizelgesi kurum tarafından onaylanarak denetimi gerçekleştirecek firmaya resmi başvuru yapılır.

Aşama 4: Denetimi gerçekleştirecek olan kurum güvenlik politikasını, risk değerlendirmesi dokümanlarını, risk eylem planını, uygunluk beyanını (SOA) ve güvenlik prosedürlerini içeren dokümantasyonu gözden geçirir. Bu işlem sonucunda, bilgi güvenliği yönetim sistemindeki sorunlu olan ve çözüme kavuşturulması gereken herhangi bir zayıflığın veya göz ardı edilen bir hususun ortaya çıkarılması hedeflenir.

Aşama 5: Masaüstü kontrolü başarılı şekilde sonuçlandıktan sonra, denetim firmasının belirlediği denetçiler tarafından yerinde denetim gerçekleştirilir. Kuruluşun büyüklüğüne ve iş tipine uygun kontrollerin olup olmadığı gözden geçirilir ve elde edilen sonuçlara göre kurumlara önerilerde bulunulur.

Aşama 6: Değerlendirmenin başarı ile tamamlanmasının ardından, Bilgi Güvenliği Yönetim Sisteminin kapsamını açık bir şekilde tanımlayan bir sertifika verilecektir. Bu sertifika 3 yıl boyunca geçerliliğini korur ve yıllık yapılan ara denetimler ile desteklenir. ISO/IEC 27001 standardına göre kurulmuş olan bir bilgi güvenliği yönetim sistemi ile, kurumların bilgi güvenliği yönetiminde, kapsamlı prosedürler aracılığıyla güvenlik kontrollerini sürekli ve düzenli olarak işletmeyi ve sistemin sürekli iyileştirilmesi gerçekleştirilmektedir. Güven ve güvenilirliğin hayati önem taşıdığı alanlarda hizmet veren kuruluşların, uluslararası geçerlilikte bilgi güvenliği yönetim sistemleri standardına uygunluk belgesine sahip olması, hem mevzuat hem de kuruluşun güvenli işleyişi açısından bir zorunluluk olarak değerlendirilmektedir.

Kuruluşumuzda ise Genel Müdürlüğümüz dâhilinde ISO/IEC 27001:2017 sertifikası 25.12.2018 tarihinden itibaren bulunmakta ve sürdürülmektedir.

5. SÜRDÜR

İşletme içindeki bilgi güvenliğinin yönetilmesi, üçüncü taraflarca erişilen işletmeye ait bilgi işleme araçlarının ve bilgi varlıklarının güvenliğinin korunması ve bilgi işleme sorumluluğu başka bir işletmenin kaynaklarından sağlandığında bilgi güvenliğinin sürdürülmesidir.

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

BGYS'nin iyileştirilmesi için kurum tarafından önleyici ve düzeltici tedbirler alınması gereklidir. Olumsuzlukların yaşanmaması için, risk değerlendirme sonuçlarına bağlı olarak değişen riskler bazında önleyici tedbirler alınmalıdır. Gerçekleştirilen önleyici faaliyetler, olası sorunların yapacağı etkiye uygun olmalıdır. BGYS gereksinimleriyle olumsuzlukları gidermek üzere düzeltici önlemler alınmalıdır. Önleyici tedbirler için gerçekleştirilen faaliyetler çoğunlukla düzenleyici tedbirler için gerçekleştirilen faaliyetlerden daha az maliyetlidir.

Kurumların ISO/IEC 27001 Sertifikası Alınmasının Avantajları

Kredilendirilebilirlik, güven ve itimat: Belgelendirme, kurum veya kuruluşun bilgi güvenliğini dikkate aldığını, bilgi güvenliğinin sağlanması için gerekli olan adımları uyguladığını ve kontrol ettiğini ispatlamaktadır. Bu sayede kurumlar veya kuruluşlar birlikte iş yaptıkları veya hizmet verdikleri kurum veya bireylerin tüm bilgilerinin BGYS sayesinde güvende tutulacağı konusunda verdikleri taahhütten dolayı iş yaptıkları kurum, kuruluş veya bireylerin kendilerini güvende hissetmelerini sağlayacaklardır. Belgelendirme sonucunda özellikle özel sektör firmalarında rekabet anlamında sertifika almamış rakiplerinin bir adım önüne geçerek avantaj sağlayacaklardır. Ayrıca günümüzde uluslararası yapılan işlerde ISO/IEC 27001 şartı koşulmaktadır.

