SPL
Sermaye Piyasası
Lisanslama Sicil ve
Eğitim Kuruluşu

Lisanslama Sınavları
Çalışma Notları

Bilgi Sistemleri Güvenliği

2023

Bilgi Sistemleri Bağımsız Denetim Sınavı

Hazırlayanlar:
Sermaye Piyasası Kurulu Uzmanları


SPL
Sermaye Piyasası
Lisanslama Sicil ve
Eğitim Kuruluşu

Sermaye Piyasası
Lisanslama Sicil ve
Eğitim Kuruluşu

Bilgi Sistemleri Güvenliği

Ders Kodu: 1023

- Bilgi Sistemleri Bağımsız Denetim Sınavı

31 Aralık 2024

Bu çalışma notu Sermaye Piyasası Kurulu uzmanları tarafından hazırlanmıştır.

SINAV ALT KONU BAŞLIKLARI
BİLGİ SİSTEMLERİ GÜVENLİĞİ

1. Bilgi Güvenliği Yönetimi
2. Varlık Yönetimi
3. Fiziksel ve Çevresel Güvenlik
4. Ağ Güvenliği
5. Erişim Güvenliği
6. Veri ve İz Kayıtlarının Güvenliği
7. Üçüncü Taraflarla İletişim Güvenliği

İÇİNDEKİLER

KISALTMALAR

AFRINIC : African Network Information Centre
ANSI :American National Standards Institute (Amerikan Ulusal Standartlar Enstitüsü)
APNIC : Asia Pacific Network Information Centre
ARIN : American Registry for Internet Numbers
ARPANET : The Advanced Research Projects Agency Network (Gelişmiş Araştırma Projeleri Dairesi Ağı)
ATM : Asynchrous Transfer Mode
BDDK : Bankacılık Düzenleme ve Denetleme Kurumu
BGP : Border Gateway Protocol (Sınır Geçit Protokolü)
BSBDL : Bilgi Sistemleri Bağımsız Denetim Lisansı
BSBD Tebliği : III-62.2 sayılı Bilgi Sistemleri Bağımsız Denetim Tebliği
BSSID : Basic Service Set Identifier (Bağımsız Temel Hizmet Takımı Tanımlayıcısı)
BSY Tebliği : VII-128.9 sayılı Bilgi Sistemleri Yönetimi Tebliği
BT : Bilgi Teknolojileri
BYOD : Bring Your Own Device (Kendi Cihazını Getir)
CA : Certification Authority (Sertifika Otoritesi)
CAN : Campus Area Network (Kampüs Alan Ağı)
CER : Crossover Error Rate (Çapraz Hata Oranı)
CISA : Certified Information Systems Auditor (Bilgi Sistemleri Denetçisi Sertifikası)
COBIT :Control Objectives for Information and Related Technologies (Bilgi Teknolojilerine İlişkin Kontrol Hedefleri)
COBO : Corporate-Owned, Business-Only (Şirkete Ait, Yalnızca İş)
COPE : Corporate-Owned, Personally-Enabled (Şirkete Ait, Kişisel Olarak Etkinleştirilmiş)
CRL : Certificate Revocation List (Sertifika İptal Listesi)
CSRF : Cross-Site Request Forgery (Çapraz Site Talep Sahteciliği)
CYOD : Choose Your Own Device (Kendi Cihazını Seç)
DAC : Discretionary Access Control (İsteğe Bağlı Erişim Kontrolü)
DARPA : The Defense Advanced Research Projects Agency (İleri Savunma Araştırma Projeleri Dairesi)
DCE : Distributed Computing Environment (Dağıtık Bilgi İşlem Ortamı)
DDO : Dijital Dönüşüm Ofisi
DES : Data Encryption Standart (Veri Şifreleme Standardı)
DLP : Data Loss Prevention (Veri Sızıntısı Önleme)
DMZ : Demilitarized Zone (Silahsızlanma Alanı / Savunmasız Bölge)
ECC : Elliptical Curve Cryptography (Eliptik Eğri Kriptografisi)
EER : Equal Error Rate (Eşit Hata Oranı)
EMI : Electromagnetic Interference (Elektromanyetik Enterferans)
FAR : False Acceptance Rate (Yanlış Kabul Oranı)
FC : Fiber Channel
FDDI : Fiber Distributed Data Interface (Fiber Dağıtılmış Veri Arayüzü)
FRR : False Rejection Rate (Yanlış Reddetme Oranı)
HTML : Hypertext Markup Language
IAB : Internet Architecture Board (İnternet Mimarisi Kurulu)
IAITAM : International Association of Information Technology Asset Managers (Uluslararası Bilgi Teknolojileri Varlık Yöneticileri Birliği)
ICANN : The Internet Corporation for Assigned Names and Numbers (İnternet Tahsisli

Sayılar ve İsimler Kurumu)
ICMP : The Internet Control Message Protocol (İnternet Kontrol Mesajı Protokolü)
IDS : Intrusion Detection System (Saldırı Tespit Sistemi)
IEEE : The Institute of Electrical and Electronics Engineers (Elektrik ve Elektronik Mühendisleri Enstitüsü)
IETF : Internet Engineering Task Force (İnternet Mühendisliği Görev Gücü)
IGMP : Internet Group Management Protocol (İnternet Grup Yönetim Protokolü)
ISS : İnternet Servis Sağlayıcıları
IoT : Internet of things n(esnelerin İnterneti)
IP : İnternet Protokolü
IPS : Intrusion Prevention System (Saldırı Engelleme Sistemi)
ISA : International Standards on Auditing (Uluslararası Denetim Standartları)
ISACA : Information Systems Audit and Control Association (Bilgi Sistemleri Denetim ve Kontrol Birliği)
ISACF : Information Systems Audit and Control Foundation (Bilgi Sistemleri Denetim ve Kontrol Vakfı)
iSCSI : Internet Small Computer System Interface
ISO : International Organization for Standardization (Uluslararası Standartlar Örgütü)
IT : Information Technologies (Bilgi Teknolojileri)
ITAF : Information Technology Assurance Framework (Bilgi Teknolojileri Güvence Çerçevesi)
ITGI : IT Governance Institute (Bilgi Teknolojileri Yönetişim Enstitüsü)
ITIL : Information Technology Infrastructure Library (Bilgi Teknolojisi Altyapı Kütüphanesi)
ITU : International Telecommunication Union (Uluslararası Telekomünikasyon Birliği)
KGK : Kamu Gözetimi Muhasebe ve Denetim Standartları Kurumu
KPI : Key Performance Indicator (Anahtar Başarı Göstergesi)-
KVKK : Kişisel Verilerin Korunması Kanunu
LACNIC : Latin America and Caribbean Network Information Centre
LAN : Local Area Network (Yerel Alan Ağı)
LDAP : Lightweight Directory Access Protocol (Basit Dizin Erişim Protokolü)
LSO : Local Shared Object (Yerel Paylaşılan Nesneler)
MAC : Mandatory Access Control (Zorunlu Erişim Kontrolü)
MAC Adresi : Media Access Control Address (Ortam Erişim Kontrolü Adresi)
MAN : Metropolitan Area Network (Büyükşehir Alan Ağı)
MEF : Metropolitan Ethernet Forum
MFA : Multi-Factor Authentication (Çok Faktörlü Kimlik Doğrulama)
MIT : Massachusetts Institute of Technology (Massachusetts Teknoloji Enstitüsü)
MLD : Multicast Listener Discovery (Multicast Dinleyici Keşfi)
NAC : Network Access Control (Ağ Erişim Kontrolü)
NFC : Near Field Communication (Yakın Alan İletişimi)
NIC : Network Interface Card
NIST : National Institute of Standards and Technology (Ulusal Standartlar ve Teknoloji Enstitüsü)
NOS : Network Operating System
NTP : Network Time Protocol (Ağ Zaman Protokolü)
OSI : Open Systems Interconnection (Açık Sistemler Bağlantısı)

OWASP : Open Web Application Security Project (Açık Web Uygulama Güvenliği Projesi)
PAN : Personal Area Network (Kişisel Alan Ağı)
PC : Personal Computer (Kişisel Bilgisayar)
PDU : Protocol Data Unit (Protokol Veri Birimi)
PKI : Public Key Infrastructure (Açık Anahtar Altyapısı)
PIN : Personal Identification Number (Kişisel Kimlik Numarası)
RA : Registration Authority (Kayıt Otoritesi)
RIPE NCC : Réseaux IP Européens Network Coordination Centre
RIR : Regional Internet Registry (Bölgesel İnternet Kayıt Kuruluşu)
RPO : Recovery Point Objective (Kurtarma Noktası Hedefi)
RTO : Recovery Time Objective (İyileşme Süresi Hedefi)
SIEM : Security Information and Event Management (Güvenlik Bilgileri ve Olay Yönetimi)
SAN : Storage Area Network (Depolama Alan Ağı)
SLA : Service-Level Agreement (Hizmet Seviyesi Anlaşması)
SMDS : Switched Multi-Megabit Data Service
SMS : Short Message/Messaging Service (Kısa Mesaj)
SNA : Systems Network Architecture
SNIA : Storage Networking Industry Association (Depolama Ağı Endüstrisi Birliği)
SPKn, Kanun : Sermaye Piyasası Kanunu
SPK, Kurul : Sermaye Piyasası Kurulu
SPL : Sermaye Piyasa Lisanslama Sicil ve Eğitim Kuruluşu A.Ş.
SQL : Structured Query Language (Yapılandırılmış Sorgu Dili)
SSID : Service Set Identifier (Hizmet Kümesi Tanımlayıcı)
SSO : Single Sign-On (Tek Oturum Açma)
SoD : Separation of Duty (Görevler Ayrılığı)
TCMB : Türkiye Cumhuriyet Merkez Bankası
TCP : Transmission Control Protocol (İletim Kontrol Protokolü)
TLD : Top Level Domain
TOR : The Onion Router
TSE : Türk Standartları Enstitüsü
TSPB : Türkiye Sermaye Piyasaları Birliği
TTK : 610 sayılı Türk Ticaret Kanunu
UDP : User Datagram Protocol (Kullanıcı Veri Bloğu Protokolü)
UPS : Uninterruptible Power Supply (Kesintisiz Güç Kaynağı)
URI : Uniform Resource Identifier (Tekbiçimli Kaynak Tanımlayıcısı)
URN : Uniform Resource Name (Tekbiçimli Kaynak Adı)
URL : Uniform Resource Locator (Tekbiçimli Kaynak Konumlayıcısı)
USB : Universal Serial Bus
VoD : Video on Demand (Talebe Bağlı Video)
VoIP : Voice Over Internet Protocol (IP Üzerinden Ses)
VPN : Virtual Private Network (Sanal Özel Ağ)
WAF : Web Application Firewall (Uygulama Güvenlik Duvarı)
WEP : Wired Equivalent Privacy (Kabloya Eşdeğer Mahremiyet)
Wi-Fi : Wireless Fidelity (Kablosuz Bağlantı Alanı)
WPA : Wi-Fi Protected Access(Wi-Fi Korumalı Erişim)
WPS : Wi-Fi Protected Setup (Wi-Fi Korumalı Kurulum)

XSS : Cross-Site Scripting(Çapraz Site Betik)
XML : Extensible Markup Language (Genişletilebilir İşaretleme Dili)
ZT : Zero Trust (Sıfır Güven)
ZTA : Zero Trust Architecture (Sıfır Güven Mimarisi)
WAN : Wide Area Network (Uzak Alan Ağı)
WLAN : Wireless Local Area Network (Kablosuz Yerel Alan Ağı)
WPAN : Wireless Personal Area Network (Kablosuz Kişisel Alan Ağı)
WWW : World Wide Web (İnternet Sunucuları Ağı)
W3C : World Wide Web Consortium (Dünya Çapında Ağ Konsorsiyumu)

Bu kitapta; bilgi sistemleri güvenliğine ilişkin bilgi güvenliği ve varlık yönetimi ele alınarak ağ güvenliği, erişim güvenliği, fiziksel ve çevresel güvenlik, veri ve iz kayıtlarının güvenliği ve üçüncü taraflarla iletişim güvenliği konularına yer verilmektedir.

1. BİLGİ GÜVENLİĞİ YÖNETİMİ

1.1. Kavram

İlk başta teknolojik ekipmanların fiziksel güvenliğiyle başlayan bilgi güvenliği konusu bugün siber güvenlik olarak kapsamı genişlemiş ve sadece BS birimlerini değil, kurumları, ülkeleri ve uluslararası organizasyonları da etkilemeye başlamıştır. Ülkemizde kurumsal düzeyde gerek kamu gerekse de özel sektör bağlamında çeşitli strateji, eylem planları, düzenleme ve rehberler seviyesinde birçok mekanizma ile makul bir güvence oluşturulmaya çalışılmaktadır. Bu konuda en yaygın örneklerden biri Uluslararası Standartlar Örgütü (ISO) tarafından yayınlanan ve her türden kurum için uygulanabilir olan Bilgi Güvenliği Standardıdır (ISO 27001:2013).

Bilgi güvenliği yönetimi, kurumda bilgi güvenliğinin kabul edilebilir düzeyde korunmasını sağlamak amacıyla geliştirilen ve kullanılan tüm mekanizmalardır. Bunlar; organizasyonel yapılar, politika ve prosedürler, süreçlerdir ve çeşitli varlıklardır. Bilgi güvenliğinde amaç bilginin aşağıda verilen üç temel özelliğini korumaktır (ISO, t.y.):

- Gizlilik (confidentiality): Bilgiye izinsiz erişimlerin engellenmesi.
- Bütünlük (integrity): Bilginin tam ve doğru olması.
- Erişilebilirlik (availability): Bilginin ihtiyaç duyulduğunda yetkili taraflarca erişilebilir olması.

Kurumsal düzeyde bilgi güvenliği nereden başlar, bu konuda aksiyon almak isteyen bir kurumun işe hangi standart/rehber/düzenlemeden başlamalıdır sorusunun cevabı olarak başlangıç noktası bilginin kurum için önemini idrak etmek ve "korunması gereken bir varlık" olarak görülmesini sağlamaktır denilebilir.

Geleneksel olarak hiçbir kurum -en azından henüz bilgi güvenliği kavramı çok yaygınlaşmadan önce- varlıklarını "sayarken" veya "envanterini gözden geçirirken" bilgiyi aklına getirmemiştir. Çünkü bilgi hem sayılabilen bir kavram değildir, hem de zaten ya kağıt üzerinde dosyaların içinde ya da bilgisayardadır. Tek başına bir varlık/değer olarak görülmemiştir. Ancak teknolojinin görece ucuzlaması, herkese ulaşması, son kullanıcıya yönelik çözümlerin çok yaygınlaşması sebebiyle artık kurumlar bilgiyi yine bir varlık olarak tanımlamasa bile öneminin farkında ve önemli olan her şey gibi bilginin de korunması/yönetilmesi gerektiğini bilmektedir.

Bilgi güvenliği yönetiminde belirli bir rehber/yönetim çerçevesi/standart takip edilebilir. Bu durumda ilgili düzenlemenin gerektirdiği yol izlenmelidir. Bu karar üst yönetim tarafından verilmelidir. Bilgi güvenliğinde genel yaklaşım aşağıdaki gibi özetlenebilir ancak seçilen yönteme göre bazı farklılıklar olabilir.

1.2. Üst Yönetimin Bilgi Güvenliği Sorumluluğu

Bilgi güvenliği teknik bir iş değildir ve kurumun her kademesini ve her çalışanını ilgilendirir. Kurumda bu işin sorumluluğunun en üstte olması beklenmektedir. Bilgi güvenliği politikasının oluşturulması ve her yıl gözden geçirilmesi, bu kapsamda görevlendirmelerin yapılması, risk yönetiminin gerçekleştirilmesi, çalışanlarının farkındalığının sağlanması, bilgi güvenliği ihlallerinin değerlendirilmesi üst yönetime verilmiş sorumluluklardır. Üst yönetim/yönetim kurulu aldığı/alacağı kararlar, uygulama tarzı ve bizzat bireysel yaklaşımıyla bu konuya verdiği önemi göstermelidir.

1.3. Roller ve Sorumluluklar

Üst yönetim tarafından bu konuyla görevlendirilmiş en az bir kişinin (tek görevi bu olmayabilir) sorumlu olarak belirlenmesi (bilgi sistemleri güvenliği sorumlusu), ayrıca kurumun büyüklüğüne göre bir ekibin de oluşturulması doğru olacaktır. Ekipte kurumdaki her birimden en az bir temsilcinin yer

alması önemlidir. Oluşturulan bu ekibin çalışma yönteminin kararlaştırılması, ekipçe alınan kararların birimlerde/kurumda uygulanabilir olmasını sağlayacak mekanizmanın belirlenmesi, ekipte görev dağılımı yapılması gerekir. Ekipte birimleri temsilen bulunanların, kendi birimindeki çalışmaları/fonksiyonları bilgi güvenliği ilkeleri özelinde gözden geçirecek ve gerekirse revize edecek/edilmesini sağlayacak yetkinlikte olması da önemli olan bir diğer unsurdur.

Bilgi güvenliği kapsamındaki her rolün görev tanımları yazılı, onaylı ve ilgililere duyurulmuş olmalıdır. Bilgi güvenliğinden sorumlu kişi ve kişiler kurum organizasyon şemasında yer almalıdır.

1.4. Farkındalık ve Eğitim

Bilgi güvenliği konusunda kurumların farkındalık yaratmak ve çalışanlarını eğitmek sorumluluğu bulunmaktadır. Tüm seviyedeki çalışanlara temel bilgi güvenliği eğitimi verilmeli, farkındalık sağlanmalı, zaman zaman konu hakkında bilgilendirmeler yapılmalıdır. Farkındalığın ve konuya verilen önemin sürdürülmesini teminen düzenli aralıklarla eğitimler tekrar edilmelidir. Ancak, eğitimlerin içeriği eğitim verilecek gruba göre düzenlenmeli ve güncel gelişmeleri de içermelidir.

1.5. Bilgi Güvenliği Politikası

Kurumlar bilgi güvenliğini uygulama yaklaşımı her ne şekilde olursa olsun, bir bilgi güvenliği politikası oluşturmalıdır. Bilgi güvenliği politikası bu konuda üst yönetimin genel yaklaşımını, konuya verilen önemi, kapsamı belirlemelidir. Diğer politikalar gibi üst yönetimce onaylanmalı, uygun şekilde duyurulmalı, çalışanların erişebilecekleri yerde olmalıdır. Belirli periyotlarda ve gerektiğinde periyot dışında gözden geçirilmeli ve tekrar onaylanıp duyurulmalıdır.

Bilgi güvenliği politikası aşağıdaki hususları ele almalıdır:

- Bilgi güvenliğinin tanımı, kapsamı, kurumsal bilgi güvenliği hedefleri
- Bilgi güvenliği ile ilgili kurumsal roller ve sorumluluklar
- Risk yönetimi
- Tabii olunan diğer düzenlemeler
- Bilgi güvenliği farkındalığı ve eğitimi
- Üst yönetimin bağlılığı/bakışı
- Bilgi güvenliği politika ve süreçlerine aykırı davranmanın olası sonuçları

İşletmede bilgi güvenliği faaliyetlerinin sadece çalışanları değil tedarikçileri, servis sağlayıcıları, müşterileri, iş ortakları kısaca dış paydaşları da etkileyeceği ve kurumun bilgi güvenliği hususlarının bunlardan etkileneceği dikkate alınmalı ve söz konusu politika uygun yöntemlerle paydaşlara duyurulmalıdır.

Bu kapsamda bilgi güvenliğine yönelik gerekirse destek politikaları oluşturulabilir. Bunlar kurumun genelinden ziyade belli bir birimi/iş sürecini hedef alabilir ve söz konusu birim/iş süreci bazında bilgi güvenliği ilkelerini düzenleyebilir veya ayrı politika dokümanları yerine tek bir bilgi güvenliği politikası da düzenlenebilir. Bu seçimde kurumun büyüklüğü, faaliyetlerin çeşitliliği, çalışan sayısı bir parametre olarak kabul edilebilir.

1.6. Risk Yönetimi

Bilgi güvenliği yönetiminin ayrılmaz bir bileşeni olan bu konu, 1020 nolu "*Bilgi Sistemleri Yönetimi ve Denetimi"* başlıklı çalışma notunda işlenmiştir. Burada kısaca tekrar etmek gerekirse bilgi sistemleri kapsamında risk yönetimi, bilgi sistemleri kullanımından kaynaklanan risklerin yönetilmesi ve bu konuda makul bir güvence sağlanması amacını taşır. Bu süreçle bilgi sistemlerine ait envanterde kayıtlı olan her tür varlığın maruz kaldığı risklerin yönetilmesi, dolayısıyla bunlar aracılığıyla iş süreçlerinin sürekliliği ve kurumsal bilginin uygun şekilde korunması amaçlanmaktadır. Risk yönetimi sürecinde ilk adım olarak belirtilen varlıkların tespiti aşamasında aşağıdaki belirtilen çerçeve dikkate alınmalıdır:

- Sunucu donanımları, depolama ortamları
- Kullanıcı cihazları (bilgisayar, tablet, akıllı cihazlar)
- Ağ cihazları
- Her türden yazılım

Burada "veri" ayrı bir varlık olarak gösterilmemiştir ancak yukarıda sayılan bilgi sistemlerini korumanın amacı esasında bu varlıklar aracılığıyla işlenen, saklanan ve iletilen veriyi korumaktır. Varlıkların belirlenmesi aşamasından sonra bu varlıkların her birinin yapısından veya kullanımından kaynaklanan her türlü zafiyet (vulnerability) tespit edilmelidir. Zafiyetlerin her biri birer istismar (exploit) noktası olduğundan bu zafiyetlerden yararlanabilecek tehditler belirlenmelidir. Bu şekilde, bilgi güvenliği riskinin üç temel noktası tespit edilmiş olur ki bu risk belirleme süreci (risk identification) olarak tanımlanmaktadır.

Bu noktadan sonra risk değerlendirmesi yapılmalıdır. Buna ilişkin çeşitli yöntemler mevcuttur. Kurum risk değerlendirme yöntemini seçmekte özgürdür. Ancak seçilen yöntemle ilgili belli bir bilgi birikimi oluşmalı ve tüm süreç buna uygun işletilmelidir.

Daha önce de belirtildiği gibi, kurumun risk yönetiminden hedefi sıfır riskli bir ortam olmamalıdır. Kurum tarafından belirli bir risk seviyesi eşik değer olarak belirlenmeli (kabul edilebilir risk değeri, risk iştahı), buna göre bu seviyenin üzerinde kalan riskler için risk işleme çalışması yapılmalıdır. Kontrolün maliyeti riskin olası maliyetini aşmamalıdır (buradaki istisna kontrolün yasal mevzuat tarafından zorunlu tutulmasıdır). Risk işleme seçenekleri aşağıda belirtilmiştir:

- **Riski azaltma**

Çeşitli kontroller yardımıyla riskin düşürülmesi. En çok tercih edilen seçenektir. Bu noktada bilgi sistemleri risklerine karşı geliştirilecek kontroller çok çeşitlidir ve politika, prosedür, talimat, yazılım, donanım gibi unsurları içerir. Seçilen rehber/yönetim çerçevesi/standartta bu konuda yardımcı olması amacıyla örnek kontrol listeleri olabilir.

- **Riski engelleme**

Riske sebep olan ürünün/hizmetin kullanımına son verme. Kontrollerle düşürülemeyecek risklerin tamamen engellenmesidir.

- **Riski paylaşma**

Riski üçüncü taraflarla paylaşma. Örneğin sigorta yaptırılması. Ancak bu seçenek riskin gerçekleşmesi olasılığını değiştirmemektedir.

- **Riski kabul etme**

Riske rağmen ürünün/hizmetin kullanımına devam etme. En kötü seçenek olarak değerlendirilir çünkü riski bilinen bir ürünü/hizmeti hiçbir şey yapmadan kullanıma devam etmektir.

Risk değerlendirme aşamasında gerekli yazılı dokümanlar oluşturulmalıdır. Bu dokümanlar asgari olarak risk değerlendirmede seçilen yöntemi, kabul edilen risk değerini, tüm varlıkların risk analiziyle beraber risk değerlerini, kabul edilebilir risk seviyesinin üzerinde kalan riskler için seçilen risk işleme yöntemini içermelidir.

Risk değerlendirme çalışması periyodik aralıklarla yenilenmelidir. Bunun dışında, bilgi sistemleri risklerinde önemli değişimlere sebep olacak (olumlu veya olumsuz) durumlarda da risk değerlendirmesi yenilenmelidir.

1.7. Bilgi Güvenliği Gözetimi, Ölçümü ve Değerlendirmesi

Bilgi güvenliği konusunda periyodik olarak gözetim, ölçüm ve değerlendirme yapılmalıdır. Bu kapsamda; uyulan tüm yasal düzenlemeler, standartlar, çerçeveler veya rehberler için söz konusu işlemlerin gerçekleştirilmesi gerekmektedir. Gözetim, ölçüm ve değerlendirme faaliyetinde amaç bilgi güvenliği kapsamında işletilen süreçlerin etkinliğini tespit etmek, bilgi güvenliği hedeflerinin başarımını ölçmek, risk değerlendirme sürecini ve risklere cevaben geliştirilen kontrollerin etkin ve işler olup olmadığının değerlendirilmesini sağlamaktadır.

Bilgi güvenliği ölçümleri için oluşturulan kontroller, ölçüt değerleri (KPI) ve risk değerlendirmeleri kapsamında iç ve dış denetimler ile doğrulanabilir. Bununla birlikte; teknik açıklıklar ve işleyişe ilişkin kısımlar, çeşitli senaryo uygulamaları, kırmızı-mavi takım alıştırmaları ve sızma testleri ile test edilebilir. Bilgi sistemlerinde yer alan açıklıkların ve zafiyetlerin önceden tespit edilmesi ve düzeltilmesi faaliyeti olan sızma testi, Sermaye Piyasası Kurulu Bilgi Sistemleri Yönetimi Tebliği uyarınca da (muaf olanlar hariç) yılda en az 1 kere gerçekleştirilmektedir.