Tasarruf: Oluşabilecek güvenlik ihlallerine karşı kontrollerin uygulanması ile maliyetler düşmektedir. Sadece bir bilgi güvenliği ihlalinin oluşturacağı zarar bile çoğu zaman çok büyük maddi kayıplara yol açabilir. Belgelendirme işlemi kurumların maruz kalacağı bu tür ihlalleri azaltarak bilgi güvenliği ihlallerinden doğan zararları en aza indirecektir.

Yasal Uygunluk: Belgelendirme işlemi, kanun ve tüzüklere uygunluğun yetkili ve ilgili makamlara yasal anlamda uygunluğun sağlandığına dair kanıt teşkil edilmesine yardımcı olur.

Taahhüt: Belgelendirme işlemi, organizasyonun tüm aşamalarında taahhüt/bağlılığın sağlanması ve kanıtlanmasında yardımcı olur.

Operasyonel Seviye Risk Yönetimi: Kuruluş genelinde, bilgi sistemleri ve zayıflıklarının nasıl korunacağı konusundaki farkındalık artar. Ayrıca donanım ve veriye daha güvenli bir şekilde erişim sağlanır.

Çalışanlar: Çalışanların kuruluş içerisindeki sorumlulukları ve bilgi güvenliği konularındaki bilinçlerinin artmasını sağlar.

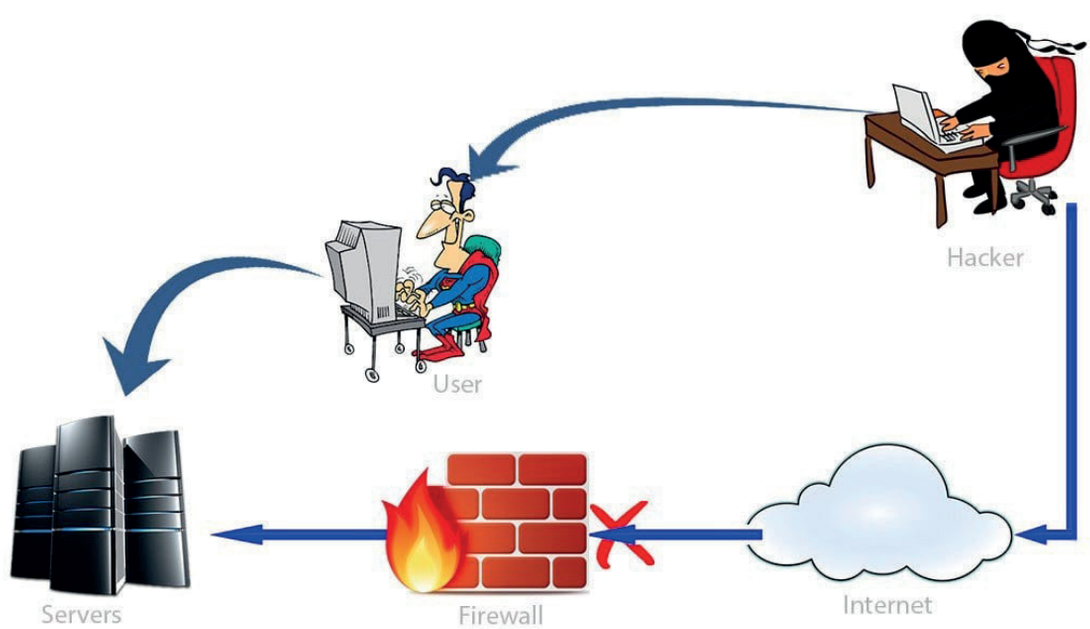
Sürekli İyileşme: Düzenli olarak gerçekleştirilen denetimlere bağlı olarak bilgi sistemlerinin etkinliği izlenecek ve izleme sonucunda tespit edilen problemler giderilerek bilgi sistemlerinde genel anlamda bir iyileşme sağlanabilecektir.

Onay: Organizasyon için tüm seviyelerde bilgi güvenliği varlığının bağımsız kuruluşlar tarafından onaylandığını göstermektedir.

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.

Çalışanların Eğitilmesi ve Farkındalık Çalışmaları

Kurumsal ve Kişisel verilerin güvenliği açısından en çok beklenen önlemlerden biri çalışanların eğitimidir ve çalışanların eğitimine ilişkin aşağıdaki hususların uygulanmasını beklenir:

- Çalışanların, kişisel verilerin hukuka aykırı olarak açıklanmaması ve paylaşılmaması gibi konular hakkında eğitim almaları Çalışanlara yönelik farkındalık çalışmalarının yapılması
- Güvenlik risklerinin belirlenebildiği bir ortam oluşturulması
- Hangi konumda çalıştıklarına bakılmaksızın çalışanların veri güvenliğine ilişkin rol ve sorumluluklarının görev tanımlarında belirlenmesi ve çalışanların bu konudaki rol ve sorumluluklarının farkında olması
- Çalışanların güvenlik politika ve prosedürlerine uymaması durumunda devreye girecek bir disiplin süreci oluşturulması

- Veri güvenliğine ilişkin politika ve prosedürlerde önemli değişikliklerin meydana gelmesi halinde; ilgili yeni eğitimlerin yapılması
- Veri güvenliğine ilişkin bilgilerin güncel tutulmasının sağlanması.

Ayrıca çalışanların işe alınma süreçlerinin bir parçası olarak gizlilik anlaşması imzalamalarının istenebilmektedir. Son olarak, veri güvenliğine ilişkin kültür oluşturulurken "Yasaklanmadıkça Her Şey Serbesttir" prensibinin değil "İzin Vermedikçe Her Şey Yasaktır" prensibine uygun hareket edilmesi gerekir.

VERİ GÜVENLİĞİNE İLİŞKİN TEKNİK VE İDARİ TEDBİRLER

Siber Güvenliğin Sağlanması

Veri güvenliğinin sağlanması için tek bir siber güvenlik ürünü kullanımı ile tam güvenlik sağlanamayabileceğini belirterek, birçok prensip dahilinde tamamlayıcı niteliğe sahip ve düzenli olarak kontrol edilen birtakım tedbirlerin uygulanması önerilmektedir. Siber güvenliğin sağlanması için gerekli olan önlemler;

- Öncelikle güvenlik duvarı ve ağ geçidinin sağlanması
- Hemen hemen her yazılımın ve donanımın kurulum ve yapılandırma işlemlerine tabi tutulması
- Yama yönetimi ve yazılım güncellemelerinin yapılması
- Yazılım ve donanımların düzgün bir şekilde çalışıp çalışmadığının ve sistemler için alınan güvenlik tedbirlerinin yeterli olup olmadığının düzenli kontrolü
- Çalışanlara, yapmakta oldukları iş ve görevler ile yetki ve sorumlulukları için gerekli olduğu ölçüde erişim yetkisinin tanınması
- Sistemlere kullanıcı adı ve şifre kullanmak suretiyle erişim sağlanması
- Şifre ve parolalar oluşturulurken kişisel bilgilerle ilişkili ve kolay tahmin edilecek rakam ya da harf dizileri yerine büyük küçük harf, rakam ve sembollerden oluşacak kombinasyonların tercih edilmesinin sağlanması
- Şifre girişi deneme sayısının sınırlandırılması
- Düzenli aralıklarla şifre ve parolaların değiştirilmesinin sağlanması
- Yönetici hesabı ve admin yetkisinin sadece ihtiyaç olduğu durumlarda kullanılması için açılması
- Veri sorumlusuyla ilişkileri kesilen çalışanlar için zaman kaybetmeksizin hesabın silinmesi ya da girişlerin kapatılması

- Bilgi sistem ağını düzenli olarak tarayan ve tehlikeleri tespit eden antivirüs, antispam gibi ürünlerin kullanılması, güncel tutulması ve gereken dosyaların düzenli olarak tarandığından emin olunması
- Farklı İnternet siteleri ve/veya mobil uygulama kanallarından kişisel veri temin edilecekse, bağlantıların SSL ya da daha güvenli bir yol ile gerçekleştirilmesi.

Bunlara ek olarak, yaygın şekilde kullanılan bazı yazılımların özellikle eski sürümlerinin belgelenmiş güvenlik açıkları bulunduğunu vurgulayarak, kullanılmayan yazılım ve servislerin güncel tutulması yerine cihazlardan kaldırılması ve silinmesi önerilmektedir.

Ayrıca, veri sorumlularının erişim yetki ve kontrol matrisi oluşturmasını ve ayrı bir erişim politika ve prosedürleri oluşturularak veri sorumlusu organizasyonu içinde bu politika ve prosedürlerin uygulamaya alınması da gerekli bir önlemdir.