Sızma testlerine yönelik tek bir standart bulunmamakla birlikte, uygulamada benzer yöntemler ve araçların kullanımı ön plana çıkmaktadır. Bununla birlikte, Sermaye Piyasası Kurulu Bilgi Sistemleri Yönetimi Tebliği ekinde yer alan "Bilgi Sistemleri Sızma Testleri Usul ve Esasları" tahdidi olmayan genel bir çerçeve belirlemektedir. Bu kapsamda,

- Sistemlere ilişkin hangi tip ön bilginin paylaşıldığı (Şirket tarafından sızma testini gerçekleştirecek taraflara sistemlere ilişkin hiç bilgi verilmeyen siyah/kapalı kutu (black box), test edilecek sistemlere yönelik bilgilerin sağlandığı beyaz/açık kutu (white box) veya kısmi bilgi sağlanan gri/şeffaf kutu (gray box) gibi farklı uygulamalar olabilir),
- Hangi sistemlere yönelik sızma testi gerçekleştirildiği (Altyapı, servisler, cihazlar, uygulamalar, sosyal mühendislik vd.),
- Hangi erişim noktalarının kullanıldığı (Internet, intranet (iç ağ), diğer ağlar),
- Hangi kullanıcı profillerinin test edildiği,
- Ayrı ayrı her bir bulgunun etkisi,
- Bulguların beraber değerlendiklerinde etkisi

hususlarının sızma testi raporunda yer alması gerekmektedir. Bu kapsamda gerçekleştirilen sızma testi sonucunda tespit edilen bulgular etki seviyesine göre değerlendirilip raporlanmalıdır.

1.8. Bilgi Güvenliği İhlal Yönetimi

Bilgi güvenliği ihlali bilgi sistemlerinde sonucu itibariyle bilgi veya bilgi barındıran ortamlarda bir zarara sebep olmuş veya olma ihtimali çok yüksek herhangi bir olay olarak tanımlanabilir. Bu bir arıza, yanlış kullanım, suiistimal, dışarıdan bir saldırı olabilir. İhlal olarak değerlendirilmesi için bilgi güvenliğini tehlikeye atmış olması yeterlidir.

Kurumda her çalışan –aldığı eğitim ve dikkati sayesinde- bir ihlali veya ihlalin belirtisini tespit edebilir, farkına varabilir. İşte bu yüzden tüm çalışanların bu tespitlerini veya şüphelerini konunun uzmanı kişilere iletebileceği bir mekanizma kurulu ve işler durumda olmalıdır. Bu bir çağrı hattı, bir yardım masası uygulaması, belli bir e-posta hesabı veya buna benzer bir yöntem olabilir. Önemli olan kurumun tümünde yaygınlaşmış olması, her seviyede personelin kullanabileceği basitlikte olması ve bu konuda tüm personelin bilgilendirilmiş olmasıdır. Hangi yöntemle yapılırsa yapılsın tüm çağrıların analiz edilmesi, gerekirse ilgili ekiplere yönlendirilmesi, çağrının sonucu konusunda çağrıyı yapan kişiye geri bildirimde bulunulması gerekmektedir. En az bir çalışan bu işle görevlendirilmiş olmalıdır.

Herhangi bir ihlal meydana geldiğinde işletilecek mekanizmalar ve tüm sorumluluklar yazılı ve onaylı olarak belirlenmiş, gerekli görevlendirmeler önceden yapılmış olmalıdır.

Bilgi güvenliği ihlali sadece çalışanlar tarafından fark edilmez. Esas olarak çeşitli gözetim mekanizmalarından elde edilen verilerin analiz edilmesiyle ortaya çıkarılır. Burada gözetim altında tutulacak birçok veri kaynağı, analiz yaparken kullanılacak da birçok ürün mevcuttur. Kurum kendi yapısı ve faaliyetlerinin çeşitliliğine uygun mekanizmaları kurmuş olmalıdır. Gözetim ve analizle ilgili sorumluluklar belirlenmelidir. Bu konuda detaylı bilgi "*Veri ve İz Kayıtlarının Güvenliği*" bölümünde mevcuttur.

Gözetim ve kurum içindeki geri bildirimlerden elde edilen veri değerlendirilmeli ve gerçekten bir bilgi güvenliği ihlali olup olmadığına karar verilmelidir.

Bilgi güvenliği ihlalinin gerçekleştiğine karar verilirse çeşitli iletişim mekanizmalarıyla gerekli iç ve dış bilgilendirmeler (bilmesi gereken ilkesine göre-need to know) yapılmalıdır. Dış bilgilendirme müşterileri ve hukuki mercileri içerebilir.

Kurum bünyesinde "Kurumsal Siber Olaylara Müdahale Ekibi" yer alıyorsa, ihlal bildirimlerinin bu ekip tarafından ele alınması gerekir. İhlalin türüne ve etkisine göre başka ekipler de devreye girebilir.

İhlalin fark edilmesinden sonraki en önemli süreç "kanıt toplama" sürecidir. Bu konuda izlenecek yolun mutlaka önceden belirlenmiş olması gerekir. Kanıt toplama sürecinin doğru şekilde yapılması için ilgili personelin eğitim alması değerlendirilmelidir.

İhlal çözümlendikten sonra gözetim işlevi için ihlale cevaben yapılan işlemler mutlaka kayıt altına alınmalıdır (log). İhlalin kök sebebi bulunmalı ve gerekli düzeltici/iyileştirici faaliyetler gerçekleştirilmelidir. Kurum her ihlalden bir şey "*öğrenmelidir*".

1.9. Bilgi Güvenliği Yönetiminin Değerlendirilmesi

Kurumda bilgi güvenliği yönetimi değerlendirilirken, diğer bölümlerde olduğu gibi burada da ilk önce ilgili tüm politika ve prosedürler incelenmeli, daha sonra da genel olarak işletmedeki bilgi güvenliği farkındalığı değerlendirilmelidir.

Bilgi güvenliği ve varsa destek politikalarının yazılı, üst yönetimce onaylanmış, tüm personele duyurulmuş ve düzenli olarak gözden geçirilmekte olup olmadığı hususu incelenmelidir. Yazılı, onaylı ve duyurulmuş bilgi güvenliği politikası olmaması veya bunun duyurulmaması risk yaratır. Bilgi güvenliği politikası sadece bilgi sistemleri birimine değil, tüm çalışanlara duyurulmuş olmalı ve her an erişilebilir yerde olmalıdır. Bunun yanı sıra yukarıda detayları belirtilen süreçlerin yazılı ve onaylı dokümantasyonda mevcut olduğu, bunların etkin bir şekilde işletildiği ve sahada karşılığının olduğu değerlendirilmelidir. Değerlendirme sırasında mümkün olduğu kadar kanıt toplanmalıdır.

Bilgi güvenliği ile ilgili çalışanlara verilen/aldırılan eğitim kayıtları incelenmelidir. Tüm personel en az bir kere eğitim almış olmalıdır.

Risk yönetim süreci değerlendirilirken geçmiş risk değerlendirmelerin sonuçlarına bakılmalı (mutlaka yazılı olarak mevcut olmalıdır), kabul edilebilir risk seviyesinin yönetimce onaylanıp onaylanmadığı gözden geçirilmelidir. Risk işleme süreci kontrol edilmeli, risk azaltma kararı verilen varlıklarla ilgili yapılacakların belli olup olmadığı (ne yapılacak, kim yapacak, ne zamana kadar yapacak) incelenmelidir.

Bilgi güvenliğinin izleme/ölçme süreci incelenmeli, ölçüm sonuçlarının üst yönetimce değerlendirilip değerlendirilmediği hususuna dikkat edilmelidir.

İhlal yönetim süreci değerlendirilirken geçmiş ihlal kayıtlarına bakılmalı, özellikle ihlalden kimin haberdar edildiği, toplanan kanıtlar, ihlale cevaben yapılan işlemler ve kök sebebin tespit edilip edilmediği incelenmelidir.

Örnek Sorular

Soru 1: Aşağıdakilerden hangisi risk işleme seçeneklerinden değildir?

A) Riski Azaltma
B) Riski Engelleme
C) Riski Paylaşma
D) Riski Öngörme
E) Riski Kabul Etme

Cevap: D

Soru 2: Aşağıdakilerden hangisi bilgi güvenliğinin üç temel özelliğidir?

A) Bütünlük-Kimlik Doğrulama-Erişilebilirlik
B) Gizlilik-Bütünlük-Yetkilendirme
C) Erişilebilirlik-Bütünlük-Gizlilik
D) Hesap Verebilirlik-İnkar Edilemezlik-Gizlilik
E) Hesap Verebilirlik-İnkar Edilemezlik-Erişilebilirlik

Cevap: C

2. VARLIK YÖNETİMİ

"Varlık" kavramı Uluslararası Standartlar Organizasyonu tarafından şöyle tanımlanmaktadır: "Varlık, kurum için potansiyel veya gerçek bir değeri olan veya olabilecek, fiziksel olan/fiziksel olmayan, sayılabilir/sayılamayan her şeydir." (ISO, t.y.).

Uluslararası Standartlar Organizasyonu varlık yönetimini ise şu şekilde tanımlamaktadır: "Bir işletmenin, bilgi teknolojisi varlıklarından değer kazanmak için koordine ettiği aktivitelerdir." (ISO, t.y.).

Uluslararası Bilgi Teknolojileri Varlık Yöneticileri Birliği'nin tanımına göre; varlık yönetimi kurum çapındaki tüm bilgi teknolojisi varlıklarının yaşam döngüsünü yönetmek ve stratejik karar almayı desteklemek için varlıkların mali, envanter, sözleşme ve risk yönetimi sorumluluklarını birleştiren yönetim mekanizmasıdır. (https://iaitam.org/what-is-it-asset-management/)

Varlık yönetiminde kayda alma ve bu kayıtları karar alma mekanizmasında kullanma vardır (Georgescu, 2021).

Varlık yönetiminin asıl olarak bilgi teknolojisi varlıklarından geniş bir kullanım alanı vardır. Ancak burada sadece bilgi teknolojisi varlıklarının (IT assets) yönetimi hakkında değerlendirme yapılacaktır.

BT varlık yönetimi birçok yönetim çerçevesi/standartta yer alan bir kavramdır ve en küçüğünden en büyüğüne tüm kurumlarda bir şekilde BT varlık yönetimi uygulamalarının yerleşmiş olması gerekir. Varlık yönetiminde çeşitli yazılım araçları mevcuttur ancak çok küçük kurumlarda böyle bir yatırım yapılmamış olabilir.

Varlık yönetimi, bilgi sistemleri stratejisinin gerçekleştirilmesinde rolü olan bir uygulamadır. Bilgi sistemleri stratejisinde belli bir zaman diliminde geliştirilecek çözümler ve bunların öncelikleri (iş hedeflerine göre) bulunur. Bu çözümlerin geliştirilmesi ve sunulmasında hangi varlıkların ne zaman gerekli olacağı sorusu varlık yönetimini de ilgilendirir. Bu konu, varlık yönetiminin kaynak yönetimi süreçleriyle de ilişkisi olmasına sebep olur.

Bunun yanı sıra varlık yönetiminin doğrudan bilgi güvenliği (varlığın işleyeceği, saklayacağı, ileteceği bilgi), risk yönetimi (varlığın maruz kalacağı riskler), bilgi güvenliği ihlalleri (varlıklar aracılığıyla oluşması), yardım masası (varlık kullanımına ilişkin problemler) ve değişim yönetimi (varlıkların kontrollü değişimi) süreçleriyle de ilişkisi vardır. Varlık yönetiminin merkezi olarak yapılması, tıpkı risk yönetimi ve strateji geliştirme süreçlerinde gördüğümüz üzere tutarlılığı ve sonuçların karşılaştırılabilmesini sağlar.

Bir işletmede BT varlık yönetimi uygulamalarına (diğer birçok konuda olduğu gibi), varlık yönetimine dair üst yönetimin bakış açısı ve ilkelerini yansıtan politika ve prosedürlerin geliştirilmesiyle başlanmalıdır. Bu politika ve prosedürler-kabaca- aşağıdakileri içermelidir:

- Varlık gereksinimlerinin belirlenmesi, onaylanması, satın alma süreçleri.
- Varlıkların test (muayene) ve kabul süreçleri.
- Tedarikçi seçimi, risk değerlendirmesi.
- Varlığın yaşam süresi boyunca izlenmesi.
- Varlığın yaşam süresi sonunda imhası.

Varlık yönetimi kapsamına aşağıda belirtilen tüm varlık tipleri girebilir:

- Tüm bilgi sistemleri donanımı (dizüstü bilgisayar, tablet, telefon, yazıcı vb) ve altyapı bileşenleri (güvenlik duvarı,).
- Satın alınan tüm yazılımlar (lisans bilgileri dahil).
- Kurumda geliştirilen yazılımlar (kodları).
- Bilgi sistemleri aracılığı ile işlenen/iletilen/saklanan tüm kurumsal veri/bilgi.

Yaşam döngüsü yaklaşımı genellikle bütün varlık yönetimi yazılımlarında bulunur.

Varlık yönetimi faydaları: kaynak kullanımı/verimliliğinde artma, risklere karşı koruma, toplam maliyette azalma olarak sayılabilir.

2.1. Varlık Yaşam Döngüsü

- **Talebin oluşması ve planlama**

İşletmede varlığa olan ihtiyacın/talebin ortaya çıkmasıyla başlar. Varlık yönetimi genelde düşünüldüğü gibi varlığın fiziksel olarak alımıyla başlamaz, varlığa ihtiyaç oluştuğu zaman başlar. Varlığa ilişkin talebin nasıl oluşturulacağı, bu noktada izlenecek adımlar, tedarik/satın alma yöntemleri bu aşamanın konusudur.

- **Alım/Tedarik**

Tedarikçi seçimi ve yönetimi kapsamında tedarikçiler kurum tarafından belirlenmiş çeşitli kriterlere göre seçilmelidir. Tedarik edilen varlıkların zamanında ve gereken niteliklerde sağlanmış olması, fiyat unsuru (diğer tedarikçiler arasında bir karşılaştırma), tedarikçinin geçmiş performansı bu kriterler arasında sayılabilir.

- **İzleme/Bakım**

Varlığın kuruma kabulü, kabul aşamasında izlenecek süreç (varlığın muayenesi/varlığa uygulanacak testler) bu aşamada gerçekleştirilir. Burada amaç tedarik edilen varlığın, kurumda talep edilen/ihtiyaç duyulan nitelikleri taşıyıp taşımadığının kontrol edilmesidir. Tedarik aşamasından önce bu nitelikler mutlaka yazılı hale getirilmelidir.

Varlığın test aşaması düzgün bir şekilde bitirilip varlık kuruma kabul edildikten sonra varlığa kabul sonrası uygulanacak işlemler gerçekleştirilmelidir. Bunlar varlığın envantere/kayda geçirilmesi, varlığın sınıflandırılması, etiketlendirilmesi, yapılandırılmasıdır.

Varlık kullanıma alınmadan önce ilgili kullanıcıların eğitim gereksinimi olup olmadığı değerlendirilmelidir. Kullanıma ilişkin olarak gerekirse talimat seviyesinde yazılı dokümanlar da oluşturulabilir.

Bu aşamada varlığın risk değerlendirmesi gerçekleştirilmelidir. Kuruma yeni bir varlık temini, bazı mevcut risklerde düşüş sağlayabilir ve/veya varlığın kendisi bazı riskleri beraberinde getirmiş olabilir.

Varlığın bakımı da bu aşamada yerine getirilmesi gereken bir süreçtir. Bakım varlığın alındığı günkü etkinliğini sürdürülebilmek, risklerini yönetilebilmek, varlıktan en iyi şekilde faydalanabilmek için gereklidir. Bakım aşamasında varlığa yapılan tüm işlemler kontrollü biçimde (değişiklik yönetimi süreçlerini de işleterek) yapılmalıdır. Her varlık türünün bakım gereksinimleri farklıdır ve bunların kararlaştırılmış olması gerekir. Bakım faaliyetleriyle kastedilen hem periyodik bakım, hem de arıza/hata sonucu yapılması gereken faaliyetleri kapsar.

- **Kullanımdan kaldırma/İmha**

Her varlığın belirli bir yaşam süresi vardır. Bu süre sonunda varlığın kullanımını sürdürmek ekstra maliyet çıkarabilir, varlık kurumda geliştirilen yeni çözümlerle uyumsuz hale gelebilir, varlığın riskleri artabilir, varlığa üretici/satıcı tarafından verilen destek son bulabilir. Bu yüzden yaşam süresi sonuna gelen varlıklar imha edilmeli veya uygun koşullarda (güvenli) kullanımdan kaldırılmalıdır. Ancak elbette bunun yöntemi de belirli ve yazılı olmalıdır. Bunları özetlersek:

- İmha süreçlerinin baştan belirlenmesi, sorumluların atanması ve eğitimi.
- Varlığın kategorisi, sınıfı ve diğer niteliklerine göre imha seçenekleri ve süreçleri.
- Varlığın üzerindeki verinin nasıl güvenli bir şekilde yok edileceği (fiziksel/mantıksal).
- Varlığın fiziksel/mantıksal olarak imhası veya güvenli bir şekilde kullanımdan kaldırılması. Bazı durumlarda varlığın imhası yerine saklanması gerekebilir. Bununla ilgili kuralların da belirlenmesi gerekir. Varlığın yer değiştirmesi/kullanıcısının değişmesi ise imha sürecinin parçası değildir.
- Yapılan işlemlerin kaydının tutulması.

2.2. Varlık Envanteri

Varlık yönetiminde önemli bir aşama varlıkların kayda almak ve kayıtların her durumda güncelliğini sağlamaktır. Özellikle büyük işletmelerde hem donanım hem de yazılım envanterini gerçek zamanlı sayılabilecek bir hassasiyetle çıkarabilmek için çeşitli yazılım çözümleri mevcuttur (asset discovery). Bunlar özellikle farklı coğrafi bölgelere dağılmış işletmelerde envanterin güncelliğini sağlamada çok kolaylık sağlar. Ancak çok küçük kurumlarda bunun için özel bir uygulama kullanılmayabilir.

Varlık envanteri çıkarılırken işletmenin diğer birimlerinde kullanılan varlık envanteri uygulamaları/yöntemleri ile beraber veya bilgi sistemlerine özel bir çözüm kullanılabilir. Ancak ayrı çözüm/yöntemler uygulanacaksa iki envanter arasında tutarsızlıklar olmaması konusuna özen gösterilmelidir. Çünkü bir varlığın iki ayrı birim tarafından ayrı ayrı kontrol edilmesi, güncellik ve daha birçok konuda anlaşmazlık ve tutarsızlık riski barındırır.

Varlık envanterinde varlığın temel bilgilerinin yanında mutlaka sahiplik bilgisi, varlığın sınıfı, varlığın hangi kullanıcıda/nerede olduğuna dair bilgi de yer almalıdır.

İşletmenin sahip olduğu lisanslar da birer varlıktır ve envanterde takip edilmelidir.

Varlık sahipliği konusu önemlidir, varlığın sahibi bir kişi/ekip/birim olabilir. Sahiplik konusu onaylı olmalıdır. Varlık sahipliği varlığın işletmeye kabulüyle (veya geliştirilme aşamasının tamamlanmasıyla) başlar, imha aşamasında sona erer. Varlık sahibi, yaşam döngüsü boyunca varlıktan sorumludur. Bu sorumluluklar; varlığın envantere kaydedilmesi, envanter bilgisinin güncelliğinin sağlanması, varlığın sınıflandırılması, varlığın risk yönetimi, korunması, uygun kullanım kurallarının belirlenmesi, bakımı ve en nihayetinde imha sürecidir. Varlık sahibi, günlük işler için bir/birden çok çalışanı görevlendirebilir ama bu kendi sorumluluğunu azaltmaz.

Varlık envanteri ilgili tüm çalışanlara açık ve erişilebilir durumda olmalıdır.

2.3. Veri/Bilgi Sınıflandırılması

Kurumlar sahip oldukları veriyi/bilgiyi uygun bir şekilde sınıflandırmalıdır. Sınıflandırmanın birincil amacı, bilgiyi önemine/kritikliğine göre korumaktır. Bilgi sınıflandırması yaparken bilgiyi işleyen/ileten/depolayan varlıkların da aynı kriterlere göre sınıflandırılması gerekir. Her bilgi aynı önemde/kritiklikte değildir. Dolayısıyla, her varlığa (bilgiye) aynı kontrollerin uygulanması gerekmez. Gerekmemekten öte her varlığa aynı kontrollerin uygulanması ya maliyeti artırıcı (eğer uygulanması maliyetli kontroller uygulanıyorsa) ya da riski artırıcı (eğer "hafif" kontroller uygulanıyorsa) sonuçlar doğurur. Bu yüzden varlıklar da ilgili oldukları bilgiye göre sınıflandırılır ve her sınıfa uygun kontroller geliştirilir.

Sınıflandırmada önemli bir aşama sınıflandırma kriterlerini seçmektir. Sınıflandırma bilginin riskine, kullanıldığı iş sürecinin önemine veya yasal gerekliliklere göre yapılabilir. Sınıflandırma kriterleri, oluşturulan sınıflar ve her sınıfın gerektirdiği koruma düzeyi tüm işletmede aynı anlamı taşımalıdır.

Uygulanan sınıflandırma kriterleri belirli aralıklarla gözden geçirilmelidir. Önemli bir diğer nokta bilginin zaman içinde sınıfının değişebileceğidir. Bu durumda bilgiyi işleyen/ileten/saklayan varlığın da sınıfı değişebilir. Bu değişimin sebebi bilginin ait olduğu iş sürecindeki değişimden veya bilginin niteliğinin değişmesinden kaynaklanabilir. Varlıklar sınıflandırılırken işlediği, sakladığı, koruduğu bilginin en yüksek kritiklik ve hassasiyet derecesine göre sınıflandırılmalıdır.

Sınıflandırma varlığın sahibinin sorumluluğudur. Sınıflandırma işletmeye özgüdür. Sınıflandırma sırasında yararlanılabilecek kritik bilgi/varlık kavramına ilişkin aşağıda iki ayrı tanıma yer verilmiştir:

Kritik Bilgi/Veri: "Güvenlik zafiyeti oluşması durumunda yasal yaptırımlara neden olabilecek, içeriğinin yetkisiz personel veya kişiler tarafından görülmesinin kuruma çok ciddi maddi veya manevi zarar vereceği her türlü bilgi/veri" (DDO, 2020).

Kritik varlık: "Kurumun hedeflerini gerçekleştirmede önemli etkisi olan varlıklardır" (ISO, t.y.).

2.4. Varlıkların Etiketlenmesi

İşletmede bulunan her bilgi sistemleri varlığı sınıflandırıldıktan sonra etiketlenmelidir. Bununla ilgili uygun bir yöntem ve sorumlular belirlenmelidir. Varlık etiketleme varlığın türüne göre değişebilir. Fiziksel varlıkların etiketlenmesiyle elektronik ortamda yer alan varlıkların (bilginin) etiketlenmesi farklı olacaktır. Ancak sonuç olarak fark etmesi kolay, tutarlı, işletmedeki herkes tarafından anlaşılır ve açık bir yöntem seçilmeli ve sürecin sorumluları belirlenmelidir.

2.5. Varlıkların Uygun Kullanımı

Varlığın uygun kullanımı ile kastedilen varlığın türüne, sınıfına, kullanılacağı süreçlere göre uygun biçimde korumak ve kullanmaktır. Uygun kullanım kurallarını belirlemenin amacı varlığın maruz kaldığı riskleri kontrol altında tutabilmek ve varlıktan beklenen faydayı görebilmektir. Her varlığın (varlık türünden bağımsız) en etkin, en verimli ve en güvenli şekilde kullanılabileceği/çalışabileceği şartlar vardır. İşte uygun kullanım kuralları, bu şartların yazılı ve onaylı hale getirilip tüm ilgililere duyurulmasıdır.

Burada unutulmaması gereken nokta, uygun kullanım kurallarının etik değerler, sorumluluk, gizliliğe riayet gibi unsurları da barındırması gerektiğidir. Bir diğer önemli nokta da, uygun kullanım kurallarının sadece işletme içi değil, işletmenin varlıklarını herhangi bir şekilde kullanan tüm dış tarafları da kapsadığıdır. Dolayısıyla gerekli dış tarafların da en azından varlıkların kullanımı öncesinde uygun şekilde bilgilendirilmeleri, şartları kabul etmiyorlarsa da varlığı kullanmamaları gerekir.

Burada ifade edilmesi gereken bir başka konu da, işletmede her varlığın kullanımının yetkilendirilmesidir. Hiçbir çalışan, uygun bir şekilde yetkilendirilmeden varlığı kullanmamalıdır. Yetkilendirme açık, anlaşılır ve organizasyon yapısına göre gerekli makamlarca onaylanmış olmalıdır ve uygun aralıklarla gözden geçirilmelidir (yetkilendirme konusu ilerleyen bölümlerde detaylı işlenecektir).

Varlıkların uygun kullanım kurallarına karşı gelmenin nasıl değerlendirileceği de belirlenmelidir.

2.5.1. Taşınabilir Varlıklar

Taşınabilir varlıklar içerdikleri özgül riskler nedeniyle ilave kontrollerle korunmalıdır. Taşınabilir varlıkların kullanımına sınır getirilmesi düşünülebilir (USB cihazları gibi). İşletme dışında işletmenin cihazlarıyla halka açık ağların kullanımı ve kişisel cihazlarla (bilgisayar, akıllı cihazlar) işletme ağına bağlanma durumunda uyulacak kurallar da belirli olmalıdır. Bunlar kurumsal bilginin açığa çıkmasına hatta veri kaybına elverişli noktalardır. Kişisel taşınabilir varlıkların işletmede kullanımı da düzenlenmelidir. Bu durum, özellikle zararlı yazılımların işletme sistemine girmesine elverişli bir noktadır.

Evrensel Seri Veri Yolu (Universal Serial Bus - USB)

Evrensel seri veri yolu, bir iletişim standardıdır. USB standardına sahip birçok taşınabilir ortam ya da cihazı bir bilgisayara bağlamak için kullanılır. USB, birçok çevre biriminin tek bir standart arabirim soketine bağlanmasına ve çalışırken değiştirilmesine veya aygıtların bilgisayarı yeniden başlatmadan veya aygıtı kapatmadan bağlanmasına ve bağlantısının kesilmesine izin vererek tak ve kullan özellikte tasarlanmıştır. Diğer önemli özellikleri, harici bir güç kaynağına ihtiyaç duymadan düşük tüketimli cihazlara güç sağlanması ve üreticiye özgü bireysel aygıt sürücülerinin kurulumuna gerek kalmadan birçok cihazın kullanılmasına izin verilmesini içermektedir.

USB bağlantı noktaları seri ve paralel bağlantı noktalarının hız ve bağlantı sayısı sınırlamalarının üstesinden gelir. USB 2.0 özellikleri saniyede 480 Megabit'e (Mbps) kadar veri aktarımını destekler. USB 3.0 bu hızın on katına, saniyede 5 Gigabit'e (Gbps) ulaşabilirken USB 3.1 10 Gbps'ye kadar aktarım hızlarına erişebilmektedir.