Veri Güvenliğinin Takibi

Verilerin bulunduğu sistemlere olan saldırıların uzun süre fark edilemediği ve müdahale için geç kalınabildiği durumlara işaret ederek, bu durumun önlenmesi için aşağıdaki eylemlerin alınması gerektiği belirtilir:

- Bilişim ağlarında hangi yazılım ve servislerin çalıştığının kontrol edilmesi
- Bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığının belirlenmesi
- Tüm kullanıcıların işlem hareketleri kaydının düzenli olarak tutulması (Log kaydının tutulması gibi)
- Güvenlik sorunlarının mümkün olduğunca hızlı bir şekilde raporlanması
- Çalışanların sistem ve servislerindeki güvenlik zafiyetlerini ya da bunları kullanan tehditleri bildirmesi için resmi bir raporlama prosedürünün oluşturulması
- Raporlama sürecinde oluşturulacak raporların otomatik olması halinde, raporların sistem yöneticisi tarafından en kısa sürede toplulaştırılarak veri sorumlusuna sunulması
- Güvenlik yazılımı mesajlarının, erişim kontrolü kayıtlarının ve diğer raporlama araçlarının düzenli olarak kontrol edilmesi
- Sistemlerden gelen uyarılar üzerine harekete geçilmesi
- Bilişim sistemlerinin bilinen zafiyetlere karşı korunması için düzenli olarak zafiyet taramaları ve sızma testlerinin yapılması
- Ortaya çıkan güvenlik açıklarına dair testlerin sonucuna göre değerlendirmeler yapılması

- Bilişim sisteminin çökmesi, kötü niyetli yazılım, servis dışı bırakma saldırısı, eksik veya hatalı veri girişi, gizlilik ve bütünlüğü bozan ihlaller, bilişim sisteminin kötüye kullanılması gibi istenmeyen olaylarda delillerin toplanması ve güvenli bir şekilde saklanması

Verilerin Bulutta Depolanması

Veri sorumluları tarafından bulut sistemlerinde veri güvenliğinin sağlanması için yapılması gerekenler:

- Bulut depolama hizmeti sağlayıcısı tarafından alınan güvenlik önlemlerinin de yeterli ve uygun olup olmadığının değerlendirilmesi
- Bulutta depolanan verilerin neler olduğunun detaylıca bilinmesi
- İlgili verilerin yedeklenmesi
- İlgili verilerin senkronizasyonunun sağlanması
- İlgili verilere gerektiği hallerde uzaktan erişilebilmesi için iki kademeli kimlik doğrulama kontrolünün uygulanması.

Bunlara ek olarak, Kurum'un, daha önce Varlık İmha Prosedüründe de bahsettiği gibi, bulut sistemlerinde yer alan verilerin gerektiğinde imhasının sağlanabilmesi için bu verilerin depolanması ve kullanımı sırasında kriptografik yöntemlerle şifrelenmesi, bulut ortamlarına şifrelenerek atılması ve veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarlarının kullanılması gerekir. Böylece hizmet ilişkisi sona erdiğinde, şifreleme anahtarlarının tamamı yok edilerek bulut sistemlerinde yer alan kişisel verilerin imhası sağlanabilecektir.

İŞ SÜREKLİLİĞİ

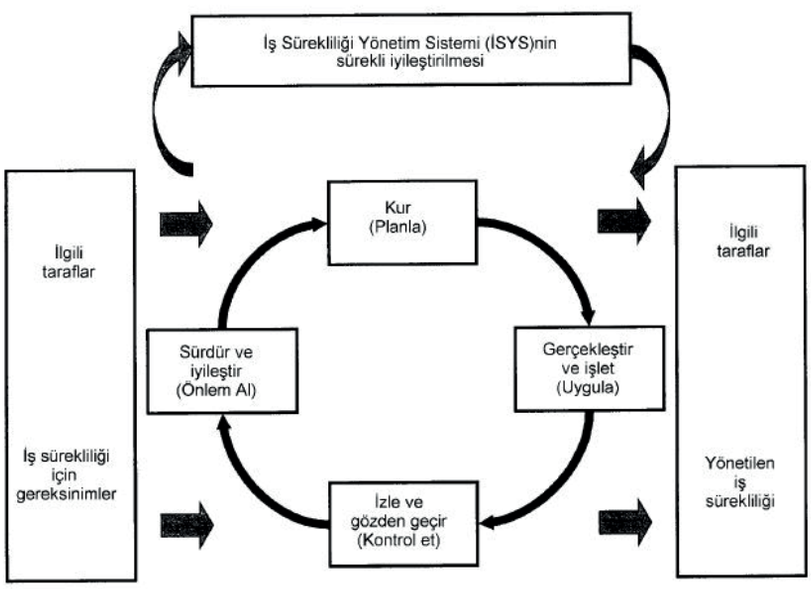
Kuruluş tarafından verilen hizmetlerin kesintisiz devam etmesi ve herhangi bir kesinti durumunda tanımlanan sürelerde tekrar hizmet vermeye devam edebilmesinin sağlanması becerisidir. İş sürekliliğini kesintiye uğratan nedenler;