USB bağlantı noktaları fareler, klavyeler, tabletler, oyun tabletleri, oyun çubukları, tarayıcılar, dijital kameralar, telefonlar, yazıcılar, kişisel medya oynatıcılar, harici bellekler ve harici sabit sürücüler gibi bilgisayar çevre birimlerini ve taşınabilir ortamları bağlayabilir. Çoğu işletim sistemi bir USB

aygıtının ne zaman bağlandığını algılamakta ve gerekli aygıt sürücülerini yüklemektedir. Yüksek kaydedilebilirlik, güç gerektirmeyen depolama ve çevresel uyum özellikleri sunmaktadır. Örnek olarak memory stick, compact flash, SD (güvenli dijital) ve harici bellek verilebilir.

USB kullanımıyla ilgili riskler

- **Virüsler ve diğer kötü amaçlı yazılımlar**

USB sürücüler bilgisayar virüslerinin bulaşmasına uygun bir ortam hazırlamakta olup korunmayı güçleştirmektedir. İki makine arasında dosya paylaşımında kötü amaçlı yazılımların (ör virüsler, casus yazılımlar ve tuş kaydediciler) aktarılma riski vardır. Bazı USB sürücülerde sürücüyü salt okunur moda geçirebilecek fiziksel bir anahtar bulunmakta olup dosyalar güvenilmeyen bir makineye aktarılırken salt okunur modda olan bir USB sürücü aygıta herhangi bir verinin (virüsler dahil) yazılmasını engellemektedir.

- **Veri hırsızlığı**

Bilgisayar korsanları, kurumsal casuslar ve hoşnutsuz çalışanlar veri hırsızlığına sebep olabilmektedir. Çoğu durumda bir USB sürücüyle birlikte USB bağlantı noktasına sahip kullanıcısı yerinde olmayan ve kilidi açılmış herhangi bir bilgisayar suç etkinliği için bir fırsat sağlamaktadır. Sosyal mühendislik yöntemleri kullanarak bir bilgisayar korsanı verileri çalmak veya casus yazılımları yüklemek için kurumsal bir bilgisayara fiziksel erişim sağlayabilir.

- **Veri ve medya kaybı**

USB sürücülerin taşınabilirliği, veri ve ortam kaybı için artan bir risk yaratmaktadır. Şifrelenmemiş bir USB cihazının kaybolması, cihazı bulan herhangi bir kişinin sürücüdeki verilere erişebilmesine sebep olabilmektedir.

- **Verilerin bozulması**

Sürücülerin uygunsuz şekilde çıkartılması bozulma nedeniyle veri kaybı yaşanmasına sebep olabilir. USB sürücüler çıkarıldığında bilgisayar otomatik olarak algılayamayabilir. Bu nedenle USB sürücüler CD-ROM ve DVD-ROM gibi diğer çıkarılabilir ortam türlerinden farklılık arz etmektedir. USB sürücülerinin kullanıcıları aygıtı çıkarmayı düşündüklerinde bilgisayarı uyarmalıdır. Aksi halde bilgisayar özellikle sürücüdeki dosyalar açıksa, aygıtın bağlantısını kesmek için gereken temizleme işlevlerini gerçekleştiremez.

- **Gizlilik Kaybı**

Kullanışlı fiziksel özellikleri nedeniyle bir USB sürücüde önemli miktarda veri saklanabilmektedir. Saklanan bazı bilgiler gizli olup disk kaybedildiğinde veri kaybı bir risk haline gelmektedir. Bu durum yasal düzenlemeleri ihlal noktasında kadar gidebilir.

USB'ler ile ilgili güvenlik önlemleri

Bir BS denetçisi, USB'lerle ilgili risklerin yönetilebilmesi için alınabilecek güvenlik önlemlerini bilmeli ve bu amaçla işletmede uygulanan kontrolleri incelemelidir:

- **Şifreleme**

İdeal bir şifreleme stratejisi verilerin USB sürücüde saklanmasına izin vermekle birlikte, güçlü bir parola veya biyometrik veri gibi gerekli şifreleme anahtarı olmadan verileri işe yaramaz hale getirebilir.

- **Detaylı kontrol**

Portların merkezi yönetimini sağlayan ürünler özel yazılım kullanılarak gerçekleştirildiği için kurumsaldan bireysel sisteme merkezi yönetim mümkündür. Tüm güvenlik sorunlarında olduğu gibi izole bir teknolojik çözüm yetersizdir. Bellek kartı ve USB sürücülerin güvenli bir şekilde çalışmasını sağlamak için güçlü politikalar, prosedürler, standartlar ve kılavuzlar uygulanmalıdır.

- **Eğitim**

Harici bellekler o kadar küçük ve göze batmaz ki kolayca gizlenip bir kuruluştan çıkarılabilirler. Fiziksel güvenlik personeli USB aygıtlarını ve oluşturdukları riski anlamalıdır.

- **Masaüstü kilitleme politikasının uygulaması**

Yüksek riskli ortamlarda masaüstü bilgisayarlar kısa aralıklardan sonra otomatik olarak kilitlenecek şekilde yapılandırılmalıdır.

- **Virüsten koruma politikası**

Virüsten korunma yazılımı, bağlı tüm sürücüleri ve çıkarılabilir medyayı tarayacak şekilde yapılandırılmalıdır. Kullanıcılar dosyaları açmadan önce tarama konusunda eğitilmelidirler.

- **Yalnızca güvenli cihazların kullanımı**

Şifreleme kullanımını zorunlu kılınmalıdır. USB'leri yönetmek, şifrelemeyi zorlamak veya yalnızca şifrelenmiş cihazları kabul etmek için mevcut yazılımlar kullanılmalıdır.

- **İade için iletişim bilgisi yazılması**

Bir USB sürücü kaybolursa iade edilmesi gereken kişi bilgisi içeren küçük, okunabilir bir metin dosyası da cihazın geri alınmasına yardımcı olabilmektedir. Şirket ayrıntıları belirtilmemeli ancak, telefon numarası veya posta kutusu yazılabilir. Ayrıca, sürücüdeki bilgilerin gizli ve yasalarla korunduğunun açıkça belirtildiği yasal bir feragatname eklemekte fayda bulunmaktadır.

2.6. Varlıkların Dolaşımı

Varlık yönetimi başlığında değerlendirilmesi gereken hususlardan biri de varlıkların halen kullanım aşamasındayken yerinin/kullanıcısın değişiminde yapılması gerekenlerdir. Özellikle kullanıcıya tahsis edilen donanımlar mesleki/kişisel bilgi içereceğinden başka bir kullanıcıya verilmeden önce gerekli veri temizleme işlemleri yapılmalıdır. Envanter kayıtlarından da aktif olarak hangi kullanıcıda olduğu görülebilmelidir.

Fiziksel varlık olarak niteleyebileceğimiz varlıkların (her tür donanım, bilgisayar, sunucu gibi) yaşam döngüsü boyunca birçok kez işletme dışına çıkması gerekebilir (arıza/bakım). Bu gibi durumlarda izlenecek yol varlık sınıfı bazında değerlendirilmeli ve yazılı süreçler oluşturulmalıdır. Varlığın işletme dışına çıkarılması yüksek veri kaybı riski içerdiğinden, önce varlığın üzerindeki verinin güvenli bir şekilde silinmesi, bunun mümkün olmadığı durumlarda üzerinde bulunan verinin sınıfına göre depolama ortamlarının asla işletme dışına çıkarılmaması, gerekiyorsa sökülmesi/yeni depolama ortamı edinilmesi, sadece cihaz arızaları için dışarı çıkartılmasına izin verilmesi gibi yaklaşımlar benimsenebilir. Ayrıca işletme dışında teslim edilecek kurumla mutlaka gizlilik anlaşması da yapılmalıdır. İşletme dışına çıkan varlıkların bu durumu envanter kayıtlarından görülebilir olmalıdır (kime teslim edildiği bilgisiyle).

2.7. Varlıklara Yönelik Tehditler ve İlgili Kontroller

İşletmede varlık yönetimi süreçleri değerlendirilirken ilk önce ilgili tüm politika ve prosedürler incelenir ve bu konuda farkındalığın olup olmadığına bakılır. Daha sonra varlık envanteri incelenip (varlık envanterinin çıkarılmış olması gereklidir) güncelliği sorgulanır. Varlıkların belirli kriterlere göre sınıflandırılmış ve her sınıfın uygun kullanım kuralları belirlenmiş olmalıdır.

İşletmede varlık yaşam döngüsünün işletilmesi değerlendirilmelidir. İlgili süreçler bu şekilde adlandırılmamış olabilir ancak mevcudiyeti ve işlerliğine bakılmalıdır. Yaşam döngüsünün her aşaması kanıtlar üzerinden gidilerek incelenmelidir.

Kullanımda olan varlıkların işletme dışına çıkarılması sırasında uygulanan kontrollere dikkat edilmelidir. Burası veri sızıntısı için risk içeren bir alandır. Taşınabilir cihazlarla ilgili ilave kontroller, varlıkların kullanım süresi sonunda gerçekleştirilen işlemler ve bunların işlerliği değerlendirilmelidir. Kişisel cihaz ve medyaların kullanımına ilişkin kontroller de değerlendirme sürecine eklenmelidir.

Örnek Sorular

Soru 1:

I- Varlık yönetimi sanal sistemler için gerekli değildir.

II- Varlık yönetiminde birden çok envanter yazılımı ile işletim kolaylığı sağlanabilir.

III- Kurumun tüm varlıkları için sınıflandırma yapmaya gerek yoktur.

IV- Veri kaybı riskini azaltmak için tamir ve bakım işlemleri şirket dışında gerçekleştirilmemelidir.

Yukarıdakilerden hangisi/hangileri varlık yönetimi kapsamında yanlıştır?

A) II ve III

B) Yalnız II

C) I ve III

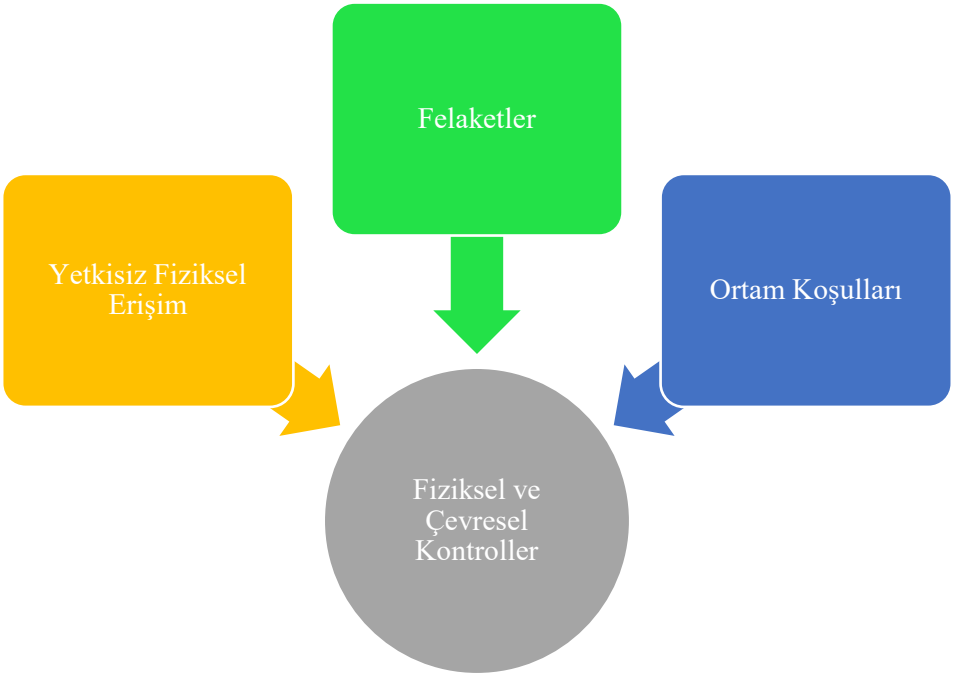
D) I,II, III ve IV

E) I, II ve III

Cevap: E

3. FİZİKSEL VE ÇEVRESEL GÜVENLİK

Bilgi sistemlerinin ve bu sistemleri barındıran fiziksel mekanların güvenliği kapsamında fiziksel ve çevresel tehditlere karşı alınması gerekli tedbirler bu başlık altında yer almaktadır.



Şekil 1: Fiziksel ve Çevresel Kontrollerin Temel Amaçları

Fiziksel kontroller ve çevresel kontroller olmak üzere konu iki başlık altında ele alınabilir:

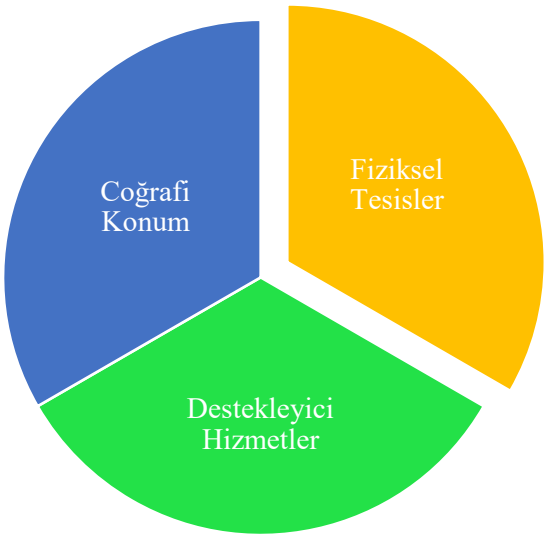
- Fiziksel kontroller
- Çevresel kontroller

Bu kontrollerdeki en temel amaçlar: (TSE, 2013)

- Yetkisiz fiziksel erişime karşı koruma
- Doğal veya insan kaynaklı felaketlere ve çevresel etkilere karşı koruma

Fiziksel ve çevresel güvenlik kontrolleriyle ilgili *bilgi işleme tesisi(olanağı)* kavramı kullanılmaktadır. Bir bilgi işleme tesisi bir yer veya bir faaliyet olarak (maddi veya maddi olmayan) bilgi işlem faaliyetlerinde kullanılan her türlü sistem, servis, altyapı ve bu bileşenlerin konuşlandırıldığı fiziksel mekanlar olarak tanımlanmaktadır. Bu bağlamda, fiziksel ve çevresel güvenlik aşağıdaki alanları kapsamaktadır: (NIST, 1995) (Şekil 2)

- Fiziksel tesisler bilgi sistemleri sistem ve ağ bileşenlerini barındıran bina, diğer yapı veya araçlardır. Bu tesislerin fiziksel özellikleri; yetkisiz erişim, yangın, su sızıntısı vb. fiziksel ve çevresel tehditlerin seviyesini belirler. Bu çerçevede sistemler çalışma konumlarına göre statik, mobil veya taşınabilir olarak sınıflandırılabilir.
  - Statik sistemler bina gibi sabit ortamlarda kurulur ve çalıştırılır.
  - Mobil sistemler, sabit bir yapının işlevini yerine getiren ancak sabit olmayan araçlarda çalışan sistemlerdir.
  - Taşınabilir sistemler, bir mekana bağlı olmadan herhangi bir yerde veya açıkta çalışabilirler.
- Fiziksel tesislerin faaliyetlerin gerçekleştirildiği coğrafi olarak konumu da doğal veya insan kaynaklı afetlere maruz kalma veya çevredeki faaliyetlerden etkilenme açısından risklerini belirler. Örneğin; deprem sel, yangın, patlama, sivil kargaşa, kimyasal dökülmeler, radar benzeri elektromanyetik yayıcı kaynaklı parazitler.



Şekil 2: Bilgi İşleme Tesisleri

• Destekleyici altyapı hizmetleri, hem teknik hem de insan tabanlı bilgi sistemlerinin işleyişini destekleyen hizmetlerdir. Bilgi sistemleri elektrik gücü, sıcaklık, nem gibi koşullar açısından kontrollü bir ortam gerektirir. Bu yönde; ortam koşullarının kontrolünün gerçekleştirilmesi bilgi sistemleri faaliyetlerinin kesintiye uğramaması ve teçhizat ve depolanan verilerin zarar görmemesi açısından önem arz etmekte olup fiziksel ve çevresel güvenliğin sağlanması elektrik gücü, iklimlendirme ve telekomünikasyon gibi destekleyici tesislere bağlıdır.

Fiziksel ve çevresel güvenlik tedbirlerinin dört ana odak noktası bulunmaktadır: (Şekil 3)

• Fiziksel hasar gerçekleştiği takdirde sistemlerin tamir edilmesi ve değiştirilmesi, sistemlerin yedek veriler üzerinden yeniden yüklenmesi gerekir.

• Faaliyetlerin kesintiye uğraması kapsamında zararın büyüklüğü hizmet kesintisinin süresine, zamanlamasına ve hizmetin özelliklerine bağlıdır.

• Bilgilerin izinsiz ifşası, bilgi sistemleri üzerindeki hassas bilgilerin gizliliğinin korunamamasına neden olunabilir.

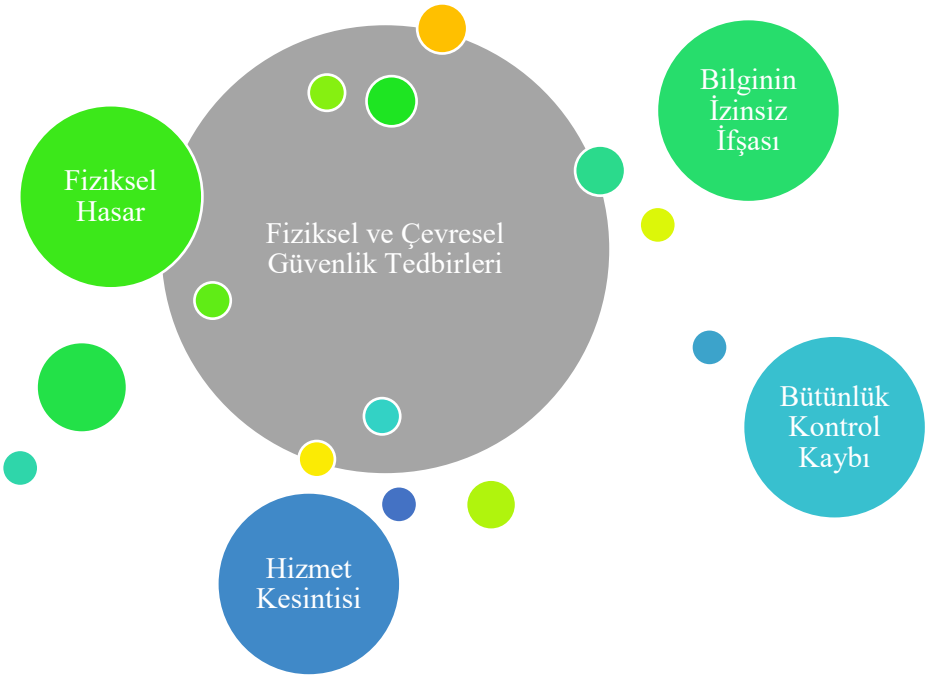
• Sistem bütünlüğü üzerinde kontrol kaybı bağlamında, bilgi sistemlerine fiziksel erişimle mantıksal erişim kontrolleri de dahil kontrollerin atlatılması ve bilgi sistemleri üzerinde kontrolün kaybolarak sistemler üzerinde yapılacak değişikliklerin önüne geçilmesi ve belirlenmesi mümkün olmayabilir.

Fiziksel ve çevresel güvenlik kontrolleri; mantıksal erişim kontrolleri, kimlik tanımlama ve doğrulama, bilgi sistemleri sürekliliği ve acil durum eylem planlaması gibi alanları destekler ve bu alanların düzgün işleyişine dayanır. Bu alanlarla birlikte emniyet, itfaiye, sağlık kurumlarının uzmanlıkları fiziksel ve çevresel kontrolleriyle yakından ilgili olduğu için bu kontrollerin planlamasında başvurulan kaynaklar arasındadır. Örneğin; (NIST, 1995)

• En iyi mantıksal erişim kontrolleri uygulanmış olsa bile bilgi sistemlerine yetkisiz fiziksel erişim sağlandığı durumlarda bu kontroller devre dışı bırakılabilir.

• İş sürekliliği kapsamında göz önünde bulundurulması gereken en önemli faktörler arasında fiziksel ve çevresel kontroller yer almaktadır. Bu kontrollerin uygun bir şekilde planlanması iş sürekliliğinin devam ettirilmesi ve felaket durumlarında kayıpların en aza indirilmesi yönünde faydalı olur.

• Fiziksel erişim kontrol sistemlerinin gerekli kimlik tanımlama ve doğrulama işlemleri için mevcut bilgi sistemleri kapsamında kullanılan kimlik tanımlama ve doğrulama mekanizmalarını kullanması mümkündür.



Şekil 3: Fiziksel ve Çevresel Güvenlik Tedbirleri Odak Noktaları

3.1. Fiziksel Kontroller

Bilgi sistemlerine fiziksel erişimler yönetilmeli ve korunmalıdır. Bu kapsamda aşağıdaki hususlar göz önünde bulundurulmalıdır: (DDO, 2020: 138)

• Tesislerin fiziksel güvenlik sınırları belirli mi?

• Fiziksel tesislerin içerisinde güvenlik kontrollerini sağlayabilecek bir güvenlik birimi mevcut mu?

• Fiziksel tesislere personel ve araç giriş/çıkışları kayıt altına alınıyor mu? Kimlik kontrol mekanizmaları mevcut mu?

• Ziyaretçilerin kuruma giriş/çıkış kontrollerini içeren bir prosedür mevcut mu?

• Kapalı devre kamera sistemi bulunuyor mu?

• Kritik bilgi sistemleri için güvenli alanlar oluşturulmuş mu? Güvenli alanlar nasıl belirlenmektedir?

• Güvenli alanlara giriş/çıkış işlemlerinde kimlik doğrulama mekanizmaları kullanılıyor mu? İşlemler kayıt altına alınıyor mu?

• Personelin hangi alanlara giriş yapabileceği belirli mi, yetkilendirme periyodik kontrolleri yapılıyor mu?

• Güvenli alanlarda çalışma kuralları belirli mi?

• Kurum dışına çıkan bilgi sistemi varlıkları kayıt altına alınmakta mıdır? Transfer için bir onay ve yetkilendirme süreci var mı?

• Destek, bakım gibi hizmetler için gelen 3. Taraf personeline refakat edilmekte mi?

• Temiz masa temiz ekran politikası uygulanıyor mu?

Kritik bilgi sistemleri için güvenli alanlar oluşturulmalı ve bu alanlara sadece yetkili kişilerce erişim sağlanacak şekilde giriş/çıkış işlemlerinde kimlik doğrulama mekanizmaları kullanılmalıdır. Bilgi sistemleri özelinde fiziksel korunması gerekli tesislere örnekler aşağıda listelenmektedir: (ISACA, 2019: 256)

- Sistem odası / Veri merkezi
- Bilgisayar odası
- Programlama alanı
- Operatör konsolları ve terminalleri
- Teyp kitaplığı, teypler, diskler ve tüm manyetik ortamlar
- Depolar ve malzemeleri
- Tesis dışı yedekleme dosyası depolama tesisi
- İletişim kabinetleri
- Telekomünikasyon ekipmanı (radyolar, uydular, kablolama, modemler ve harici ağ bağlantıları dahil)
- Mikrobilgisayarlar ve PC'ler
- Güç kaynakları
- Atık alanları
- Özel telefonlar/telefon hatları
- Santral odası
- Taşınabilir ekipmanlar (el tipi tarayıcılar ve kodlama cihazları, barkod okuyucular, dizüstü bilgisayarlar, yazıcılar, cep yerel ağ (LAN) adaptörleri ve diğerleri)
- Yerinde ve uzak yazıcılar
- Yerel alan ağları (LAN)
- Sistem, altyapı ve yazılım belgeleri

Fiziksel erişim kontrollerinin amaçlarının can güvenliğinin sağlanması amacıyla çeliştiği söylenebilir. Şöyle ki; acil durumlarda can güvenliği kapsamında tesislerden kolay bir şekilde çıkış yapılması önemlidir fakat fiziksel erişim kontrollerinde giriş/çıkışlar kontrol edilmeye çalışılmaktadır. Bu manada can güvenliği öncelikle göz önünde bulundurularak, iki hedef arasında bir denge sağlanması gerekmektedir (NIST, 1995) Bazı fiziksel erişim kontrolleri aşağıda açıklanmaktadır: (ISACA, 2019: 256)

- **Sürgülü kapı kilitleri:** Geleneksel kapı kilitlerini açmak için metal anahtar gerekir. Anahtarın kullanılması, saklanması ve kopyalanmaya karşı korunması ile ilgili kontroller sıkı şekilde uygulanmalıdır.

- **Kombine kapı kilitleri (Şifreli kilitler):** Sayısal bir kombinasyonun bir tuş takımı veya kadran aracılığıyla girilebildiği şifreli kilitlerdir. Giriş sağlamak için kullanılan kombinasyonun sadece yetkili kişiler tarafından bilinmesi sağlanmalıdır. Bu bağlamda, düzenli aralıklarla ve gerekli durumlarda kullanılan kombinasyon değiştirilmelidir.

- **Elektronik kapı kilitleri:** Bu tip kilitlerde erişim sağlamak için sensörlü bir okuyucunun tanıyabildiği manyetik ve çip tabanlı kartlar kullanılır. Kartta saklanan kod sensör tarafından okunarak kilit mekanizması açılır. Kişilere kartların ve yetkilerinin verilmesi ve geri alınması yönetimi etkin bir şekilde gerçekleştirilmelidir. Sürgülü ve şifreli kilitlere göre avantajları arasında erişim için kişiye özel kart verilebilmesi, kişiye özel erişim kısıtlamaları yapılabilmesi, kopyalanmasının zor olması, kolayca devre dışı bırakılabilmesi, yetkisiz giriş denemelerini izlemek için alarm oluşturulabilmesi sayılabilir.

• **Biyometrik kapı kilitleri:** Kişilerin parmak izi, retina, ses, el geometrisi gibi biyometrik özelliklerinin erişim sağlanması esnasında kimlik doğrulamak için kullanıldığı mekanizmalardır. Askeriye gibi, kritik ve hassas tesislerin erişim güvenliğinin sağlanmasında biyometrik erişim kontrolleri tercih edilmektedir.

• **Günlük kayıtlarının elle tutulması:** Fiziksel tesislere giriş/çıkış kayıtları yazılı halde bir defterde saklanabilir. Erişim güvenliği sağlanan tesise, fiziksel erişim sağlamadan önce mekan dışında kimlik kartları ile kimlik doğrulaması yapılmalı ve gerekli bilgiler kayıt altına alınmalıdır. Örneğin; bir binaya ziyaretçi girişi esnasında ziyaretçilerin adları, çalıştıkları şirket, ziyaret nedenleri, görüşülecek kişiler; giriş/çıkış saatleri, ziyaretçi imzası vb. bilgilerin toplanması sağlanmalıdır.

• **Elektronik kayıt:** Bütün başarılı veya başarısız fiziksel erişim denemeleri otomatik olarak erişim kontrol sistemleri tarafından izlenebilirlik açısından günlüğe kaydedilmelidir.

• **Yaka kartları:** Kimlik kartları (fotoğraflı kimlik kartı) çalışanlar tarafından takılmalıdır. Bu personelin tanımlanabilmesi açısından kolaylık sağlar. Bununla birlikte ziyaretçiler için de yaka kartları kullanılmalı personelden ayrılabilmesi için farklı tip ve renkte kartlar kullanılmalıdır. Yaka kartları elektronik kart anahtarı olarak da kullanılabilir. Yaka kartı verilmesi ve geri alınması süreçleri tanımlı olmalıdır.

• **Kamera sistemleri:** Kameralar aracılığıyla kritik görülen mekanlar (kurum binasına giriş noktaları, bina içindeki koridorlar, sistem odası, güvenli alanlar, bina çevresi) güvenlik görevlileri tarafından düzenli bir şekilde izlenmeli, görüntüler kayıt altına alınarak ihtiyaç duyulan süre için ve yeterli çözünürlük kalitesinde uygun koşullarda saklanmalıdır. Kamera sistemlerine erişimler yetkilendirmeli, yetkisiz erişimlere karşı korunmalıdır.

• **Güvenlik görevlileri:** Fiziksel tesisin büyüklüğü, bulunduğu coğrafi alan ve mevcut diğer fiziksel erişim kontrolleri (kartlı giriş sistemleri, kamera sistemleri) ile orantılı bir şekilde ve bilgi düzeyinde güvenlik görevlisi bulundurulmalıdır. Güvenlik görevlilerinin etkinliği otomatik fiziksel erişim kontrolleri ve kamera sistemleriyle desteklendiğinde artacaktır. Güvenlik personeli tarafından görevlerin tam olarak gerçekleştirilip gerçekleştirilmediği düzenli kontrol edilmelidir.

• **Ziyaretçiye refakat edilmesi:** Ziyaretçilere (bakım personeli, satış elemanları, danışmanlar, denetçiler, arkadaşlar vb..) fiziksel tesiste bulunduğu zaman süresince bir güvenlik personeli veya ilgili bir personel tarafından eşlik edilmelidir.

• **Emniyet kapısı (Deadman door):** Mantrap veya hava kilidi (airlock) girişi olarak da tanımlanır. Yüksek güvenlik gerektiren fiziksel tesislere iki kapılı bir mekanizma ile giriş sağlanır. Birinci kapı ile ikinci kapı arasındaki boşluğa yetkili bir tek kişinin girmesine izin verilir ve birinci kapı kilitlendikten sonra ikinci kapı açılır. Bu sayede; yancı geçiş (piggybacking, tailgating), yetkili bir kişiyi takip eden yetkisiz bir kişinin güvenli bir alana girmesi, riski azaltılmış olmaktadır.

• **Bilgisayar kilitleri:** Özellikle, taşınabilir dizüstü bilgisayarlar masaya sabitlenip kilitlenerek hırsızlığa karşı korunmalıdır.

• **Kontrollü bir tek giriş noktası:** Bir binaya birçok noktadan giriş yapılabilmesi kontrolsüz giriş ihtimalini arttırır. Örneğin; bir binanın dışarıda sigara içilen mola alanları gibi bölgelerine açılan kontrolsüz giriş kapılarına önlem alınmalıdır. Güvenlik veya resepsiyon görevlisi tarafından izlenen kontrollü bir tek veya en az giriş noktası fiziksel mekanlara girişte kullanılmalıdır. Acil çıkışlar, hızlı tahliye için alarmlı bir acil çıkış mandalına bağlanabilir.

• **Alarm sistemi:** Etkin olmayan giriş noktaları, hareket sensörleri, tek yönde giriş ve çıkış yapılabilen kapıların tersi yönünde sesli uyarı sistemleri kullanılmalıdır. Bu alarm sistemleri ikaz durumuna geçtiğinde ilgili güvenlik personeli tarafından duyulabilmelidir.

• Kullanılmayan donanımlar, kağıt ortamındaki evraklar kilitli ortamlarda (odalar/dolaplarda) bulundurulmalıdır.

• Bilgi sistemlerinin bulunduğu tesisler dışarıdan görünür ve tanımlanabilir olmamalıdır. Pencere ve yön işaretleri olmamalıdır. Pencerelerin bulunması durumunda güçlendirilmiş camlar kullanılmalı, parmaklık vb. tedbirler alınmalıdır.

3.2. Çevresel Kontroller

Bilgi sistemleri doğal veya insan kaynaklı felaketlere ve çevresel etkilere karşı korunmalıdır. Çevresel kontroller kapsamında ele alınması gerekli hususlara aşağıda yer verilmektedir: (DDO, 2020: 138)

• Bina çevresinde güvenliği tehdit eden yerler nereleri?

• Depreme karşı dayanıklılık testi yapılmış mı?

• Yangın, sel, deprem gibi felaket durumunda yapılması gereken eylemler neler? Acil durumda aranacaklar listesi var mı?

• Sistem odası yerleşimi yapılırken hangi konular dikkate alınmıştır?

• Sistem odası yedekli enerji hattı var mı?

• Sistem odası topraklama ölçümleri ne sıklıkla yapılıyor?

• Sistem odası/veri merkezi nem, sıcaklık ve duman kontrolü nasıl yapılmaktadır?

• Ortam koşullarının izlemesi yapılmakta mıdır?

• Sistem odası iklimlendirme için kullanılan klima yedekli mi, özellikleri nelerdir?

• Teçhizatların ve destekleyici altyapı hizmetleri(UPS, jeneratör, klima vb.) periyodik bakımları sağlanıyor mu?

• Kablolama güvenliğini sağlamak için uygulanan kontroller nelerdir?

Çevresel kontroller kapsamında, bilgi sistemlerinde olası hasarların ve faaliyetlerin kesintiye uğramasının önüne geçmek amacıyla en önemli fiziksel korumanın gerektiği tesis sistem odası/veri merkezi olmaktadır. Bu bağlamda, azaltılması gerekli çevresel risklerin doğal ve insanların neden olduğu afetler ile birlikte ortam koşulları kaynaklı olduğu görülmektedir. Genel olarak; sistem odasının stratejik olarak yerinin belirlenmesi, ortam koşullarının gerçek zamanlı izlenmesi, iklimlendirmenin yapılması, yangınlara karşı güvenliğin sağlanması, su sızıntılarına karşı önlemlerin alınması, elektrik kesintilerine karşı kontrollerin uygulanması gerekmektedir. Bu hususlara ilişkin detaylar aşağıda açıklanmaktadır: (ISACA, 2019: 253)

• **Sistem Odasının Yerinin Belirlenmesi**

Su baskını ve yangın ihtimalini azaltmak için sistem odasının yerleşiminde mümkün mertebe su ve gaz borularının geçtiği güzergahlarda olmaması göz önünde bulundurulmalıdır. Bu yönde; mutfak, tuvalet, havalandırma kanalları ve üniteleri, sulu yangın söndürme sistemleri, doğalgaz ve yanıcı bileşenleri depolandığı yerler, atık su gideri, kağıt depoları vb. mekanlardan uzak olacak şekilde sistem odasının konumlandırılmasına dikkat edilerek bu ortamlardan kaynaklı oluşabilecek risklerden kaçınılmış olacaktır. Yangın, duman ve su hasarı riskini azaltılması açısından; sistem odasının bina içinde orta katlarda konumlandırmanın en iyisi olduğunu belirten araştırmalar bulunmaktadır. Su baskını riskinin özellikle en alt ve en üst katta daha fazla olduğu söylenebilir. Deprem riskine karşı çok yüksek katlarda sistem odası tesis edilmemelidir. Bodrum katta sistem odası konumlandırılmışsa, sel ve su baskınlarına karşı teçhizatları koruyabilecek ek tedbirler düşünülmelidir. Bunun yanında; dış ve çevresel tehditlere karşı binanın yerinin belirlenmesi sürecinde civarda tehlike arz edebilecek diğer kuruluşların faaliyetleri de göz önünde bulundurulmalıdır.

• **İklimlendirme kontrolü**

Bilgi sistemleri donanımlarının kullanım ömürleri, performansları açısından belirli sıcaklık ve nem ortamında çalışmaları gerekmektedir. Bu bağlamda; sistem odasında sıcaklık ve nemin kontrolü hassas kontrollü (havanın yükseltilmiş taban altına üflenmesi) klimalar kullanılarak sağlanmalıdır.

Klimalar yedekli olarak çalıştırılmalı ve sistem odasının büyüklüğüyle odaya yerleştirilecek bilgi sistemleri donanımlarının yoğunluğu ve oluşabilecek ısı göz önünde bulundurularak kapasite planlamaları yapılmalıdır. Sistemler tarafından, üretilen sıcaklık ve nem verisi gerçek zamanlı izlenmelidir. Mevcut değerler belirlenen aralık dışına çıktığında uyarı verecek otomatik alarm mekanizmaları oluşturulmalıdır. Dünya standartlarına uygun bir sistem odası sıcaklığı 21°C (+/-1), nem oranı ise %50 (+/-5) RH olarak kabul edilmektedir. (EKC Grup, n.d.).

- **Su ve Duman Algılama Sistemleri (Dedektörleri)**

Yangın, su baskını, duman tespiti için çevresel koşulları izleyen dedektörler güvenli alanlarda konumlandırılarak merkezi bir uyarı sistemi ile gerçek zamanlı gözlenmelidir. Dedektörlerin konumları, erken uyarı verebilecek şekilde planlanmalıdır ve yerlerinin belirli olması, kolaylıkla erişebilmek için etiketleme ve işaretleme yapılmalıdır. Düzenli aralıklarla çalışıp çalışmadıklarına, yeterli güç kaynağına sahip olup olmadıklarına dair kontrolleri yapılmalıdır. Örneğin, sistem odasında su sızıntılarına karşı yükseltilmiş zeminlerin altına ve drenaj deliklerinin yanına su dedektörleri yerleştirilmelidir. Benzer şekilde duman dedektörleri tesislerin genelinde yükseltilmiş zemin altıyla birlikte tavan döşemelerinin üstüne ve altına konumlandırılmalıdır. Dedektörler, suyu/dumanı fark ettikleri zaman sesli alarm konumuna geçmelidir.

- **Yangın Kontrol Panelleri**

Bir tesisin içerisindeki farklı alarm bölgelerinin kontrol edilmesi, devre dışı bırakılabilmesi, etkinleşen alarmların sessize alınması vb. alarm kontrol panelleri aracılığıyla gerçekleştirilir. Bu paneller, ayrı bir elektrik hattı ile beslenmeli, yetkisiz personelin erişimine karşı kontrollü bir ortamda bulundurulmalıdır. Güvenlik veya ilgili personelin her zaman erişimi sağlanmalı, yerel düzenlemelere ve gereksinimlere uygun olarak hava koşullarına dayanıklı bir kutuda bulundurulmalıdır.

- **Taşınabilir Yangın Söndürme Tüpleri**

Yangın söndürme tüpleri tesis genelinde stratejik yerlerde konumlandırılmalıdır. Yangın tüplerinin türleri, miktarları ve yerleri mevcut risklere göre belirlenmeli, yerlerinde işaretlenmeli ve düzenli kontrolleri yapılmalıdır.

- **Yangın Uyarı Butonları**

Yangın uyarı sisteminin otomatik mekanizmalar dışında insanlar tarafından manuel olarak da devreye girmesi sağlanabilir. Bunun için yangın uyarı butonları tesis genelinde özellikle yangın kaçış yollarında stratejik olarak tesis edilir (Binaların Yangından Korunması Hakkında Yönetmelik, 2007).

- **Yangın Söndürme Sistemleri**

Yangın söndürme sistemleri, tesislerde yangın sürecinde kullanılan sabit söndürme tesisatıdır. Yangın esnasında panik çıkmasını önleyecek, yangını söndürecek ve kimseye zarar vermeyecek şekilde tasarlanması, tesis edilmesi, çalışır durumda tutulması gerekir. Bu yönde; sistemin periyodik olarak kontrolleri ve testleri gerçekleştirilmelidir. Tesislerde çıkacak yangınları önleyebilecek kapasitede olması, bölümlere ayrılarak yangınlara bölgesel müdahale etme imkanı sağlaması, otomatik veya el ile devreye girerek fonksiyonunu yerine getirebilmesi gerekir. Yangını sınırlamak için yangın kapılarının kapatılması, itfaiyeye haber verilmesi, havalandırma kanallarının kapatılması, elektrikli cihazların kapatılması gibi mekanizmaları otomatik olarak tetiklemelidir (Binaların Yangından Korunması Hakkında Yönetmelik, 2007).

Yangın söndürme sistemlerinin bazı tiplerine aşağıda yer verilmektedir:

- Yağmurlama sistemleri (Sprinkler sistemleri); yangına erken tepki verilmesinin sağlanması, yangının kontrol altına alınması ve söndürülmesi için belirli bir süre içerisinde belirli bir alana belirlenen miktarda suyun boşaltılmasını sağlar. Bu kapsamda, yağmurlama başlıkları, borular, bağlantı parçaları ve askılar, tesisat kontrol vanaları, alarm zilleri, akış göstergeleri, su pompaları ve acil durum güç kaynağı gibi elemanlardan meydana gelir (Binaların Yangından Korunması Hakkında Yönetmelik, 2007). Yağmurlama sistemleri iki tipte olabilir:

o *Islak borulu yağmurlama sistemleri:* Su yangın esnasında anında kullanım için borularda hazır olarak bulunmaktadır. Bu minvalde, borularda meydana gelebilecek su sızıntıları nedeniyle teçhizatların zarar görme riski ortaya çıkmaktadır. Kuru tipe göre daha efektif ve güvenilir olarak kabul edilir.

o *Kuru borulu yağmurlama sistemleri:* Normal süreçte borularda su bulunmaz, su sızıntısı riski olmaz bu durumda. Yangın esnasında alarmın etkinleştirilmesiyle birlikte sistemin aktif hale geçmesi ve borulara pompayla su gönderilmesi gerekir. Borulardan su sızıntısı riski olmamakla birlikte kuru tipte sisteme su verilememesi riski bulunmaktadır. Bu yüzden daha az güvenilirdir.

• Gazlı yangın söndürme sistemleri; suyun söndürme etkisinin yeterli görülmediği ve uygun olmadığı durumlarda kullanılır. Her türlü gazlı söndürme sistemi kurulurken, kişileri uyaracak ve söndürme bölgesinin boşaltılmasını sağlayacak sesli ve ışıklı uyarılar temin edilmek zorundadır. Gazlı yangın söndürme sistemlerinde kullanılan gazların en sık karşılaşılanları aşağıda açıklanmaktadır:

o Halon gazı, ozon tabakasını incelten maddelere dair Montreal Protokolü ile çevreye verdiği zararlı etkilerden dolayı kullanımı yasaklanmıştır.

o FM-200, HFC-227 olarak da adlandırılan Halon gazına alternatif olarak ortaya çıkmış ısıyı gidererek yangını söndüren temiz bir söndürücü gazdır. Küresel ısınmaya etkisi olsa da, ozon tabakasının incelmesine neden olmazlar ve insanlar için zararsız olması nedeniyle en tercih edilen gazdır.

o Argonite, Argon ve Nitrojen (Azot) gazlarının karışımından oluşmaktadır. Çevre için güvenilir olmakla birlikte insan yaşamı için tehlikeli olabilir.

o Karbondioksit ortamdaki oksijeni gidererek yangını söndürür. Bu yüzden insan bulunan ortamlarda uygulanmamalıdır.

• **Kesintisiz Güç Kaynağı/Jeneratör**

Bilgi sistemleri ve destekleyici altyapı hizmetleri enerji kesintisine karşı korunmalıdır. Bilgi sistemlerini barındıran güvenli alanların elektrik beslemesi yedekli olacak şekilde kesintisiz güç kaynakları (UPS) tarafından sağlanmalı, kesintisiz güç kaynakları da jeneratör ile desteklenmelidir. Elektrik kesintileri büyüklüklerine ve süresine göre dört ana grupta ele alınabilir:

• Tam arıza (*karartma/blackout):* Fırtına, deprem gibi doğal afetler veya elektrik dağıtım şirketi kaynaklı tek bir bina veya geniş bir bölgeyi etkileyen elektrik kesintisi.

• Düşük gerilim/voltaj (*kısmi karartma/brownout*): Elektrik dağıtım şirketinin kabul edilebilir seviyelerde bir süre güç sağlayamaması. Bu durum teçhizatın zorlanmasına ve kalıcı hasarına sebep olabilir.

• Gerilimde kısa süreli değişimler: Bu kapsamda karşımıza çıkan anormallikler voltaj seviyesinde anlık düşüşler (*gerilim çökmesi/sag*), geçici yükselişler (*gerilim kabarması*/*surge*) ve gerilimde daha yüksek değerlerde ani sıçramalar (*gerilim sıçraması/spike*) olarak donanımlar üzerinde fiziksel hasarlara, veri kaybına ve veri bozulmasına neden olabilir.

• Elektromanyetik enterferans/girişim (EMI): Fırtına veya motorlar, floresan aydınlatma, radyo vericileri gibi elektrikli aletlerin oluşturduğu gürültü/parazit nedeniyle sistemler askıda kalabilir, çökebilir ve gerilimde yaşanan kısa süreli dalgalanmalarda ortaya çıkan benzer sorunlar oluşabilir.

Gerilimde mikrosaniyeler ve milisaniyeler seviyesinde gerçekleşen kısa süreli değişimler için *gerilim aşımı koruyucusu (surge protector) ve gerilim düzenleyiciler (voltage regulator)* kullanılarak cihazların hasar görme riski azaltılabilir. Gerilim aşımı koruyucular, voltaj yükselmelerine karşı koruma sağlarken gerilim düzenleyiciler hem anlık yükseliş hem de anlık düşüşlere karşı koruma sağlar. Kesintilerin süresi arttıkça bu cihazlar yeterli olmayacaktır. Bu manada, gerilimdeki bu tür anlık değişikliklere karşı korumalar UPS sistemlerde bulunmakla birlikte, üzerinden bulunan akülerin kapasitesine göre UPS'ler anlık kesintilerden saatlerce süren kesintilere kadar koruma sağlamak için kullanılabilir. Elektrik şebekesinde meydana gelebilecek daha uzun kesinti süreleri için bina

altyapısında bulunan veya taşınabilir cihazlar olarak dizel, benzin veya propan gibi kaynaklardan güç alan jeneratörler önlem olarak tesis edilmelidir.

Bu kapsamda sistem odasının enerji kesintilere karşı korunması için aşağıdaki hususlara dikkat edilmelidir: (DDO, 2020: 142)

- Sistem odasında cihazlara giden voltajın tutarlı olması için enerji ihtiyacı şebekeden değil UPS cihazlarından sağlanmalıdır.

- Sistem odasına gelen elektrik enerji hattının yedekliliği sağlanmalıdır. Sistemlerin en az iki farklı enerji kaynağına bağlantısı yapılmalıdır.

- Jeneratörler olası şebeke kesintilerine karşı yakıt deposu dolu ve yedekli şekilde kullanıma hazır tutulmalıdır.

- UPS cihazlarının ve jeneratörlerin periyodik bakım, ölçüm ve test işlemleri gerçekleştirilmeli ve kayıt altına alınmalıdır.

- **Acil Durum Eylem Planları**

Acil durum eylem planları hazırlanarak dokümante edilmeli ve test edilmelidir. Bu kapsamda yangın, deprem vb. doğal afetler için acil durum senaryoları oluşturulmalı; bu durumlarda tüm personelin yapması gerekenler belirlenmeli, acil durumda aranacaklar listesi güncel bir şekilde tutulmalıdır.

- **Acil Kapatma Anahtarı**

Sistem odasının enerjisinin acil durumlarda hızlı bir şekilde kesilmesi gerekebilir. Bu amaç için, acil kapatma anahtarları sistem odası içerisinde ve dışarısında kolayca erişilebilir şekilde tesis edilmelidir. Yetkisiz kişilerin erişimine karşı anahtarlar korunmalı, kamerayla izlenmeli ve yanlışlıkla etkinleştirmeyi önlemek için korumaya sahip olmalıdır. Benzer şekilde su, gaz ve diğer destekleyici altyapı hizmetlerini kesmek için kullanılan acil durum anahtarları ve vanalar acil çıkışların ve ekipman odaların yakınına konumlandırılmalıdır.

- **Kablolama güvenliği**

Güç kabloları, haberleşme kablolarından ayrılmalıdır. Elektriksel bir yangının oluşmasını ve yayılmasının önüne geçilmesi için yanmaya dayanıklı kablolar kullanılmalı ve bütün kablolar, yangına dayanıklı yükseltilmiş taban altında yer alan yapısal kablo kanallarından geçirilmelidir.

Ana binaya gelen enerji hattı elektrik kesintisi riskini azaltmak için iki farklı trafo merkezinden yedekli bir şekilde tesis edilmelidir.

Binanın topraklama kontrolleri yapılmalı ve kayıt altına alınmalıdır.

- **Yangına dayanaklı sistem odası**

Sistem odası duvarları ve zemini neme ve aleve dayanıklı yalıtım malzemeleri ile kapatılmalıdır. Bu duvarlar yükseltilmiş tavan ve zemin dahil sistem odasını açık alan kalmayacak şekilde çevrelemeli, yangını baskılamalı, yayılmasını önlemeli ve en az iki saatlik yangına dayanıklılık derecesine sahip olmalıdır. Sistem odasında kullanılan genel ofis malzemeleri de yangına dayanıklı olmalıdır.

Sistem odası yerleşkesinde depreme karşı dayanaklılık testi yapılmış olmalıdır. Bunun yanında, bina için yeterli koruma seviyesine sahip bir paratoner kullanılmalı, periyodik bakımları yapılmalı ve kayıt altına alınmalıdır.

- **Sistem Odasında Engellenen Faaliyetler**

Güvenli alanlarda çalışma kuralları oluşturulmalıdır. Bu kapsamda, teçhizatların hasar görmesine neden olabilecek faaliyetler yasaklanmalıdır. Örneğin, yiyecek ve içecek ile girilmesi, sistem odası içerisinde sigara içilmesinin yasak olduğu uyulması ve yapılması gerekli kurallarda belirtilmeli ve uygulanmalıdır.

Örnek Sorular

Soru 1: Aşağıdakilerden hangisi fiziksel kontroller kapsamında ele alınması gerekli hususlar arasında değildir?

A) Kritik bilgi sistemlerinin güvenli alanlarda bulundurulması

B) Kapalı devre kamera sistemiyle izleme

C) Ziyaretçilerin kuruma giriş/çıkış kontrollerinin yapılması

D) Sistem odasına yedekli elektrik hattı tesis edilmesi

E) Güvenlik personeli istihdam edilmesi

Cevap: D

Soru 2:

I. Yetkisiz fiziksel erişim

II. Ortam koşulları

III. Felaketler

Yukarıdakilerden hangisi/hangileri fiziksel ve çevresel kontrollerin temel amaçlarındandır?

A) Yalnız I

B) I, II

C) I, III

D) II, III

E) I, II, III

Cevap: E

4. AĞ GÜVENLİĞİ

Bir işletmenin ağ ortamı içerisinde transfer edilen bilgi potansiyel bir saldırı hedefidir. Bu sebepledir ki, kurumsal ağların ve ağları kullanan bilgi sistemlerinin gerek şirket içinden gerek şirket dışından gelebilecek tehditlere karşı korunması bilgi güvenliğinin sağlanması açısından önem arz etmektedir. Bu bölümde öncelikle bilgisayar ağlarına ilişkin temel kavramlar ve çalışma prensipleri sunulmakta, ağ güvenliği ile ilgili riskler ve ağları güvence altına almak için uygulanabilecek ağ güvenliği kontrolleriyle birlikte bilgi sistemleri ve ağ altyapısı unsurları olan kullanıcıların, iş istasyonlarının, sistem ve uygulamaların güvenliği üzerinde durulmaktadır.

4.1. Ağ Çeşitleri ve Topolojileri

Ağ, paylaşılan bir ortam aracılığıyla birbirleriyle iletişim kuran iki veya daha fazla uç nokta cihazı seti veya kümesi olarak tanımlanabilir. Bir ağ yapısı oluşturulmasındaki iki temel amaç uç noktalar arası bilgi paylaşımı yapılabilmesi ve ağa bağlı bir uç nokta donanımının ağdaki diğer uç noktaları tarafından kullanılabilmesidir (Anadolu Üniversitesi, 2018:3). Bu amaçlarla bir ağ ortamına bağlanabilecek uç nokta cihazlar denildiğinde ilk akla gelen bilgisayar, yazıcı, sunucu olmasıyla birlikte telefon, televizyon, araba, oyun konsolu, buzdolabı, oyuncak, ısıtma sistemi, kamera vb. iletişim ihtiyacı olan herhangi bir cihaz da eklenerek liste çoğaltılabilir (Davies, 2019).

Uç noktası cihazların; birbiriyle iletişim kurabilmek için uyulması gereken bir dizi kural veya standardı ifade eden ağ protokollerini desteklemesi, ağa bağlanabilmek için bir arayüze (NIC- network interface card) ve bir ağ işletim sistemine (NOS network operating system) sahip olması gerekir. Ağ protokolleri çerçevesinde, paylaşılan ortamda uç noktaları tanımlamak ve yerini belirleyebilmek için bilgisayar adı (hostname), IP adresi ve MAC adresi kullanılır. Ağ altyapısını oluşturan temel yapı taşları arasında anahtarlar, yönlendiriciler, kablosuz erişim noktaları, güvenlik duvarları vd. ağ donanımları yer alır. Bu bağlamda, bir takım öğelerden oluşan bir kümenin ağ olarak tanımlanabilmesi için aşağıdaki temel bileşenlere sahip olması gerekir: (Sosinsky, 2009)

- **Bağlı uç nokta cihazlar**

Ağa bağlanması gerekli bilgisayar, sunucu, yazıcı, mobil cihaz, depolama ortamı, nesnelerin İnterneti (IoT) cihazı vd.

- **Bağlantı yazılımı**

Ağ yazılımı uç noktaların işletim sistemlerinde, ağ kartlarında, ağ donanımlarında ağa bağlanması gerekli bütün sistemlerde bulunur.