- Yangın
- Kuruluş itibarına yönelik saldırı
- Doğal Afet
- Tedarik Zinciri Kesintisi
- Enerji, İletişim ya da 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.

Kişisel Veri Güvenliğine İlişkin Teknik ve İdari Tedbirler

Öncelikle alınması gereken teknik ve idari tedbirleri genel başlıklar halinde sıralanabilir. Kurul'un buna ilişkin belirttiği özet tedbirler;

Teknik Tedbirler;

- Yetki Matrisi
- Yetki Kontrol

- Erişim Logları
- Kullanıcı Hesap Yönetimi
- Ağ Güvenliği
- Uygulama Güvenliği
- Şifreleme
- Sızma Testi
- Saldırı Tespit ve Önleme Sistemleri
- Log Kayıtları
- Veri Maskeleme
- Veri Kaybı Önleme Yazılımları
- Yedekleme
- Güvenlik Duvarları
- Güncel Anti-Virüs Sistemleri
- Silme, Yok Etme veya Anonim Hale Getirme
- Anahtar Yönetimi

İdari Tedbirler

- Kişisel Veri İşleme Envanteri Hazırlanması
- Kurumsal Politikalar (Erişim, Bilgi Güvenliği, Kullanım, Saklama ve İmha vb.)
- Sözleşmeler (Veri Sorumlusu – Veri Sorumlusu, Veri Sorumlusu – Veri İşleyen Arasında)
- Gizlilik Taahhütnameleri
- Kurum İçi Periyodik ve/veya Rastgele Denetimler
- Risk Analizleri
- İş Sözleşmesi, Disiplin Yönetmeliği (Kanun'a Uygun Hükümler İlave Edilmesi)
- Kurumsal İletişim (Kriz Yönetimi, Kurul ve İlgili Kişiyi Bilgilendirme Süreçleri, İtibar Yönetimi
- Eğitim ve Farkındalık Faaliyetleri (Bilgi Güvenliği ve Kanun)
- Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) Bildirim

Kişisel Veri İhlaline İlişkin Sonuçlar

Kurum'un ve Kurum'a bağlı olan Kişisel Verileri Koruma Kurulu'nun Kanun'un kişisel veri güvenliğine ilişkin 12. maddesi çerçevesindeki yükümlülüklere uyumu denetlerken göz önüne alacağı kriterlerdir.

Kanun'da veri güvenliğine ilişkin yükümlülüklerin ihlali halinde yükümlülükleri yerine getirmeyenler hakkında **15.000 Türk Lirasından 1.000.000 Türk Lirasına** kadar idari para cezası verilebileceği unutulmamalıdır.

Bu bağlamda veri sorumluları, bilgi güvenliğinden sorumlu çalışanları veya teknik uzmanlar ve hukukçuları yardımıyla yukarıda belirtilen unsurları sağlamak adına harekete geçmelidir.

Buna ek olarak, kendileri adına veri işleyenlerle imzalanacak sözleşmelerin hazırlanması, çalışanlarının eğitilmesi ve tüm çalışanlarının uyması gereken güvenlik önlemlerinin belirlenmesi, bunlara ilişkin taahhütlerin hazırlanması, denetim şartlarının belirlenmesi gibi kişisel veri güvenliğine ilişkin idari tedbirlerin de uygulanmasına mümkün olduğunca hızlı bir şekilde başlanmasını öneriyorum. Hali hazırda veri envanterlerini hazırlamış ve politikalarına dair ön çalışmalarını yapmış olan veri sorumlularının, var olan politika ve uygulamalarını yukarıda anlatılanlar çerçevesinde yeniden gözden geçirmesi yararlı olacaktır.

Ek Bilgi: 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.