- **Ağ donanımı**

Anahtarlar, yönlendiriciler, modemler, kablosuz erişim noktaları, güvenlik duvarları vd. ağ donanımları.

- **Fiziksel iletim ortamı**

Fiziksel iletim ortamı, bir elektromanyetik sinyali iletebilen herhangi bir ortamı ifade eder. İletim ortamı hava (radyo frekansı), metal (bakır veya koaksiyel kablo) veya cam (fiber optik kablo) olabilir (Solomon & Kim, 2021).

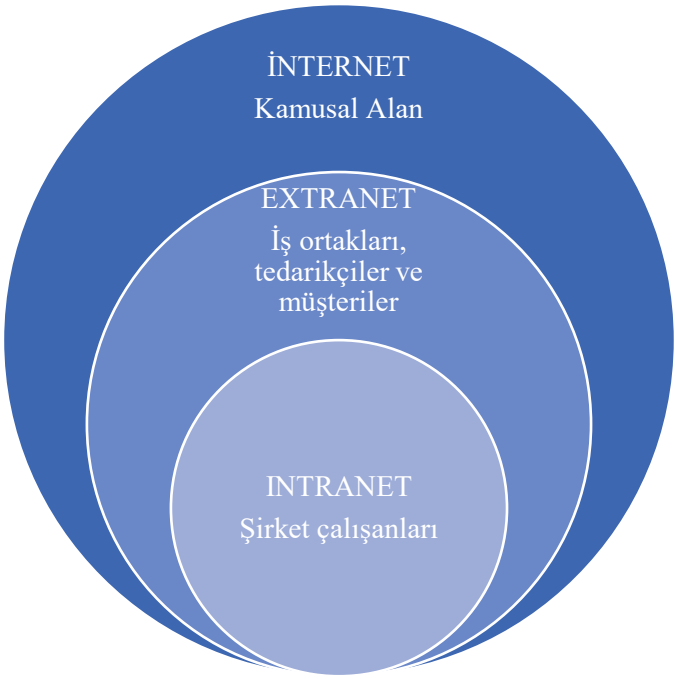
- **Bir adresleme sistemi**

İletişimin otomatik olarak yapılması için ağ ortamında bulunan unsurların her birinin adresleme gereksinimi sağlanır.

Ağ protokolleri ve bu detaylar ilerleyen bölümde ele alınacaktır ama öncelikle bu bölümde ağ çeşitlerine ve topolojilerine değinilecektir. Ağlar, sinyallerin taşındığı iletim ortamı, bant genişliği, iletişim protokolleri, ağ boyutu, topoloji, trafik kontrol mekanizması ve organizasyon amacı dahil birçok kritere göre sınıflandırılabilir (“Computer Network,” 2022). Bu kısımda öncelikle ağları organizasyon bakış açısıyla inceleyecek daha sonra topolojilerine ve coğrafi ölçeğe göre ağ çeşitleri açıklanacaktır.

4.1.1. Organizasyon Amacına Göre Ağlar

Ağlar genellikle onlara sahip kuruluşlar tarafından yönetilir. Şirketlerin özel kurumsal ağları bünyesinde intranet ve extranet birleşimi bir yapı oluşturulmakta ve İnternet'e erişim sağlanmaktadır ("Computer Network," 2022). (Şekil 4)



Şekil 4: Organizasyon amacına göre ağlar

İnternet

İnternet, *internet* (*inter-network*), *İnternet sunucuları ağı* (*WWW*) kavramları genellikle birbirine yerine kullanılmakla birlikte aralarında küçük farklar bulunmaktadır. Internetwork kavramı birden çok farklı türde bilgisayar ağının yönlendiriciler ve ağ geçitleri kullanılarak tek bir bilgisayar ağı oluşturacak şekilde bağlantısını ifade eder. İnternet ise ağların ağı olarak internetwork'ların en büyüğünü temsil eder ve aşağıdaki gibi tanımlanmaktadır:

"İnternet Mimarisi Kurulu (IAB) tarafından belirlenen protokoller setini ve İnternet Tahsisli İsimler ve Numaralar Kurumu (ICANN) tarafından yönetilen isim ve adres alanlarını paylaşan ticari, resmi, eğitimsel ve diğer bilgisayar ağlarından oluşan, dünya çapında birbirine bağlı tek sistem" ("Internet - Glossary | CSRC," n.d.).

Ağ tarihçesine bakıldığında, bugün bilinen şekliyle tasarlanan ilk ağ oluşumu Amerika Birleşik Devletleri Savunma Bakanlığı'na bağlı DARPA (İleri Savunma Araştırma Projeleri Dairesi) tarafından geliştirilen ARPANET (Gelişmiş Araştırma Projeleri Dairesi Ağı) ağıdır. İnternet, *TCP/IP dizisi* (TCP/IP suite) veya *İnternet iletişim kuralları dizisi* (IP protocol suite) ağ teknolojilerine dayanmaktadır. World Wide Web (WWW), Nesnelerin İnterneti (IoT), video aktarımı ve çok çeşitli bilgi hizmetlerini etkinleştirmek için fiber optik ağ omurgası ve bakır iletişimi kullanılır. İnternet servis sağlayıcıları (ISS) ve büyük kuruluşlar Sınır Geçit Protokolü (BGP) aracılığıyla adres alanlarının erişilebilirliği konusunda bilgi paylaşımında bulunarak dünya çapında yedekli bir iletim hattı oluşturmaktadır ("Computer Network," 2022).

Kısacası, internet baş harfi küçük yazıldığında farklı ağlar arası bağlantıyı (inter-network) ifade eder. İnternet baş harfi büyük harfle yazıldığındaysa şirketlerin kendi altyapılarında desteklediği özel kurumsal ağları dışında herkese açık olarak yer alan hizmetleri ve bu hizmetleri destekleyen altyapıyı ifade eder.

İnternet ile iç içe geçmiş bir diğer kavram da İnternet Sunucuları Ağı (WWW)'dır. WWW, son kullanıcılara hizmet veren İnternet sitelerini sağlayan sunucular kümesi olarak İnternet'in büyük bir

kısmı olsa da İnternet üzerinde sağlanan hizmetlerin sadece bir bölümüne karşılık gelmektedir. WWW, web sayfası olarak adlandırılan hiper metinlere (hypertext) dayanan bir protokoldür (Anadolu Üniversitesi, 2018:5). World Wide Web (WWW) kısaca *web* sözcüğü ile ifade edilir. İnternet üzerinde bilginin metin, grafik, ses ve video biçiminde karşılıklı alıp verildiği, kullanıcı dostu grafik arayüzleri yardımıyla kullanıcıların faydalanabildiği bir hizmettir (Davies, 2019).

Bu noktada, web'in farklı kısımlarını tanımlamak faydalı olacaktır. Web dünyasının 3 temel katmanı şu şekildedir: (Demchenko, 2022)

- **Surface Web (Yüzey ağ)**

Web dünyasının görünen kısmıdır. İnternet erişimi bulunan herhangi birisi tarafından Google, Yahoo, Bing gibi arama motorları kullanılarak ulaşılabilecek bütün İnternet siteleri ve sayfalarını içerir. Arama motorları sürekli olarak web sayfalarını web emekleyicileri (web crawler) marifetiyle dolaşarak bilgi toplamakta, her bir bağlantıyı dizinleyerek kullanıcıların aradıkları bilgileri kolayca ulaşmasını sağlamaktadır.

- **Deep Web (Derin ağ)**

Surface web herhangi bir web tarayıcısından erişilebilir, herkese açık bilgiyi içerirken deep web'teki bilgiye arama motorları üzerinden ulaşmak mümkün değildir. Çünkü bu bölümdeki içerik parola ile korunduğu veya özel sunucularda depolandıkları için arama motorları tarafından dizine eklenemez. Deep web'te yer alan sitelere örnekler aşağıdaki gibidir:

- Şirketlerin dahili platformları,
- E-posta servisleri,
- Devletle ilgili yasal bilgileri içeren siteler,
- İnternet bankacılığı,
- Eğitim ve kütüphane web siteleri,
- Bulut hizmetleri
- Tıbbi kayıtları bulunduran web sayfaları

Deep web, web dünyasının büyük bir çoğunluğunu oluşturmaktadır. Web'in bu bölümündeki içeriğe erişmek nispeten güvenli olmakla birlikte kullanıcı hesaplarında yer alan kişisel bilgiler saldırganlar tarafından hedef alınabilmekte bu anlamda bilgi güvenliği hususlarına dikkat edilmesi önem arz etmektedir.

- **Dark Web (Karanlık ağ)**

Dark Web (Dark Net), web dünyasında inşa edilmiş şifreli bir ağ içerisinde gizlenmek üzere tasarlanmış siteleri içerir. Karanlık ağdaki siteler çoğunlukla hatırlanması, tahmin edilmesi veya anlaşılması imkansız .onion uzantılı URL'lere sahiptir ve sadece özel programlar kullanılarak erişilebilir. Bu ağlara erişim yapan kullanıcıların kimlikleri gizlenebildiği ve yasa dışı faaliyetler desteklendiği için karanlık ağ olarak tanımlanmaktadır. Dark web sitelerinin içeriğine ilişkin aşağıdaki örnekler verilebilir;

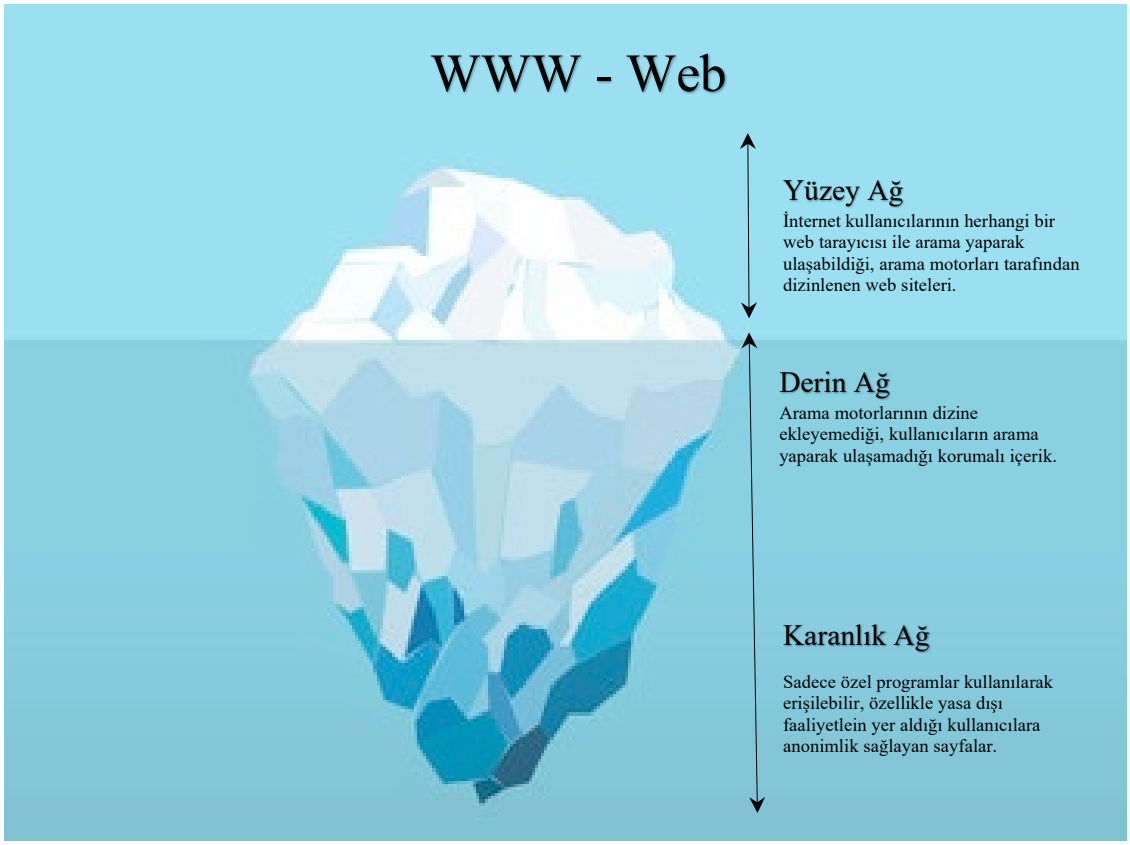
- Yasa dışı maddelerin satışı,
- Veri sızıntısı sonucu elde edilen bilgiler,
- Sahte teknolojik ürünler,
- İnsan kaçakçılığı,
- Kiralık katiller

Karanlık ağdaki her şey yasadışı da değildir. Devlet kurumları, askeri servisler, gazeteciler, insan hakları veya siyasi faaliyetler için gizli bir iletişim kanalı olarak da kullanılmaktadır. Anonimlik kazanmak isteyen herhangi bir aktör buralarda bulunabilir ve bu yönde karanlık sayfalara erişmenin en

yaygın yöntemi TOR (The Onion Router) tarayıcılarıdır. TOR tarayıcısı tarafından her içerik ve eylem şifrelenmekte ve dünya genelinde farklı ülkelerde bulunan TOR sunucuları üzerinden kullanıcı trafiği yönlendirilerek karanlık ağ üzerinde anonim ve gizli erişim elde edilmektedir (Albayrak, 2021)

Özetle; yüzey ağı arama motorları tarafından dizine eklenebilen ve herkese açık bilgilerden oluşan kısımdır. Derin ağda ise parola korumalı ve özel sunuculardaki barındırılan web tabanlı e-posta, çevrimiçi bankacılık, talebe bağlı video (VoD) vd. yaygın içerik yer alır. Bu tür içerik arama motorları tarafından dizine eklenemez ve yalnızca özel bir bağlantı, kullanıcı adı şifre ile erişim sağlanabilir. Karanlık ağdaki siteler de arama motorları tarafından dizine eklenemez ve genellikle yasadışı faaliyetler bulunmaktadır. Bu tür sayfalara erişmek için TOR benzeri anonimlik sağlayan tarayıcılar kullanılır.

WWW alt kısımları arasındaki fark en kolay şekilde Denis Shestakov'un buzdağı analojisiyle anlaşılabilir. Web, düzenli olarak ziyaret edilen en küçük parçası en üstte, görünmeyen büyük kısmı altta yer alan bir buzdağı gibidir. Yüzeyde çalışmak çoğunlukla güvenlidir ve derinliklere indikçe şüpheli faaliyetler artar.



Şekil 5: İnternet Sunucuları Ağı (World Wide Web)

Intranet

Intra eki içeride anlamına gelir ve Intranet için bu manada bir şirketin kendi içindeki ağ iletişimiyle ilgili olduğu söylenebilir. Intranet, ISACA terimler sözlüğünde (2018) şu şekilde tanımlanmaktadır:

"İnternet ve World Wide Web'in altyapısını ve standartlarını kullanan, ancak güvenlik duvarı kullanılarak yapılan engellemeler sayesinde halka açık İnternet'ten izole edilen özel bir ağ."

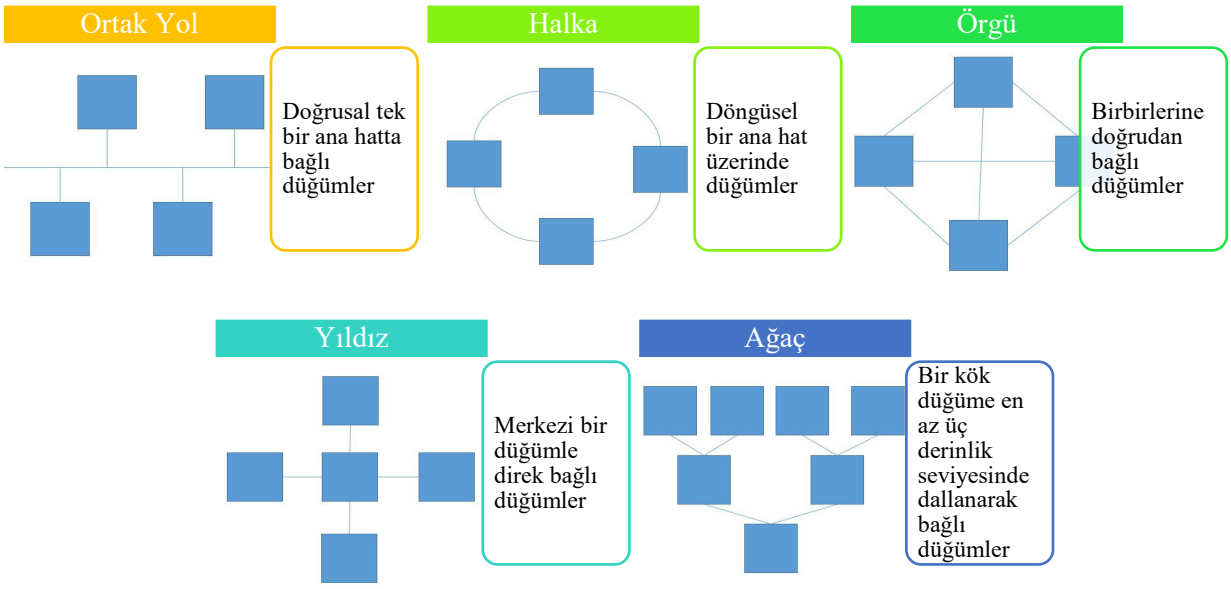
Bir şirketin intranet içinde sağlanan hizmetleri şirket ağıyla sınırlıdır ve intranet kullanımı yetkili kullanıcılar/cihazlar ile sınırlandırılır. Intranet bir şirketin dahili yerel alan ağıdır. Burada şirket içi kurumsal bilgi paylaşmak, ortak çalışma yapmak için dahili web sayfalarını barındıran en az bir web sunucusu yer alır. Bu yönde yerel alan ağındaki yönlendiricilerin arkasındaki bu hizmetlere şirket intraneti de denir ("Computer Network," 2022; Davies, 2019).

Extranet

Şirketler, kendi içerisindeki intranet iletişimini kontrol altında bulundurduğu şekilde belirli harici ağların intranet'e erişimini de kontrol eder. Şöyle ki; ağ bağlantıları üzerinden işlerin daha verimli hale getirilmesi için iş ortakları, tedarikçiler ve müşteriler ile güvenli bir şekilde bilgi paylaşımına izin verilmesi gerekir. Bu yönde extranet, harici ağlara sınırlı bağlantıları destekleyen özel ağları ifade eder. Bir extranet'te güvenilir ve yetkilendirilmiş harici unsurlara erişim izni verilir ve yalnızca ihtiyaç duydukları kaynaklarla sınırlı erişim sağlanır. Extranet'e ağ bağlantısı genellikle uzak alan ağı (WAN) teknolojileri aracılığıyla gerçekleştirilir. Extranet dijital sertifikalar ve alternatif kullanıcı kimlik doğrulaması yöntemleriyle birlikte trafiğin şifrelenmesine dayanır. Güvenlik ve mahremiyet sağlanabilmesi için sanal özel ağ (VPN) ve tünelleme mekanizmaları kullanılır ("Computer Network," 2022; Davies, 2019; ISACA, 2018).

4.1.2. Topolojilerine Göre Ağlar

Ağlar, kullandıkları topolojilere göre de sınıflandırılır. Ağ topolojisi, ağdaki uç noktaların birbirine nasıl bağlandığını gösteren bir ağın gerçek tasarımıdır. Bir ağ üzerindeki düğümlerin ve bağlantıların düzenlenme şekli, ağın performansına ve güvenilirliğine önemli derecede etki eder. Bir grafik teorisi uygulaması olarak ağ üzerinde iletişim kuran cihazların düğümler olarak modellendiği, düğümler arasındaki bağlantıların ise çizgilerle modellendiği bir ağın topolojik yapısı fiziksel veya mantıksal olarak tasvir edilebilir. Fiziksel topolojide, bir ağın çeşitli bileşenlerinin (ağdaki cihazların konumu ve kabloların kurulumu) yerleştirilmesi yer alır ve ağ fiziksel yapısı açısından tanımlanır. Mantıksal topoloji ise bir ağ içinde bilginin nasıl aktığını gösterir. ("Network Topology," 2022 ; "Computer Network," 2022)



Şekil 6: Ağ Topoloji Türleri

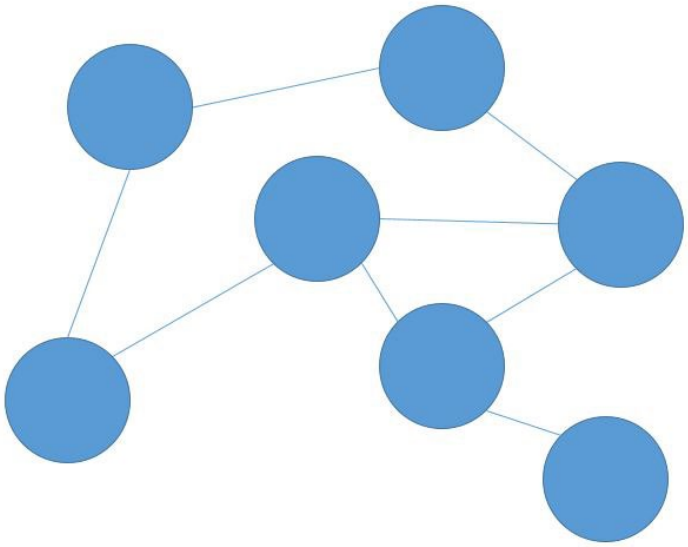
Fiziksel, mantıksal veya ikisinin birleşimi hibrit bir topoloji kullanılarak bir ağ tanımlanabilir. Bir ağın fiziksel ve mantıksal topolojileri aynı olabileceği gibi çoğunlukla tamamen farklıdırlar. Herhangi bir ağ tarafından kullanılan belirli bir topoloji; ağın hızından, iletişim kurmak için kullanılan protokollerden, ağ düğümünden veya bağlantı türlerinden bağımsız olarak aynı olabilir. Topoloji, yalnızca öğelerin birbirlerine göre düzenlenmesini ifade eder. Ortak Yol (Bus), Halka (Ring), Örgü (Mesh), Ağaç (Tree) ve Yıldız (Star) gibi çeşitli ağ topolojileri bulunmaktadır. Ağ topolojileri türlerinin açıklamalarına aşağıda yer verilmektedir: (Sosinsky, 2009)

Ortak Yol Topolojisi

Ortak yol (bus), iki veya daha fazla ağ düğümünü bağlayan ortak bir iletim ortamıdır. Örneğin, tek bir koaksiyel kablo üzerinde BNC konnektörlü ethernet kartlara sahip uç noktalarla bu ağ türü oluşturulur. Bu yapı, sınırlı sayıda düğüm ve mesafeler için kullanılmaktadır. Tanımlanmış bir hiyerarşi, merkezi bir düğüm yoktur. Aynı kablo, ağa bağlı bütün uç noktalar tarafından ortak kullanılacağı için toplam ağ kapasitesi aralarında bölünecektir ve hız düşük olacaktır (Anadolu Üniversitesi, 2018:5). Backbone (omurga) veya trunk (ana hat) bağlantılar doğrusal bir ortak yola örnektir. Bunun sebebi, verilerin tek bir veri yolu üzerinden bir uç noktadan diğerine hareket etmesidir. Şöyle ki, bir veri yolu üzerinde bir düğümden diğerine gitmesi gerekli veriler, gönderen düğüm tarafından öncelikle bir sonraki düğüme iletilmekte hedeflenen alıcısına ulaşana kadar verinin bir sonraki düğüme iletilmesine düğümler arasında sırasıyla devam edilmektedir.

Halka Topolojisi

Halka topolojisinde, ağdaki her düğüm iki komşu düğümle bağlanarak iletişim halinde bulunur ve ağdaki ilk ve son düğüm arasında bir bağlantı yapılarak döngü tamamlanır. Bir halka ağında her düğüm herhangi bir veri iletiminin hem başlangıç hem de bitiş noktasıdır ve alıcı sistem veriyi kabul edene kadar veri ağ içerisinde düğümler arası sinyal gönderiminde problemleri önlemek için aynı yönde hareket eder. İkili halka topolojileri, trafiği iki farklı yönde iletme veya ikinci halkayı hata dayanıklılığı (fault tolerance) için kullanma imkanı sağlar. Halka topolojisi örnek uygulamaları Token ring (Andıçlı halka), Arcnet (Benzeşik bilgisayarlar ağı), Token bus (Andıçlı ortak yol), FDDI (Fiber dağıtılmış veri arayüzü) ağlarıdır. Andıçlı halka ortamında bir andıç (3 bayttan oluşan bir veri paketi) düğümler arası dolaşır ve bu andıca sahip düğüm veri gönderme hakkına sahiptir. Bu şekilde andıçla halkanın tümü dolaşılarak düğümlerin sırayla veri göndermesi sağlanır (Anadolu Üniversitesi, 2018:8).



Şekil 7: Kısmen bağlı örgü topolojisi

Örgü Topolojisi

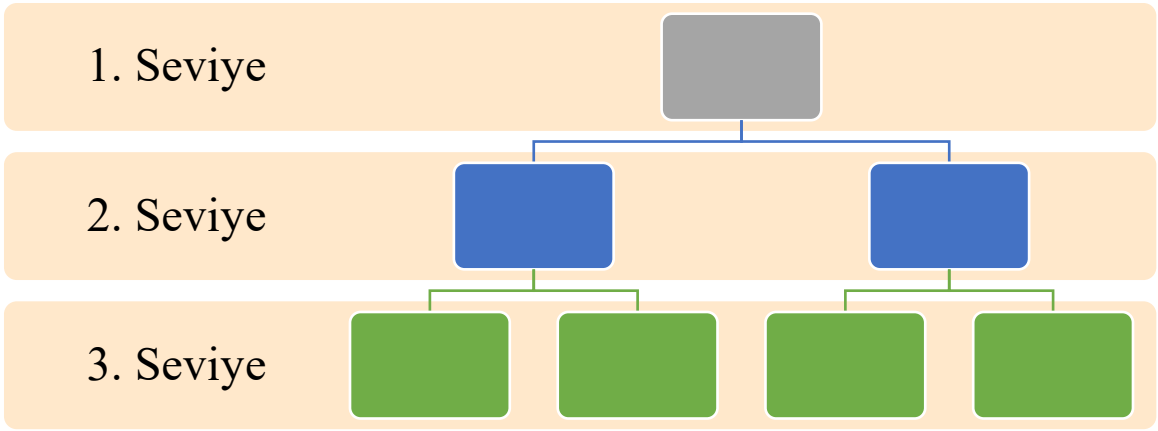
Örgü topolojisinde, düğümler arasında noktadan noktaya bağlantılarla bir ağ oluşturulur. Ağdaki her düğüm bütün düğümlere noktadan noktaya bağlıysa "tamamen bağlı örgü topolojisi", düğümler birbirine sıkı bir şekilde tamamen bağlı değilse "kısmen bağlı örgü topolojisi" olarak ifade edilir. (Şekil 7) İnternet, kısmen bağlı örgü topolojisine bağlı bir örnektir. Örgü şeklinde yapılan bağlantılar, ağda hatalı düğümlerin olmasına karşı düğümler arası veri akışında alternatif yollar sunarak yedeklilik sağlar. Örgü topolojisinde veriler düğümden düğüme yayılarak ya da takip edilecek güzergah yönlendirmeyle belirlenerek iletilir.

Ağaç Topolojisi

Ağaç topolojisinde en üst seviyede merkezi kök (gövde) düğümün yer aldığı, hiyerarşik bir yapı oluşturulur. Merkezi düğümün üstünde bir başka düğüm yoktur. Kök düğüme ikinci seviyede bir veya daha fazla düğüm ile bağlantı yapılır. Bu düğümler de üçüncü seviyede bir veya daha fazla düğüm ile bağlanarak kollara ayrılır. Bir ağın bu şekilde bir ağaç topolojisinde kabul edilebilmesi için en az üç seviyesi bulunmalıdır. Ağaç topolojisi, Şekil 8'de şematik olarak gösterildiği üzere en tepede yer alan kökten düğümlerin dallandığı tersten bir ağaç şeklinde çizilir.

Bir ebeveyn düğüme bağlı alt düğüm sayısı dallanma faktörü olarak tanımlanır. Dallanma faktörü 1 olduğunda doğrusal bir topoloji ortaya çıkar. Ağlarda genellikle simetrik dallanma uygulanır. Bu durumda dallanma faktörü 2 veya daha fazla olacaktır.

Ağaç topolojisinde bir dezavantaj, hiyerarşide yukarı çıktıkça veri iletişimiyle ilgili düğümlerin yükünün artmasıdır. Diğer yandan arama algoritmaları doğrusal veya örgü topolojilerinden ziyade hiyerarşik ağaç yapısında daha verimli çalışır. Bu nedenle; dosya sistemleri, veritabanları ve dizin sistemleri bu topolojileri kullanır. Bunun için, düğümlerde depolanan verilerin indekslenmesi gerekir. Arama algoritmasıyla ağaçta bir alt seviyeye inilerek diğer dallardaki düğümler devre dışı bırakılır, aranmalarına gerek kalmaz.



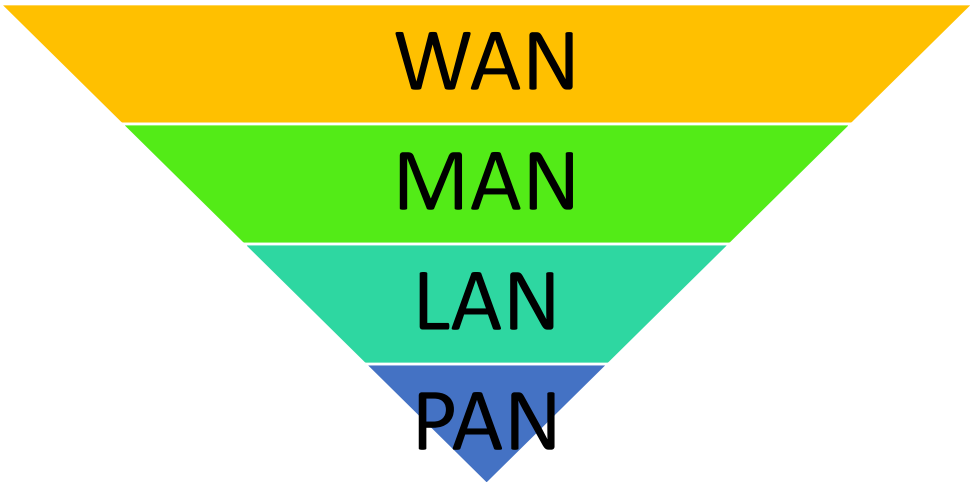
Şekil 8: Ağaç Topolojisi

Yıldız Topolojisi

Yıldız topoloji, merkezde dağıtıcı bir düğüme direkt bağlı düğümlerle oluşturulur. Ağ üzerinde dolaşan veri, merkezi düğüm üzerinden akmalıdır. Günümüzde ağ ortamlarında çoğunlukla bu topolojiden faydalanılmaktadır. Şirketlerin iç ağlarında merkezi düğüm olarak bir kenar anahtar (switch) kullanılırken, kablosuz ortamlar için erişim noktası (Access point) cihazları kullanılmaktadır. Bütün düğümler merkezi düğüm üzerinden iletişim kurduğu için, ağın performansı merkezi düğümün kapasitesine bağlı olmaktadır. Merkezi düğümden her bir düğüme kablolama maliyeti artırmakla birlikte her bir düğüme ayrı kablolamayla düğümler arası veri iletişiminin aynı anda ve daha hızlı bir şekilde yapılmasına imkan sağlanmaktadır (Anadolu Üniversitesi, 2018:8).

4.1.3. Coğrafi Ölçeğe Göre Ağlar

Ağlar; coğrafi kapsama alanına göre temelde kişisel alan ağı (PAN), yerel alan ağı (LAN), büyükşehir alan ağı (MAN), geniş alan ağı (WAN) şeklinde adlandırılır. Büyüklüklerine ve amaçlarına göre değişik ağ türlerinin açıklamalarına aşağıda yer verilmektedir (Anadolu Üniversitesi, 2018:5; "Computer Network," 2022)



Şekil 9: Büyüklüklerine göre ağlar

PAN (Kişisel Alan Ağı)

Kişisel alan ağı kısa mesafelerde örneğin bir oda içerisinde, bir kişinin yakın çevresindeki kişisel cihazlarla oluşturulan ağlardır. Telefon, tablet, yazıcı, fotoğraf makinesi, saat, kulaklık, dizüstü bilgisayar, fare, klavye vb. arasında iletişim kurmak ve İnternet gibi farklı bir ağa bağlanmak için kullanılır. Genellikle kişisel alan ağında bağlantı USB, Firewire gibi veri yollarıyla sağlanır. Kablosuz kişisel alan ağı ise (WPAN); Bluetooth, IrDA, ZigBee gibi ağ teknolojileriyle kurulabilmektedir.

LAN (Yerel Alan Ağı)

Ev, okul, iş binaları vb. sınırlı alanlarda bulunan uç nokta cihazlar tarafından oluşturulan ağdır. Fiziksel olarak yakın mesafede örneğin bir şirketin ofisinde bulunan bilgisayar ve diğer uç nokta cihazların bağlanarak bir araya geldiği ve veri alışverişi gerçekleştirdiği ortam yerel alan ağıdır. Yerel alan ağı, birçok uç noktası cihazı ve protokolü destekler. Kablolu ortam için Ethernet, kablosuz yerel alan ağları (WLAN) için ise Wi-Fi teknolojileri yaygın olarak kullanılmaktadır. Yerel alan ağlarının en temel özelliği yerel hizmetlere ihtiyaç duyulan yüksek hızlarda ve sürekli bir şekilde erişime imkan sağlamasıdır. Uygulama ve depolama sunucularının, yazıcıların ve faks makinelerinin ortak kullanımı, e-posta ve anlık mesajlaşma uygulamalarının kullanımı, İnternet erişimi gibi birçok uygulama ve hizmete erişim sağlanır. Bu ölçekte LAN ve WLAN kavramlarıyla birlikte, üniversitelerin veya kurumsal şirketlerin yerleşkelerini birbirine bağlayan CAN(Kampüs alan ağı) ve sunucuları depolama cihazlarına bağlamayı sağlayan SAN (Depolama alan ağı) gibi kullanım amaçlarına göre farklı şekilde tanımlanan ağ çeşitleri de yer almaktadır.

MAN (Büyükşehir Alan Ağı)

Genellikle yerel alan ağlarının bir araya getirilmesiyle metropol şehir büyüklüğünde bir coğrafi alanı kapsayan ağlardır. Dolayısıyla, yerel alan ağından daha büyük bir ağ yapısıdır ve coğrafi kapsamı LAN ile WAN arasında kalır. LAN'ları İnternet gibi daha geniş ağlara bağlar. Yerel alan ağlarının birbirine bağlanması fiber optik kablolar veya kablosuz ağ ortamları üzerinden gerçekleştirilir ve ağlar arası geçiş yönlendici (router) ağ cihazlarıyla sağlanır. MAN ağlarında FDDI, ATM, SMDS kullanılan bazı ağ teknolojileridir.

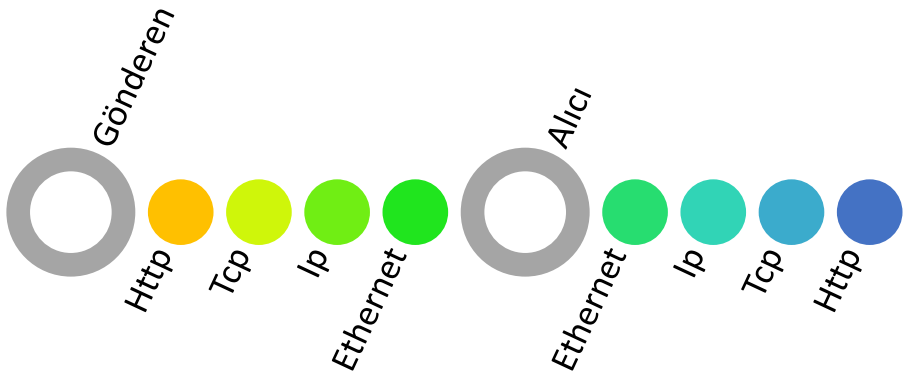
WAN (Geniş Alan Ağı)

Geniş alan ağı, LAN ve MAN ağlarının bir araya geldiği, ülkeler çapında geniş bir coğrafi alanı hatta kıtalararası mesafeleri kapsayan en geniş alan ağıdır. Geniş alan ağları kablolar, telefon hatları ve hava dalgaları gibi birçok ortam türünü birleştiren bir iletişim kanalı kullanır. Dünya üzerinde bulunan bütün cihazların birbirine bağlandığı en geniş alan ağı İnternet'tir. İnternet ortamında bulunan uzak bir cihaz üzerinden güvenli bir şekilde yerel alan ağına bağlanma, yerel alandaki bir cihaz gibi veri alışverişinde bulunabilme imkânı sağlayan ağ türü Sanal özel ağ (VPN) olarak adlandırılmaktadır.

4.2. Ağ Modelleri ve Protokolleri

Bu bölümde, katmanlı ağ mantığı üzerine geliştirilmiş OSI ve TCP/IP ağ modelleri ve TCP/IP protokol takımı işlenecektir.

Ağ yığını (network stack – protocol stack), bir bilgi sisteminde başlayıp başka bir bilgi sisteminde biten ağ işlemlerini tanımlamak için kullanılan bir mimari modeli ifade etmektedir. (Şekil 10) Bir bilgi sisteminde oluşturulan veri, ağ ortamında alıcı bilgi sistemine giderken farklı katmanlardaki protokollere göre işlenmektedir. Bu yönde, ağın bir seviyesinden diğerine iletişime olanak sağlayan endüstri standartlarının gelişmesine izin vermek ve cihazları ve hizmetleri standartlaştırmak için geliştirilmiş en önemli iki ağ modeli *OSI modeli*(Açık Sistemler Bağlantısı) ve İnternet ortamını oluşturan *TCP/IP modelidir*. Her iki model de, farklı türdeki ağ cihazlarını, hizmetlerini ve yazılımlarını, bir dizi mimari katmana ayırır. Bu şekilde yapılan katman tanımları ve aralarındaki ilişkiler modern ağ teknolojilerinin kategorize edilip ele alınması için bir araç sağlamaktadır (Sosinsky, 2009).



Şekil 10: İnternet Protokol Yığını

Ağ iletişiminin başarılı bir şekilde gerçekleşmesi için gereken işlevleri açıklayan bu modellerden TCP/IP modeli bir protokol modeli, OSI modeli ise referans modeli olarak birbirinden farklılaşır (Cisco Networking Academy, 2022).

Protokol modeli

Bu model türü, veri ağında iletişim kurulabilmesi için gerekli fonksiyonelliği sağlayan protokoller kümesinin (protokol takımı) yapısıyla uygun oluşturulur. Bu anlamda, TCP/IP protokol takımının her bir katmanında yer alan işlevleri açıkladığı için TCP/IP modeli bir protokol modelidir.

Referans modeli

Referans modeli geliştirilmesindeki temel amaç, ağ iletişiminde gerekli işlevlerin ve süreçlerin daha iyi anlaşılmasına yardımcı olmaktır. Bu yönde, işlevlerin nasıl hayata geçirileceğine odaklanılmadan sadece her bir katmanda tamamlanması gerekli işlevlerin tanımı yapılır. Dolayısıyla bir referans modeli olarak OSI, hangi katmanda hangi protokolün çalışması gerektiğini kesin olarak belirleyecek şekilde uygulamaya yönelik olmaktan ziyade kavramsal bir modeldir.

4.2.1. OSI Modeli

Ağ modelleri ve protokolleri ile ilgili standartlar, aşağıdaki gibi çeşitli kuruluşlar tarafından geliştirilmekte, yayınlanmakta ve sürdürülmektedir:

- **Amerikan Ulusal Standartlar Enstitüsü (ANSI):** ANSI, ürün ve hizmetler için standartlar oluşturan bir kuruluştur.

- **Uluslararası Standartlar Teşkilatı (ISO):** ISO standartları, veri iletişimi konularında geliştirilmektedir.

• **Uluslararası Telekomünikasyon Birliği (ITU):** Telekomünikasyon Standartları Sektörü (ITU-T), Radyokomünikasyon Sektörü (ITU-R), Telekomünikasyon Kalkınma Sektörü (ITU-D) grupları tarafından iletişim standartları geliştirilir. ISO, ITU üyesidir.

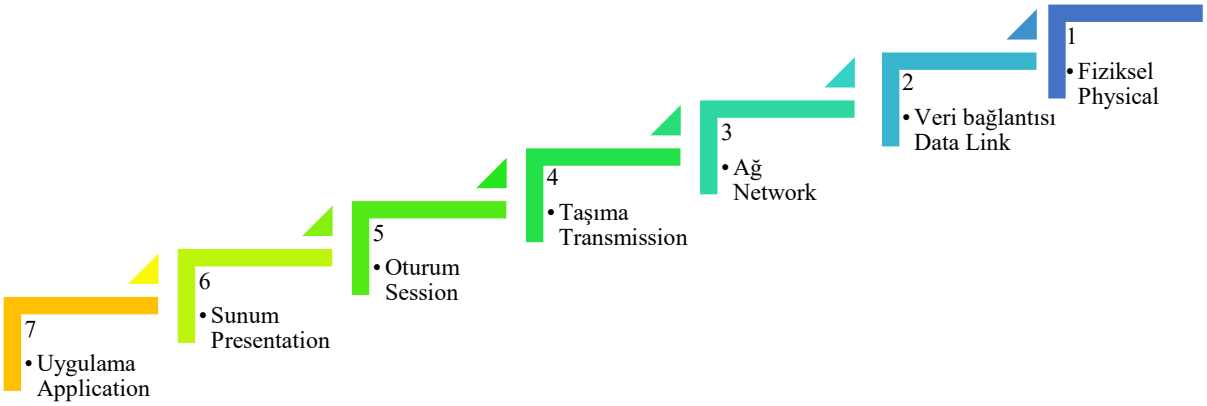
• **İnternet Mühendisliği Görev Gücü (IETF):** IETF, TCP/IP ile İnternet protokollerini tanımlayan kuruluşlarla işbirliği içinde İnternet standartlarını oluşturur.

• **Elektrik ve Elektronik Mühendisleri Enstitüsü (IEEE):** IEEE, kablolu ve telsiz iletişim standartları için ana kuruluştur.

• **Depolama Ağı Endüstrisi Birliği (SNIA):** SNIA, FC (fiber channel), iSCSI, yüksek hızlı Ethernet vd. depolama ağı standartlarını tanımlar.

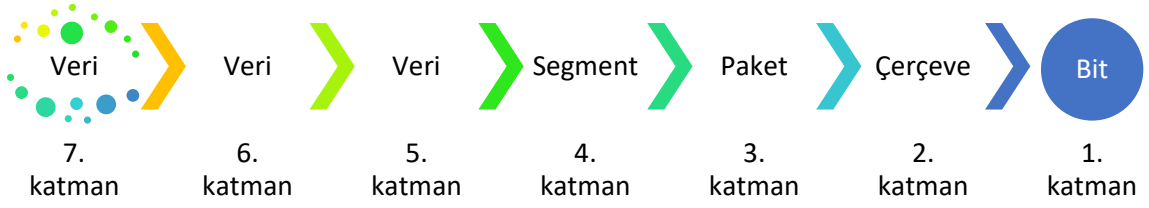
• **Dünya Çapında Ağ Konsorsiyumu (W3C):** W3C, HTML ile ilgili standartları ve Web sunucuları tarafından kullanılan protokolleri tanımlar. (Sosinsky, 2009)

Açık sistemler bağlantısı (OSI) referans modeli ISO'nun Açık Sistemler Bağlantısı Projesi tarafından veri ağı tasarımı (network design), işleyiş özellikleri (operation specifications) ve sorun giderme (troubleshooting) için kullanılmak üzere geliştirilmiştir (Cisco Networking Academy, 2022). Bu model ağ iletişimini yedi katmana ayırır: (Şekil 11)



Şekil 11: OSI modeli katmanları

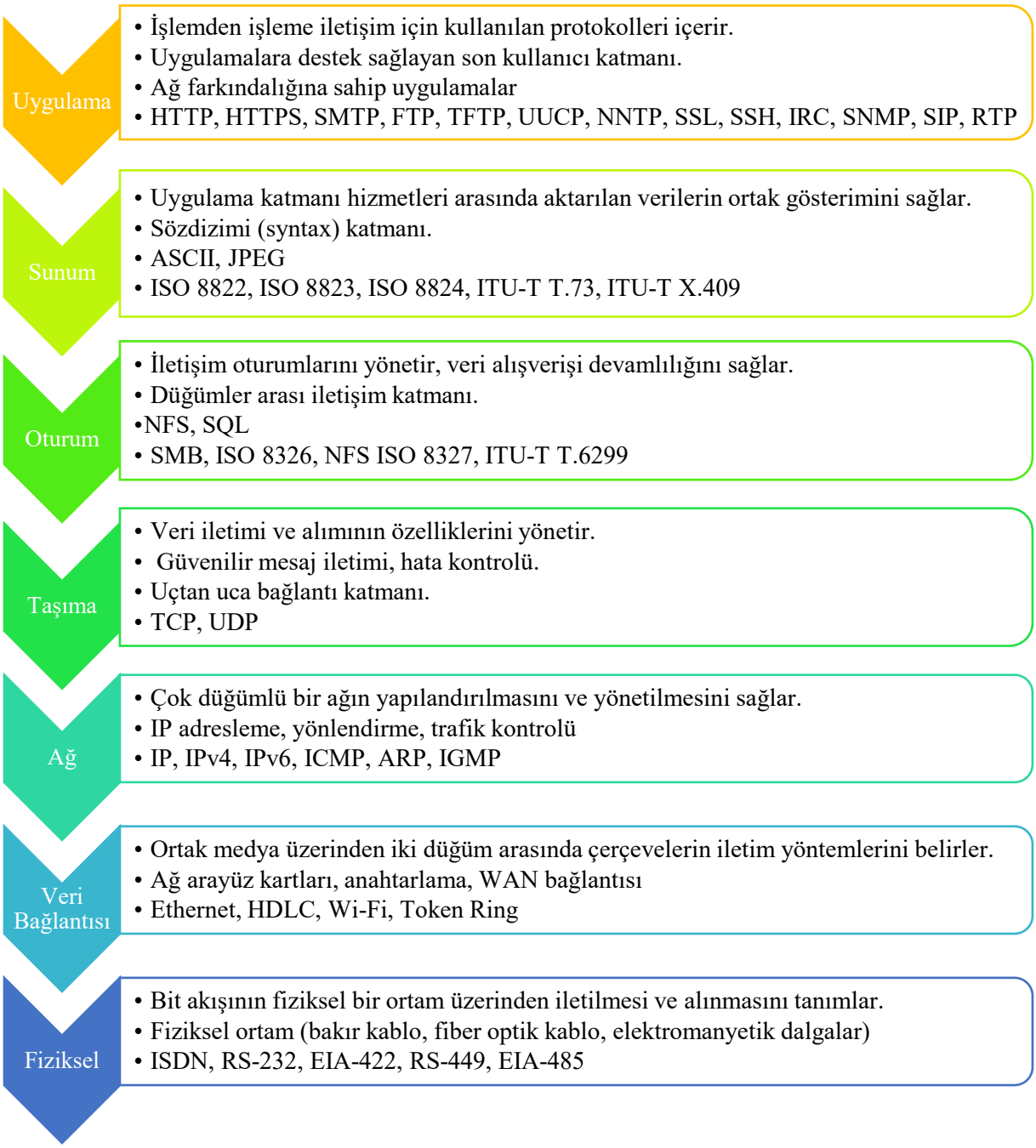
OSI modelinin katmanları fiziksel katman 1. katman olacak şekilde yukarı doğru numaralandırılmaktadır. Temelde ilk dört katman donanımla ilgiliyken, kalan diğer katmanlar yazılımla ilgilidir. Bu katmanlar kullanılarak verilerin bir ağda nasıl hareket ettiği görselleştirilebilir. Ağda düğümler arası iletişim sürecinde gönderilecek veriye yukarıdan aşağı her katman tarafından daha fazla veri eklenirken, verinin alıcısı tarafında aşağıdan yukarı doğru sırasıyla bu bilgiler çıkarılıp kullanılır (Sosinsky, 2009). Bu akışta, genel olarak *Protokol Veri Birimi* (PDU) terimiyle ifade edilen katmanlar arası aktarılan bilgiye her katmanın kendisi tarafından anlamlandırılabilen farklı isimler verilmektedir. PDU; katman 7 ile 5 arasında *veri* (data), katman 4'te *segment* (datagram), katman3'te *paket* (packets), katman 2'de *çerçeve* (frame), katman 1'de *bit* olarak adlandırılır. (Şekil 12)



Şekil 12 OSI katmanları protokol veri birimleri

OSI modelinin uygulama katmanında uygulamalarla ağ arasındaki ağ bağlantısı yönetilir. Verilerin alıcı sistemde işlenebilecek bir formatta olmasıyla birlikte verilerin şifrelenmesi ve sıkıştırılması sunum katmanında sağlanır. Oturum katmanı, oturumların kontrol edilmesinden sorumlu olarak gönderen ve alıcı sistemler arasında bağlantıları sürdürür. Taşıma katmanı tarafından uç nokta cihazlar arasındaki iletişimler için verilerin bölümlere ayrılması, aktarılması, yeniden birleştirilmesi hizmetleri tanımlanır. Ağ katmanında ise, veri iletiminde kullanılacak adresleme hizmeti sağlanır. Veri bağlantı katmanı donanım adreslerini yönetir ve ortak bir medya üzerinden iletilecek verinin formatını belirler. Fiziksel katman ham bit akışının sinyaller şeklinde iletimi için gerekli kablo, ışık hüzmesi, radyo frekans vd. fiziksel iletim ortamı tanımlar.

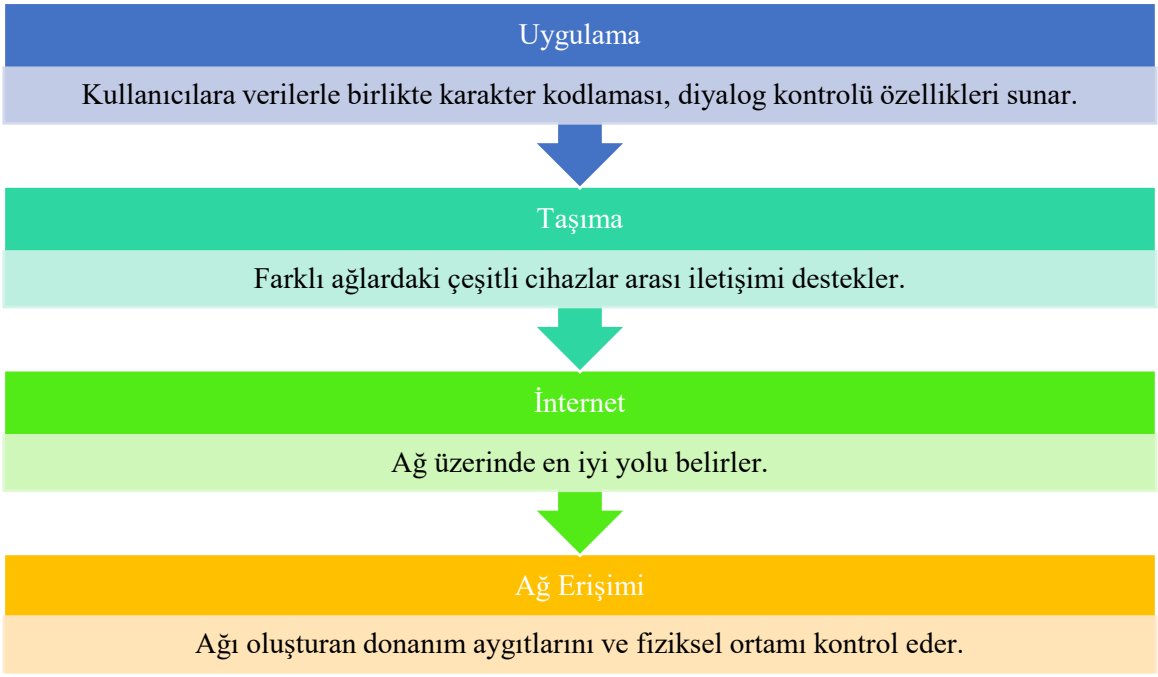
Şekil 13'de OSI modeli katmanlarıyla ilişkili bileşenlere ve her bir katmanda kullanılan çeşitli protokol örneklerine yer verilmektedir (Anadolu Üniversitesi, 2018:9; Sosinsky, 2009; Cisco Networking Academy, 2022; J. S. Beasley & Nilkaew, 2021).



Şekil 13: OSI referans modeli

4.2.2. TCP/IP Modeli

Ağlar arası iletişim için 1970'li yılların başlarında oluşturulan ilk katmanlı model, *İnternet modeli*, genellikle TCP/IP modeli olarak adlandırılır. Bunun nedeni; ağ iletişimi için kullanılan TCP/IP protokol takımının bu modelin yapısını oluşturmasıdır. TCP/IP modelinde iletişimin başarılı olması için gerçekleşmesi gerekli aşağıdaki gibi dört işlev tanımlanır: (Şekil 14) (Cisco Networking Academy, 2022)



Şekil 14: TCP/IP modeli katmanları

TCP/IP modeli, aktarım ve veri formatı için 3 farklı protokol kullanılır. TCP (İletim Kontrol Protokolü) ve UDP (Kullanıcı Datagram Protokolü) protokolleri taşıma katmanı protokolleriyken, IP protokolü (İnternet Protokolü) İnternet katmanı protokolüdür. TCP protokolü, İnternet üzerindeki sistemler arasında nasıl bağlantı kurulacağını tarif eder. UDP protokolü ise, bağlantısız veri iletişimiyle nasıl çalışılacağını açıklar. Paketlerin iletim için nasıl formatlanacağını, IP protokolü tanımlar (Sosinsky, 2009)

TCP/IP ve OSI modelleri karşılaştırması

OSI ve TCP/IP modelleri üzerinden katmanlı ağ mantığı anlaşılmaya çalışıldı. Bu katmanlı modellerle sağlanan temel avantajlar aşağıdaki gibidir: (Cisco Networking Academy, 2022)

- Belirli katmanlarda çalışan protokoller üzerinde tanımlı bilgilerden ve üstteki ve alttaki katmanlara tanımlı arayüzlerden faydalanılır. Bu sayede protokol tasarımına yardımcı olur.
- Farklı üretici ürünleri birlikte çalışabilir ve rekabet sağlanır.
- Teknoloji değişikliklerinden en az şekilde etkilenilir.
- Ağ işlevleri ve yeteneklerini tanımlamak için ortak bir dil sağlanır.

TCP/IP modeliyle OSI modeli yan yana koyulduğunda görüleceği üzere göze çarpan ilk fark, farklı katman sayılarına sahip olmalarıdır. (Şekil 15) TCP/IP modelinin dört katmanlı yapısına karşı OSI modeli yedi katmanlı oluşturulmuştur. Bilindiği üzere, İnternet iletişim kuralları dizisi 1970'lerde geliştirildi ve İnternet'in atası ARPANET ağı çalışmalarında kullanıldı. OSI modelinin daha öz bir biçimi olarak nitelendirilebilecek TCP/IP modeli, bu şekilde uygulamaya dayalı TCP/IP ağ teknolojileri geliştirildikten sona dört katman olarak şekillendi. OSI modelinin yedi katmanlı olmasının temel nedeniyse, IBM şirketinin ağ endüstrisini kontrol edeceği varsayımından kaynaklanmaktadır. IBM

tescilli SNA (Systems Network Architecture) mimarisinin yedi katmanlı bir yapısı bulunmaktaydı ve 1970'li yıllarda OSI modeli çok fazla değişiklik yapılmadan SNA teknolojisine uygulanabilecek şekilde inşa edildi.

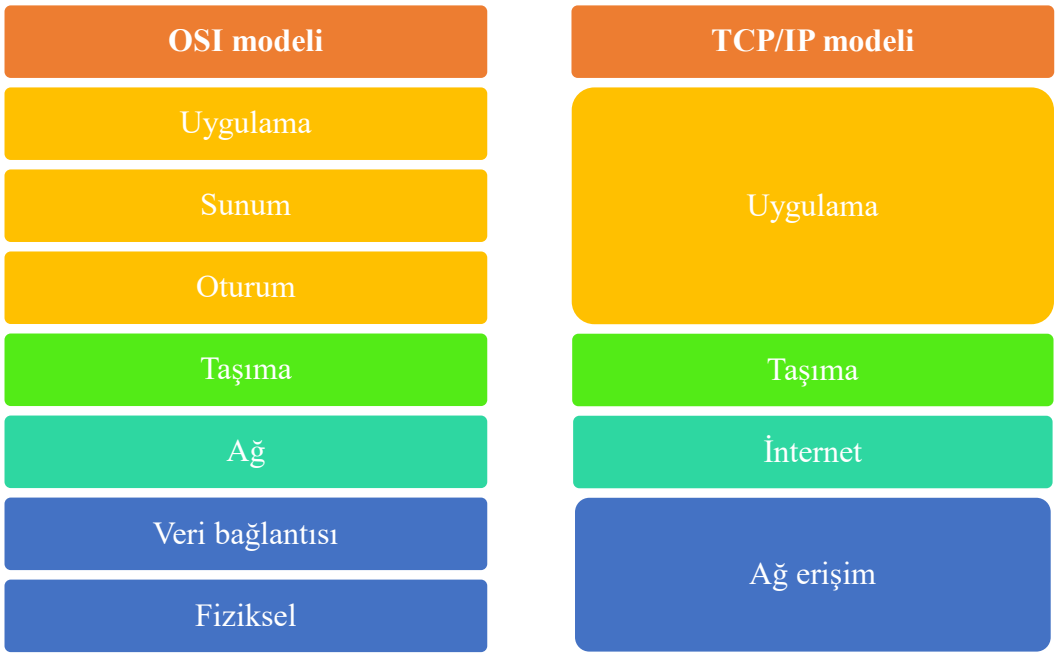
TCP/IP protokol takımını oluşturan protokoller, OSI modeli açısından açıklanabilir. TCP/IP İnternet katmanında gerçekleşen işlevler, OSI modelinin ağ katmanında yer almaktadır. Bununla birlikte, taşıma katmanı işlevselliği her iki model arasında aynıdır. Temel farklılıklar ağ erişim ve uygulama katmanlarındadır. TCP/IP modeli ağ erişim ve uygulama katmanları OSI modelinde ayrık işlevleri açıklamak için daha fazla katmana bölünmüştür. Diğer bir deyişle, her iki model taşıma ve ağ katmanlarının üstündeki ve altındaki katmanlarla nasıl ilişkili olduklarına göre farklılık gösterir: (Cisco Networking Academy, 2022)

• Mesajları adresleyen ve ağ üzerinden yönlendiren protokolleri tanımlayan OSI modeli katman 3 doğrudan TCP/IP modeli İnternet katmanına eşleşir.

• Kaynak ve hedef ana bilgisayarlar arasında düzenli ve güvenilir veri iletimi sağlayan hizmetleri ve işlevleri açıklayan OSI modeli katman 4, TCP/IP aktarım katmanına eşleşir.

• OSI modeli 5,6,7 katmanları ağlarda çalışan uygulamalar üretmek için uygulama yazılımı geliştiricileri için referans olarak kullanılırken, TCP/IP modelinde tek bir uygulama katmanı son kullanıcı uygulamalara belirli özellikleri sağlayan protokolleri içerir.

• OSI 1,2 katmanları fiziksel ortama erişim için gerekli prosedürleri ve bir ağ üzerinden veri göndermenin fiziksel yollarını tanımlar. TCP/IP protokol takımında, bu iki katmana karşılık gelen ağ erişim katmanında fiziksel bir ortam üzerinden iletim yapılırken hangi protokollerin kullanılacağı veya iletim için sinyal kodlama yöntemleri belirtilmemektedir. Bu yönüyle, bu iki katmana atıfta bulunulurken yaygın olarak OSI modeli kullanılır.



Şekil 15: OSI ve TCP/IP modelleri karşılaştırılması

Yıllar geçtikçe, her iki modelde ağ endüstrisinin kelime dağarcığını geliştirmiştir. Bununla beraber, her ikisi de gerçek dünya ağlarına uygulamalarda kusurlar içerir. TCP/IP baskın standart haline gelen protokol takımıyla gerçek ürün ve teknolojilerde ifade bulurken; OSI modeli ağ iletişimini anlamak için bir soyutlama olarak kalmış, ürünler tarafından önemli ölçüde desteklenmemektedir.

TCP/IP modeli, çok sayıda ürün tarafından desteklenmekle birlikte, başka protokolleri destekleyen ağlara uygulanabilecek şekilde genel olmadığı için eleştirilmiştir. Arayüzlerin, hizmetlerin ve protokollerin modele nasıl entegre edileceği açıkça belirtilmemektedir. Örneğin sunum ve oturum

katmanlarının bulunmaması, ağ erişim katmanının bir arayüz olarak daha doğru bir şekilde tanımlanmaması. Bu da pratikte; üstünkörü, geçici çözümler içeren protokol standartları ortaya çıkarmıştır.

OSI modelini benimseyen ağlarda bile özellikle oturum ve sunum katmanları hiç doldurulmasa bile çok az doldurulur. Diğer taraftan, veri bağlantısı ve ağ katmanları çok işleve ve hizmete sahiptir ve bu katmanlar birkaç alt katmana ayırılarak çözülebilecek durumdadır. OSI katmanının karmaşıklığının bir kısmı da bazı anahtar teknolojileri tek katman yerine farklı katmanlara dağıtmasından kaynaklanır. Gerçek dünyada, aynı cihaz içinde OSI modelinin birkaç katmanı kapsanarak bu sorunların üstesinden gelinmektedir.

Sonuç olarak, bu ağ modellerini fazla ciddiye almamak en iyisidir. OSI, teorik tartışmalarda kullanılan esnek bir model sağlasa da, TCP/IP modeli ürünlerde hayat bulsa da her iki model de doğrudan gerçek dünya ağlarına uygulanamaz. TCP/IP protokollerine dayalı olan, OSI referans modelinden daha az katman kullanan ve OSI referans modelinin karmaşıklığını bir şekilde azaltan hibrit modeller mevcuttur. (Sosinsky, 2009)

Ağ modelleriyle ilgili, bölümün başında Şekil 10'da İnternet protokol yığınında da gösterildiği üzere, tipik bir ağ üzerinde iki uç nokta cihaz arasındaki iletişim belirli protokoller üzerinden sağlanmaktadır. Yığında, her bir üst düzey protokolün alt düzeydeki protokollerin hizmetlerine bağlı olduğu katmanlı bir hiyerarşi gösterilmektedir. Ağ iletişimi temel olarak istemci-sunucu ilişkisi içerir. Örneğin web gezintisi, e-posta gönderme, video izleme vd. her gün başkalarıyla iletişim kurmak ve düzenli olarak işlerimizi yerine getirmek için kullandığımız birçok ağ hizmeti bu mimariye dayanmaktadır. *Sunucu* terimi burada ağa bağlı diğer uç noktalara (istemci) bilgi veya hizmet sağlayan bir yazılım uygulaması çalıştıran bilgi sistemlerini ifade etmektedir. İstemci-sunucu sistemlerin temel özelliği istemcinin sunucudan bir istekte bulunması ve sunucunun gerekli işlevleri yerine getirerek istemciye yanıt vermesidir.

Web sunucusu ve istemcisi arasında bilgi alışverişi sürecinde mesajların alındığından ve anlaşıldığından emin olmak için TCP/IP modelinin her bir seviyesinde kullanılan protokoller aşağıdaki gibidir: (Cisco Networking Academy, 2022)

- Uygulama katmanında HTTP protokolü tarafından istemci-sunucu arasındaki web isteklerinin ve yanıtlarının biçimi tanımlanır.

- Aktarım katmanında TCP protokolü tarafından sıra dışı alınan paketlerin sıralanması veya eksik paketlerin yeniden gönderilmesi sağlanarak, uygulama verisinin yer aldığı IP paketlerinin güvenilir ve eksiksiz bir şekilde karşı tarafa ulaşması yönetilir.

- İnternet protokolü (IP) alt katmanda, mantıksal adreslemeyi yapar. TCP segmentleri hedefe yönlendirmek üzere gerekli bilgileri içerek şekilde paketler halinde kapsüllemekten sorumludur.

- Ağ erişim katmanı fiziksel ağda kullanılan ortam türüne ve iletim yöntemlerine bağlıdır. Ethernet protokolleri verilerin çerçeve şeklinde nasıl biçimlendirildiğini ve kablolu ağ üzerinden nasıl iletildiğini tanımlar.

Şimdi bu kapsamda, kullanıcıların ağlar ve İnternet ile etkileşime girdiği ağ uygulama hizmetleriyle birlikte iletişimleri için gerekli TCP, UDP, IP, ARP, Ethernet vd. temel ağ protokolleri ele alınacaktır.

4.2.3. Uygulama Katmanı Hizmetleri

Ağ uygulama hizmetleri; kullanıcılar tarafından IP adresleri yerine alan adları kullanılması, web sunucularından bilgi alınması, e-posta gönderip alınması, dosya paylaşımı yapılması gibi olanaklar sağlar. Ağ servisleri için kullanılan protokollerden bazıları DNS, SSH, SMTP, POP, IMAP, DHCP, HTTP'dir. İstemci-sunucu sistemleri tarafından sağlanan bu hizmetler tek bir sunucu tarafından veya birkaç sunucu üzerinden sağlanabilir. Bununla birlikte, bir sunucu üzerinde birden fazla hizmet de çalışıyor olabilir. Bu yönde, sunucu ağ üzerinden bir mesaj aldığında, istemci tarafından hangi hizmetin istendiğini belirleyebilmesi gerekir. Bu yönde TCP/UDP protokolleri kullanılarak istemciden gelen talepler iletilirken talep edilen protokoller ve hizmetler bir *port numarasıyla* (bağlantı noktası)

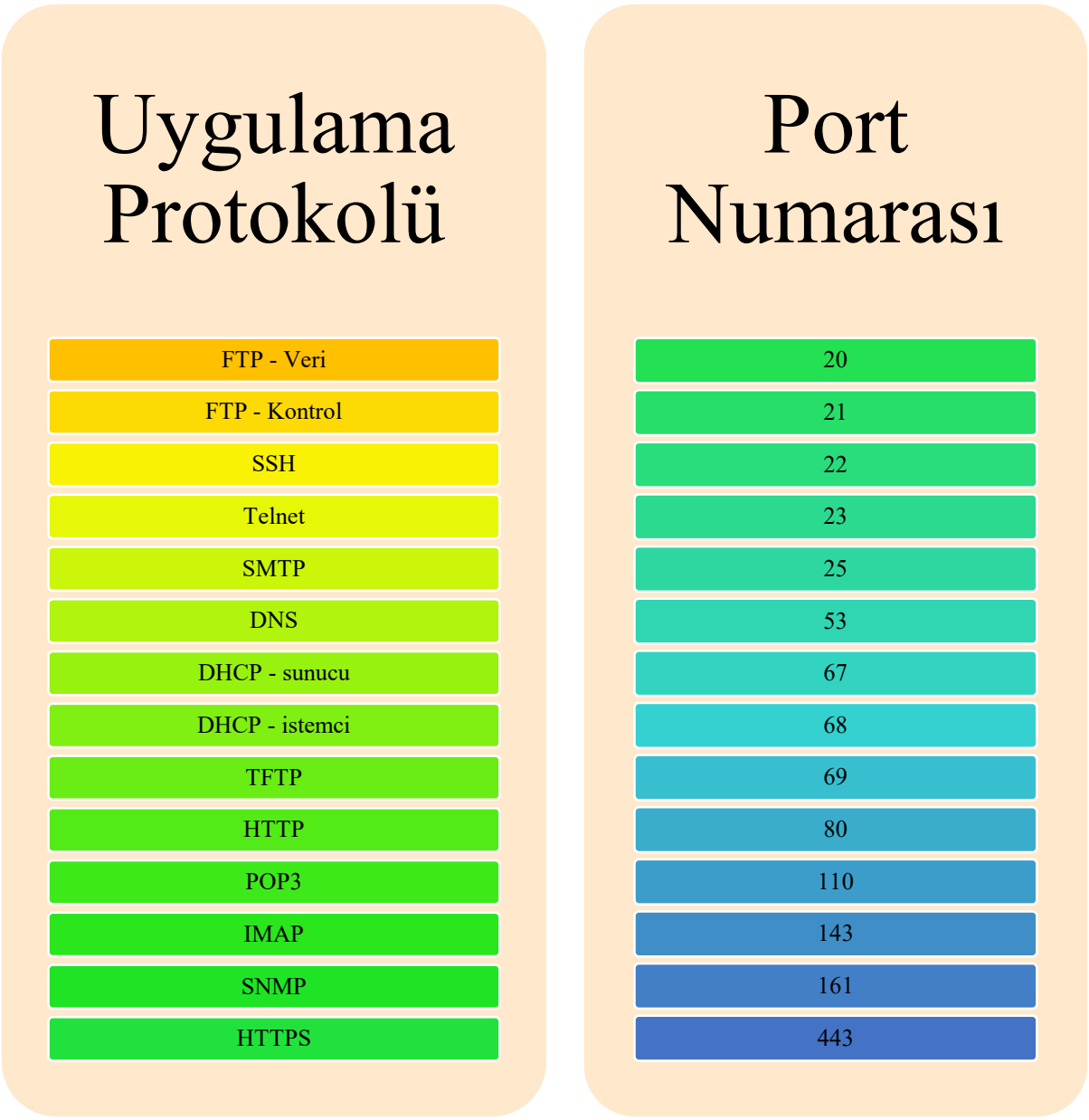
tanımlanır. Örneğin, HTTP web sunucularına istek göndermek için 80 portu kullanılır. Bağlantı noktaları ICANN (İnternet Tahsisli Sayılar ve İsimler Kurumu) tarafından yönetilir. Bağlantı noktaları 1-65535 aralığında yer alır ve aşağıdaki gibi üç kategoriye ayrılır: (Cisco Networking Academy, 2022)

- **İyi bilinen bağlantı noktaları (Well-known ports):** 1-1023 aralığındaki bağlantı noktaları yaygın kullanılan ağ uygulamalarına ayrılmıştır. IANA tarafından yönetilir.

- **Kayıtlı bağlantı noktaları (Registered ports):** 1024-49151 arasındaki bağlantı noktaları hedef ve kaynak bağlantı noktası olarak kullanılabilir. IANA tarafından kontrol edilmez ama kayıt defterinde listelenir.

- **Özel bağlantı noktaları:** 49152 ile 65535 aralığındaki bağlantı noktaları IANA'ya kayıtlı değildir. Herhangi bir uygulama tarafından kullanılabilir. Uygulamalar tarafından bağlantı noktası güvenliği sağlamak için bağlantı sırasında rastgele seçilir ve bağlantı kapandığında önemini kaybeder.

İyi bilinen bağlantı noktaları ve bunlarla ilişkili uygulamaların bazılarının açıklamalarına aşağıdaki yer verilmektedir: (Şekil 16) (Solomon & Kim, 2021; Davies, 2019; Cisco Networking Academy, 2022)



Şekil 16: Uygulamalar ve port numaraları

- **DNS (Domain Name System – Alan Adı Sistemi)**

TCP/IP ağlarda iletişim IP adresleri üzerinden sağlansa da birçok uygulama yaygın olarak ana bilgisayar adı (hostname) / tam alan adı (FQDN) kullanır. Kullanıcıların İnternet hizmetlerine erişimi esnasında IP adresleri yerine alan adlarını kullanmasına imkan sağlayan protokol, etki alanı adı sistemi DNS'tir. DNS sunucusu üzerinde bir etki alanındaki bilgisayar adlarıyla IP adresleri eşleştirilmesi liste halinde tutulur ve istemcilerden gelen sorgulara, alan adlarına karşılık gelen IP adresi bilgileri bulunarak cevap verilir. İstemcilerin DNS sunucularıyla iletişim kurabilmesi için istemci tarafında cihaz IP adresi yapılandırmasıyla birlikte DNS sunucuları IP bilgilerinin de tanımlanması gerekir. Bu sayede, IP adresi yerine örneğin bir web sunucunun adına sahip olunması yeterli olmaktadır. Kullanıcı web sayfasına erişmek istediğinde arka planda tanımlı DNS sunucularına 53 numaralı bağlantı noktası üzerinden istekte bulunabilmekte ve gerekli adres çözümlemesi yapılarak istemci-sunucu arasında başarılı bir şekilde iletişim kurulmaktadır.

Ağ adlandırma ve ad çözümleme işlemleri İnternet'in başlangıç evresi Arpanet'te "hosts" adlı özel metin dosyaları kullanılarak her sistem üzerinde kendisi tarafından gerçekleştirilmekteydi. Ağdaki sistemler üzerinde yer alan bu dosyalarda her sistemin adıyla eşleşen IP adresleri yer alıyordu. Bu bilgilerin güncellenmesi manuel olarak yapılıyor ve günlük olarak gece saat 02:00'de bütün bilgisayarlara yansıtılıyordu. Bu dosyalar günümüz bilgisayarlarında hala bulunsa da İnternet büyüdükçe ağlar arasında çalışacak daha esnek bir adlandırma sistemi ihtiyacına karşı etki alanı sistemi oluşturuldu. Etki Alanı Sistemi (DNS), ana bilgisayar adlarının IP adresleriyle ilişkilendirilmesine izin veren hiyerarşik bir adlandırma sistemidir. Dağıtılmış bir ad çözümleme hizmeti sağlar (Solomon & Kim, 2021).

DNS çalışma mekanizması, en üst seviye DNS sunucularının işlerinin bir kısmını yan DNS sunucularına devretmesi, onların da işlerinin bir kısmını diğer sistemlere devretmesi şeklinde yetki devrine (delegation) dayanır. Alan adları ve IP adresleri depolama işinin hiyerarşik yapısının en tepesinde dünyaya dağılmış 13 adet DNS kök sunucusu (root servers) yer alır. Herkese açık İnternet üzerinde erişilebilen her alan adı bu sunucular tarafından kapsanmaktadır. Bu sunucuların tek görevi, ad çözümlemesini daha özel DNS sistemlerine devretmektir. Hiyerarşide kök sunucuların altında yer alan ve yetkiyi devralan sunucular TLD sunucuları (top level domain servers) olarak adlandırılır. ICANN, üst düzey alan adı (TLD) oluşturma yetkisine sahiptir. Orijinal üst düzey alan adları .com, .org, .net, .edu, .gov, .mil ve .int şeklinde olmakla beraber bunlara uluslararası ülke kodu adları ve diğerleri eklenmektedir. TLD sunucuları da etki alanına özgü DNS sunucularına yetki verir. Etki alanına özgü DNS sunucularında etki alanı zone'ları altında etki alanı sunucularının adları ve IP bilgileri tutulur ve ilgili etki alanı için yetkili sunucu olarak talep eden istemcilerle kayıtlı bilgiler paylaşılır. (Beasley & Nilkaew, 2021)

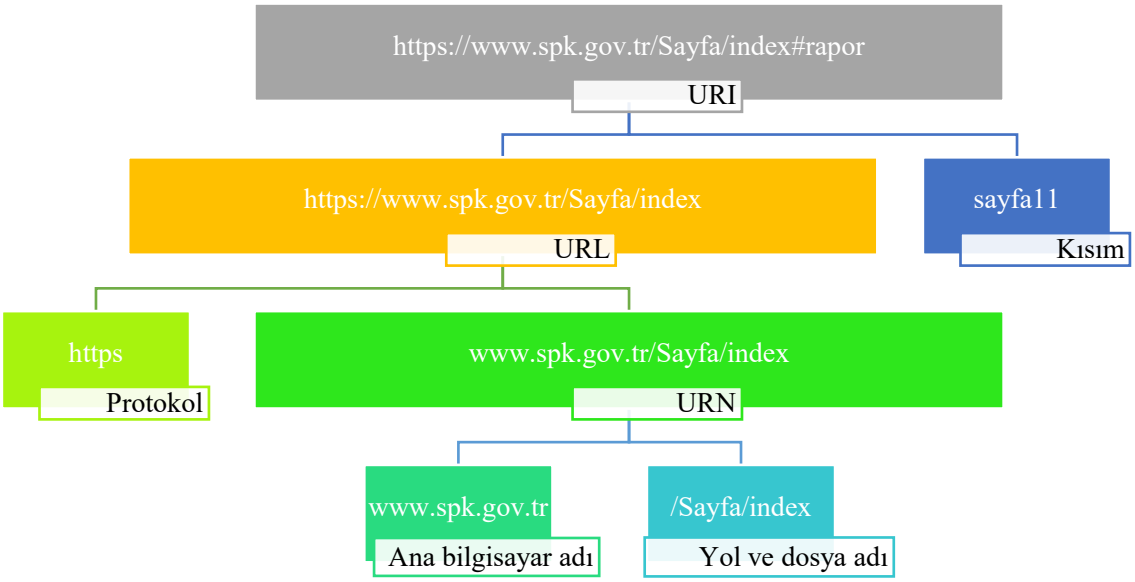
- **HTTP (Hyper Text Transfer Protocol - Hiper Metin Transfer Protokolü)**

Web istemcileri ve web sunucuları arasında iletişim HTTP ve HTTPS (**s**ecure-güvenli) protokolleri üzerinden gerçekleştirilir. Web kaynakları ve hizmetleri *URI* (Tekbiçimli Kaynak Tanımlayıcısı) ile tanımlanır. URI, belirli bir ağ kaynağını tanımlayan karakter dizisi, aşağıdaki kısımlardan oluşmaktadır: (Cisco Networking Academy, 2022)

- Protokol/şema (protocol /scheme)
- Ana bilgisayar adı (hostname)
- Yol ve dosya adı (path and file name)
- Kısım (fragment)

URI ile birlikte Şekil 17'de görüldüğü üzere karakter dizisindeki farklı kısımları içeren *URN* (Tekbiçimli Kaynak Adı) ve *URL* (Tekbiçimli Kaynak Konumlayıcı) kavramları da bulunmaktadır. URN, protokole atıfta bulunmadan bu karakter dizisinin ana bilgisayar adıyla birlikte yol ve dosya adı kısımlarını tanımlamaktadır. URL ise protokol kısmını da içerir ve ağdaki belirli bir kaynağın ağ konumunu belirtir. Genellikle tarayıcılarda (web istemci yazılımı) kullanılan bir web adresini oluşturan karakter dizisini tanımlamaktadır.

Bu çerçevede, İnternet'te bir web sayfasını ulaşmak için tarayıcıda bir URL bilgisiyle web sunucusuna istekte bulunulur. URL; kullanılan protokolü (HTTP), erişilecek sunucunun alan adını ve sunucu üzerinde erişilmek istenen kaynağı belirler. Web sunucusunun IP adresinin bulunması için DNS protokolü devreye girer. İstemci web sunucusunun IP adresini aldığında, web sunucusu üzerindeki kaynağa erişmek için web sunucusunun 80 numaralı bağlantı noktasına istekte bulunur. Bu istek HTTP isteği olarak karşı tarafa iletilir. Sunucu ise, 80 portu isteğine HTML gibi özel biçimlendirme dilleri kullanılarak kodlanan web sayfası içeriğini cevap olarak gönderir. İstemci tarafında tarayıcı web sayfa içeriğini sunucudan gelen biçimlendirmeye göre gösterimini sağlar.



Şekil 17: URI, URN ve URL

• DHCP (Dynamic Host Configuration Protocol – Dinamik Ana Bilgisayar Konfigürasyon Protokolü)

Ağlar için otomatik IP adresi yapılandırma protokolüdür. TCP/IP ağlarda cihazların iletişim kurabilmesi için IP adresine sahip olması gerekir. Bir ağda cihazların IP adresi statik olarak ayarlanabilmektedir. Bununla birlikte, DHCP protokolü her bir cihazı teker teker yapılandırmak zorunda kalmadan son kullanıcı cihazların IP adreslerini ve diğer yapılandırma bilgilerini (varsayılan ağ geçidi, alt ağ maskesi, DNS sunucularının IP adresleri vd.) isteyip alabilmek için DHCP sunucusuyla iletişime geçebilmesini mümkün kılmaktadır. IP yönetiminin DHCP sunucusu tarafından yapılması sayesinde, bir ağ ortamında cihazların aldığı tüm IP adreslerinin benzersiz olması sağlanır.

• SMTP (Simple Mail Transfer Protocol – Basit Posta Gönderim Protokolü)

E-posta sunucuları arasında e-posta gönderimi ve alımı protokolüdür. 25 numaralı bağlantı noktası e-posta gönderimine ayrılmıştır. E-posta istemcileri çoğunlukla POP3 ve IMAP protokollerini kullanır.

• POP3 (Post Office Protocol – Posta Ofisi Protokolü)

Bir e-posta sunucusu üzerinde posta kutusu olan kullanıcılar e-postalarına ulaşmak için bir e-posta istemcisi kullanır. İstemci 110 numaralı bağlantı noktası üzerinden e-posta sunucusu ile iletişim kurar. Kullanıcıya gelen e-postalar istemciye indirildikten sonra varsayılan olarak sunucu tarafında silinir.

• IMAP (Internet Message Access Protocol – İnternet Mesaj Erişim Protokolü)

IMAP protokolü de POP3 gibi kullanıcı e-postalarının işlenmesinde kullanılan bir uygulama protokolüdür. IMAP sunucular 143 numaralı port üzerinden istekleri dinler. POP3'ten farklı olarak istemci tarafından silinmediği sürece, e-postalar posta kutusunda tutulmaya devam eder.

- **SNMP (Simple Network Management Protocol – Basit Ağ Yönetim Protokolü)**

Ağ cihazlarının yönetimsel bilgilerinin aktarılması için kullanılan protokoldür. Bu protokol üzerinden cihazların kullanım durumuna ve performansına ilişkin bilgiler uzaktan sorgulanabileceği gibi cihazların konfigürasyonları da yapılandırılabilmektedir.

- **FTP (File Transfer Protocol – Dosya Transfer Protokolü)**

Dosyaları ağ düğümleri arasında aktarmak için kullanılan bir protokoldür. FTP işlemci yazılımıyla dosya alışverişi yapılması, silinmesi veya yeniden adlandırılması vd. dosya yönetimi komutlarının uzaktan ftp sunucusu üzerinde gerçekleştirilebilmesine olanak tanır. İstemci-sunucu arası iletişim iki farklı port üzerinden sağlanır. FTP sunucusuna oturum açmak için, kontrol bağlantısı istekleri 21 numaralı bağlantı noktasından gerçekleşirken veri dosyaları aktarımı 20 numaralı bağlantı noktası üzerinden geçer.

- **Telnet (Teletype Network – Uzaktan Yazma Ağı)**

Ağdaki bir bilgisayar üzerinden kullanıcının uzak bir bilgisayarda oturum açarak komut satırı kullanmasına imkan sağlayan bir uygulama protokolüdür. Telnet protokolüyle uzak sanal terminal oturumu esnasında trafik şifrelenmemiş olarak iletildiği için dinlemelere karşı güvenli değildir. Bu yüzden, ağ cihazlarında varsayılan olarak etkin ise devre dışı bırakılmalı ve telnet yerine, uzaktaki bir cihazı yönetmek için SSH gibi protokoller kullanılmalıdır.

- **SSH (Secure Shell – Güvenli Kabuk)**

Ağ ortamında güvenli bir şekilde uzaktaki bir bilgisayar üzerinde oturum açmayı ve komut yürütmeyi sağlamaktadır. Bu kriptografik ağ protokolü 22 numaralı bağlantı noktası üzerinden bir SSH sunucuya güvenli bir kanal sağlar.

4.2.4. TCP/UDP Protokolleri

Taşıma katmanı, daha öncede ifade edildiği gibi ana bilgisayardan ana bilgisayara iletişimden ve iki cihaz arasında mantıksal bir bağlantı oluşturmaktan sorumludur. Taşıma katmanı aşağıdaki hususları içerir: (Davies, 2019)

- Cihazlar arasında bağlantıyı başlatmayı
- Cihazlar arasında akış kontrolünü
- Gönderenden çıktığı şekilde aynı sıralamada teslimatı
- İki cihaz arası aynı anda birden fazla görüşmeyi, çoklu iletişimi

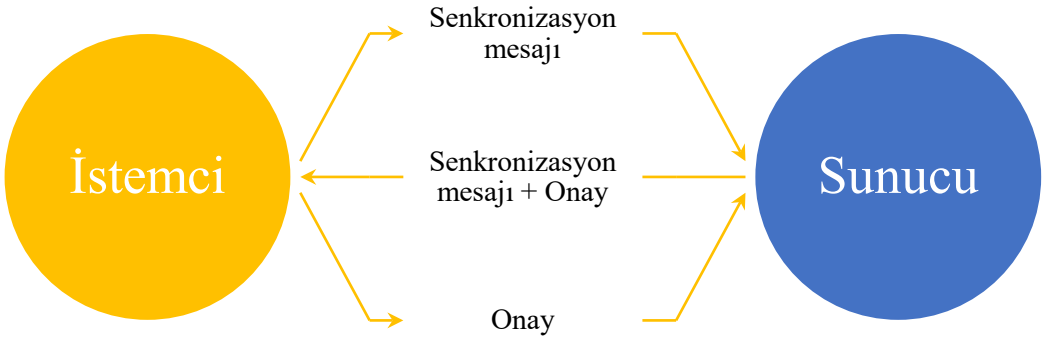
Taşıma katmanın iki protokolü TCP ve UDP protokolleridir. Uygulama katmanı hizmetlerinde bahsedildiği üzere, her iki protokolde ortak özellik mantıksal bağlantı noktası numaralarının kullanılıyor olmasıdır. Her iki protokol başlığı da bir kaynak bağlantı noktası ve bir hedef bağlantı noktası numarası içerir. Kaynak bağlantı noktası numarası, yerel ana bilgisayardaki kaynak uygulama ile ilişkilendirilirken hedef bağlantı noktası numarası uzak ana bilgisayardaki hedef uygulamayla eşleştirilir. Kaynak bağlantı noktası iki cihaz arasındaki görüşmeyi tanımlamak için dinamik olarak gönderen cihaz tarafından oluşturulur ve birden fazla görüşmenin aynı anda yürütülebilmesini sağlar. Hedef bağlantı noktası ise hedef sunucudan hangi hizmetin talep edildiğini bildirmek için segmente yerleştirilir. Segmentler daha sonra kaynağın ve hedefin IP adresini içeren bir IP paketi içinde kapsüllenir. Kaynak IP adresiyle kaynak bağlantı noktası numarasının veya hedef IP adresiyle hedef bağlantı noktası numarasının birleşimi *soket* olarak bilinmektedir.

Soketler istemci tarafında çalışan birçok işlemin birbirinden ayırt edilmesini ve bir sunucuya yapılan birçok bağlantının da birbirinden ayırt edilmesini sağlar. Kaynak bağlantı numarası, istekte bulunan uygulama için bir dönüş adresi görevi görür. Aktarım katmanı bu bağlantı noktasını takip etmesi sayesinde kendisine dönen yanıtların doğru uygulamaya iletilmesini sağlar. Ağa bağlı bir ana bilgisayarda hangi TCP bağlantılarının açık olduğunu ve çalıştığını görmek için komut satırında netstat komutu kullanılabilir. Netstat komutu IP adreslerini, alan adı isimlerine, port numaralarını da iyi bilinen uygulamalara çözümlemeye çalışır.

Temel olarak uygulamalar tarafından mesajlar karşı tarafa güvenilir bir şekilde iletilmek isteniliyorsa TCP protokolü, mesajlar hedefe mümkün olan en kısa sürede ulaştırılmak isteniyorsa UDP protokolü tercih edilmektedir (Cisco Networking Academy, 2022).

TCP (Transmission Control Protocol – İletim Kontrol Protokolü)

TCP protokolü, bağlantı odaklı bir protokoldür. Veri gönderiminden önce alıcının verileri almaya hazır olduğundan emin olmak için *üç yollu el sıkışma* (three-way handshake) metoduyla bağlantı sağlanır. (Şekil 18) Bu süreç, istemcinin sunucuya TCP senkronizasyon mesajı göndermesiyle başlar. Sunucu bu isteği aldığına dair bir onay ile birlikte TCP senkronizasyon mesajını istemciye cevap olarak gönderir. İstemcinin son adımda sunucuya bir onay mesajı göndermesiyle el sıkışma tamamlanır (Anadolu Üniversitesi, 2018:12). Cihazlar iletişimi durdurmak istediklerindeyse dört yönlü bir anlaşma sürecini takip ederler ve el sıkışma tamamlandıktan sonra portlar kapatılır. TCP protokolü bir bağlantıda tek bir alıcıya mesaj gönderebilmektedir. Çoklu gönderim (multicast, broadcast) için ayrı ayrı bağlantılar açılması gerekmektedir.



Şekil 18: TCP üç yollu el sıkışma

TCP hedefe garantili teslimatı; *sıra numaraları* (sequence numbers), *alındı bildirimleri* (acknowledgments) ve *akış kontrolü* (flow control) özellikleriyle sağlar. İletim kontrol protokolünün alıcı bilgisayarın tampon belleğini (buffer) aşacak kadar hızlı ve çok paket gönderimi yapmaması akış kontrolü (flow control) olarak adlandırılmaktadır. TCP'nin kendi içerisinde çalışan belirli metotlarla hattın durumunu gözlemlemesi ve hattın kapasitesini aşacak kadar fazla paket gönderimine engel olması ise *tıkanıklık kontrolü* (congestion control) olarak adlandırılmaktadır. Güvenilir iletimin bedeli ise TCP başlık bilgisine gönderi başına eklenen ek verilerin ve alındı bildirimlerinin fazladan bant genişliği tüketimi ve yavaşlık oluşturmasıdır (Davies, 2019).

UDP (User Datagram Protocol – Kullanıcı Veri Bloğu Protokolü)

UDP protokolünde veri iletilmeden önce üç yollu el sıkışma olmadığı için, TCP'den farklı olarak bağlantısız bir protokoldür. Verilerin karşı tarafa ulaşıp ulaşmadığıyla ilgilenilmediği için en iyi çabalı protokol olarak anılmaktadır. İstemci tarafından veri gönderildikten sonra verinin sunucu tarafından alınacağı beklenilmektedir. UDP başlık bilgisi daha azdır ve bant genişliğini artıracak alındı bildirimleri (onay) olmadığı için daha hızlı bir protokoldür. Ayrıca, UDP çok alıcıya gönderim (multicast, broadcast) için kullanılmaktadır.

Bir ağ protokolünün hem TCP'yi hem de UDP'yi kullanacağı durumlar oluşacaktır. Örneğin, o sırada hangi işlevi yerine getirdiğine bağlı olacak şekilde DNS hizmeti her iki aktarım katmanı protokolü üzerinden de çalışmaktadır. İstemciler bir DNS sunucusuna istek gönderirken UDP kullanıyorken, DNS sunucuları arasındaki iletişimde TCP tercih edilmektedir. Bir başka örnek; UDP, alındı onayı gerektirmeyen ve hızın önemli olduğu ses akışı ve VoIP gibi uygulamalarda tercih edilir. Özetle; veri

iletimi kritik olduğunda ve zaman kısıtlaması olmadığında TCP, hızın önemli olduğu ve veri iletiminin önemli olmadığı durumlarda UDP daha uygun bir aktarım protokolü olabilir (Davies, 2019). TCP ve UDP özelliklerinin karşılaştırmasına aşağıda yer verilmektedir: (Anadolu Üniversitesi, 2018:13)

Özellik	TCP	UDP
Başlık büyüklüğü	20-60 bayt	8 bayt
3 yollu el sıkışma	Var	Yok
Güvenilirlik	Var	Yok
Sıralı gönderim	Var	Yok
Tek alıcıya gönderim	Var	Var
Çok alıcıya gönderim	Yok	Var
Akış kontrolü	Var	Yok
Tıkanıklık kontrolü	Var	Yok

Şekil 19: TCP-UDP karşılaştırması

4.2.5. İnternet Katmanı

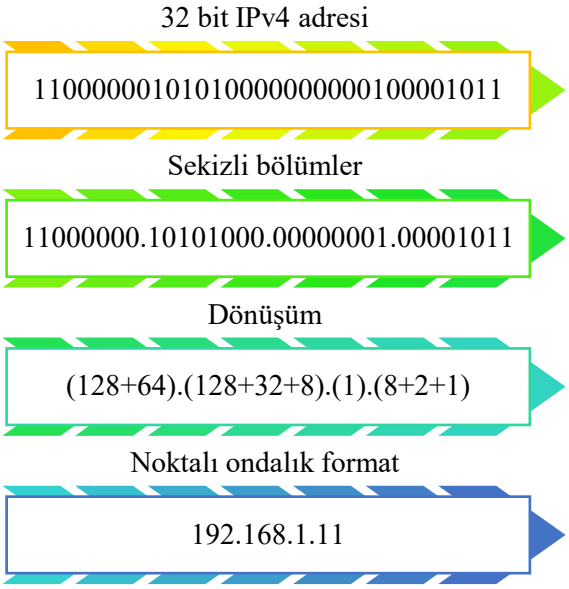
İnternet katmanında (OSI modeli 3. Katmanı/ağ katmanı) en yaygın protokol *IP (İnternet Protokolü)* tüm ağların çekirdeğini oluşturur. Bu katmanda, protokol veri birimi bir *paket* olarak anılır ve başlığı, kaynak ve hedef IP adreslerini içerir. Bu katmanda IP adresleriyle mantıksal adresleme sağlanmasıyla birlikte iletilecek veriler için rota seçimi yani paketlerin kaynaktan hedefe kadar izleyecekleri yol belirlenir. Şöyle ki, IP adreslerini ve alt ağ maskesini (subnet mask) kullanarak hedef ana bilgisayarın, gönderen cihazla aynı mı uzak ağda mı olduğu belirlenir. Hedef uzak bir ağdaysa, IP adresi bu katmanda çalışan ağ cihazları tarafından (yönlendiriciler, yönlendirici sunucular, 3. Katman kenar anahtarları) yol seçimi ve verilerin iletilmesi sürecinde kullanılır. Her ana bilgisayar bağlı olduğu ağdaki yönlendiricinin IP adresini bilmelidir. Bu yönlendirici *varsayılan ağ geçidi* (default gateway address) olarak yerel alan ağı ile İnternet arasında sınır görevi görür. IP bağlantısız (connectionless) bir protokoldür. Her bir paket ayrı olarak ele alınır ve ağdaki düğümlerin durumuna ve ağ koşullarına göre hedefe ulaşmak için farklı yollar izleyebilir.

Bu katmanda IP protokolü ile birlikte *ICMP (İnternet Kontrol Mesajı Protokolü)* ve *IGMP (İnternet Grup Yönetim Protokolü)* protokolleri de bulunmaktadır. ICMP protokolü bir ana bilgisayarın erişilemez olduğu, bir ana bilgisayara erişilebildiği ancak ana bilgisayardaki porta erişilemeyeceği, ağın erişilemez olduğu vb. hata ve kontrol mesajlarını ağdaki cihazların birbirlerine göndermesi için kullanılır. IGMP ise çoklu dağıtım (multicast) üyelerini oluşturmak ve yönetmek için kullanılır.

Ağ iletişimin önemli bir bölümü, ağdaki cihazları tanımlamayla ilgilidir. Ana bilgisayar adları ya da alan adlarından DNS protokolünde bahsedilmişti. Ağdaki cihazları tanımlamak için alan adlarıyla birlikte IP adresleri ve MAC adresleri kullanılmaktadır. MAC adresleri bir sonraki bölümde ele alınacaktır. Bu bölümde IP protokolüyle birlikte IP adreslerinin yapısı, nasıl ve ne zaman kullanıldıkları açıklanacaktır. IP protokolünün birincil işlevi mantıksal adresleme günümüzde IPv4 ve IPv6 şeklinde iki IP protokol sürümü ile sağlanmaktadır. (Davies, 2019).

IPv4

IPv4 adresleri; 32 basamaklı, her basamağında 1 ve 0 değerleri bulunan ikili (binary) sayı sisteminde sayılardır. IETF tarafından 1981 yılında IPv4 tanımı yapıldı. *IPv4 adresi* TCP/IP ağı üzerinde cihazları tanımlamak için 32 bit uzunluğunda benzersiz bir numara olarak tarif edilebilir (ISACA, 2018). İnsanlar tarafından okunması, yazılması ve hatırlanması hususlarında kolaylık sağlanması için noktalı ondalık (dotted decimal) formatta gösterimi yapılır. Bu yönde octet (sekizli) olarak adlandırılan dört gruptan her biri, 10 tabanında değerleri yazılarak nokta ile ayrılır. Bu sekizlilerin her biri 0 (bitlerin hepsi 0) ile 255(bitlerin hepsi 1) arası değere sahip olabilir. IPv4 adreslemesini anlamak için ikilik ve onluk tabanlar arasında dönüşümün nasıl yapılacağının bilinmesi gerekir. 1 olan bitlerin basamak değerleri toplanarak sekizlinin değeri belirlenir. Aşağıdaki şekilde bir IPv4 adresi örneği gösterilmektedir:



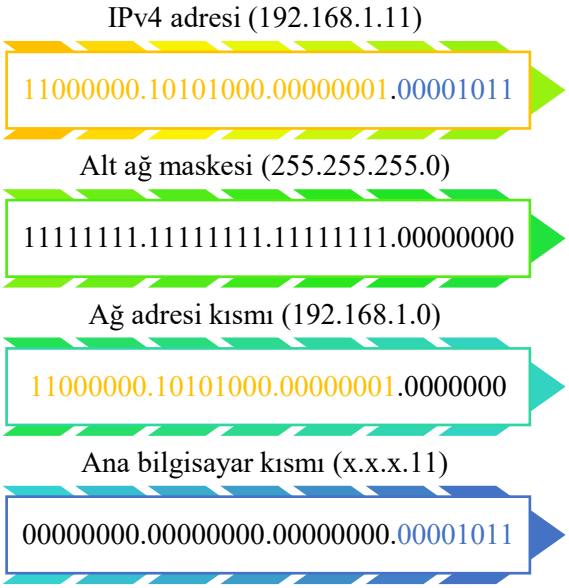
Şekil 20: IPv4 adresi

IPv4 adresleri hiyerarşik bir yapıya sahiptir ve ağ ve ana bilgisayar olmak üzere iki bölümden oluşur. Ağa bağlanacak bir ana bilgisayar yapılandırılırken, bir IPv4 adresiyle birlikte alt ağ maskesi (subnet mask), ağ geçidi (gateway), dns sunucuları (dns servers) bilgileri de ayarlanır. İşte bunlardan *alt ağ maskesi* bir IPv4 adresinin hangi bölümünün ağ, hangi bölümünün ana bilgisayar kısmı olduğunu belirtir. Alt ağ maskesi de benzer şekilde 32 bitlik bir değerdir (soldan başlayarak sürekli 1'lerden oluşan) ve bu değer içindeki 1 olan bitler ağ bölümünü, 0 olan bitler host bölümünü temsil eder. Şekil 21'de görüldüğü üzere 192.168.1.11 IP adresini, 255.255.255.0 alt ağ maskesi 192.168.1.0 ağ adresiyle, 0.0.0.11 ana bilgisayar kısımlarına ayırır. Bu hesaplamalar, hedefin yerel mi uzak ağda mı olduğunu belirlemeye yarar. Bir ana bilgisayar bir paket gönderirken alt ağ maskesini kendi adresi ve hedef adresi ile karşılaştırarak paketi yerel olarak doğrudan hedefe mi veya uzak ağ üzerinden hedefe göndermek için ağ geçidine mi ileteceğine karar verir (Cisco Networking Academy, 2022).

IPv4 adresinin ağ bölümü, adresin bulunduğu ağı gösterir. Ana bilgisayar kısmı ise bu ağ içinde kaç cihaz bulunabileceğini belirtir. Aynı ağdaki bütün bilgisayarlar aynı ağ adresine ve alt ağ maskesini sahip olacaktır. Yukarıdaki örnekte; 192.168.1.0/24 ağında 8 bit, ağdaki bilgisayarları numaralandırılmak için bırakılmıştır. O zaman, bu ağda bulunabilecek ana bilgisayar sayısı $2^8 - 2 = 254$ olarak hesaplanır. Toplam değerden ikiyi çıkarmamızın sebebi, her ağın bir ağ adresi (192.168.1.0) ve yayın adresi(192.168.1.255) bulunması ve bunların ağdaki ana bilgisayarlara atanamamasıdır. Burada açıklanması gerekli bir husus IP adresi ve alt ağ maskesinin tek bir ifadede gösteren 192.168.1.0/24 notasyonudur. Bu gösterimde, "/24" prefix(öneki) 192.168.1.0 ağında 255.255.255.0 alt ağ maskesindeki 1 değerlerinin kaç tane olduğunu belirtmektedir.

IP adresi sadece uzak bir ağdaki cihazlarla değil aynı ağdaki cihazlarla iletişim kurmak için de kullanılır. Trafik kaynak IP adresinden hedef IP adresine gönderilir. Bunun başarılı bir şekilde

gerçekleştirilebilmesi için IP adreslerinin ağa bağlanan her bir cihaza birbirinden farklı benzersiz şekilde tanımlanması gereklidir. Hedef IP adresi 3 farklı türde olabilir. Bunlar *unicast*(tek yöne yayın), *multicast*(çok noktaya yayın), *broadcast*(yayın) adresi olarak tanımlanmaktadır. Cihazlar arasındaki iletişim genellikle istemci-sunucu veya ana bilgisayardan ana bilgisayara şeklinde tek noktaya yayındır. Çok noktaya yayın, iletimin bir kaynaktan belirli bir multicast gruba üye olmuş seçili bilgisayarlara tekil bir adres üzerinden yapılmasıdır. Yayın adresi ise bundan farklı olarak ağdaki bütün ana bilgisayarların gönderilen bir paketi alması istendiğinde kullanılan ağa özel tekil adrestir.



Şekil 21: Alt ağ maskesi

TCP/IP üzerine inşa edilmiş İnternet üzerinde de sorunları önlemek için benzersizlik sağlanmalıdır. Bu bağlamda, IP adresleri IANA tarafından yönetilir. İnternet üzerinde kullanılan *genel IP adresleri* (public IP address) IANA tarafından aşağıda listelenen Bölgesel İnternet Kayıt Kuruluşlarına (RIR) tahsis edilerek IP adres bloklarının bütün dünyaya dağıtımı sağlanmaktadır. Bu kayıt şirketlerinin her biri kendi bölgesinde İnternet Servis Sağlayıcı'lara (ISS) IP adresi vermekten sorumludur. ISS'ler de daha küçük ISS'lere, diğer kuruluşlara ve kamunun kullanımına sunar. Kuruluşlar da RIR politikalarına göre IP adreslerini doğrudan tabi oldukları RIR'den alabilirler. (Cisco Networking Academy, 2022)

- **AFRINIC (African Network Information Centre):** Afrika bölgesi
- **APNIC (Asia Pacific Network Information Centre):** Asya/Pasifik Bölgesi (Doğu Asya, Okyanusya, Güney Asya ve Güneydoğu Asya)
- **ARIN (American Registry for Internet Numbers):** Kuzey Amerika Bölgesi (Antarktika, Kanada, ABD ve Karayipler'in bazı bölgeleri)
- **LACNIC (Latin America and Caribbean Network Information Centre):** Latin Amerika ve Karayip Adalarının çoğu
- **RIPE NCC (Réseaux IP Européens Network Coordination Centre):** Avrupa, Orta Doğu ve Orta Asya

Bir ağ sınıflı (classful) veya sınıfsız (classless) ağ türlerinden biri kullanılarak adreslenebilir. Sınıflı ağlarda, adresler Şekil 22'de görüldüğü üzere aralıklara ayrılır. Sınıflı ağlar ön tanımlı alt ağ maskelerine sahiptir. Sınıflı ağlarda bir ağın sınıfı IP adresinden kolayca tanımlanabilir. İnternet IPv4 adresleri, ağda ihtiyaç duyulan düğüm sayısına bağlı olarak öncelikle üç sınıftan (A,B,C) birine göre tahsis edildi. İnternet büyüdükçe IP adreslerinin boşa harcandığı ve verimli şekilde kullanılmadığı anlaşılmıştır. Bu nedenle zaman içinde terk edilerek IANA tarafından ağ adreslemesi *CIDR (Sınıfsız alanlar arası yönlendirme)* kullanılarak yönetilmeye başlandı. Sınıfsız ağlar, gerektiğinde daha büyük

veya daha küçük ağları tanımlamak için herhangi bir adres alanının bölümlere ayrılmasına izin verip ön tanımlı ağların sınırlarını ortadan kaldırarak IP adreslerinin daha verimli kullanılmasını sağlamaktadır. CIDR, hepsi aynı boyutta birden çok ağa sahip olmak yerine ağların farklı boyutlarda alt ağlara bölünmesine izin vermek için *VLSM (Değişken uzunlukta alt ağ maskeleme)* yöntemini kullanmaktadır. Sınıflı adreslemenin D sınıfı çok noktaya yayın (multicast) adreslerinden oluşur. E sınıfı ise deneysel adres bloğudur.

Sınıflı Ağlar	**Sınıf**	**IP aralığı**	**Öneki (Prefix) - Düğüm sayısı**
	A	0.0.0.0 - 127.255.255.255	8 - 16.777.214
	B	128.0.0.0.0 - 191.255.255.255	16 - 65.534
	C	192.0.0.0 - 223.255.255.255	24 - 254
	D	224.0.0.0 - 239.255.255.255	
	E	240.0.0.0 - 255.255.255.255	

Sınıfsız Ağlar (Örnek: 192.168.1.0/24)	**Alt ağ**	**IP aralığı**	**Öneki (Prefix) - Düğüm sayısı**
	1	192.168.1.0 - 192.168.1.127	25 - 126
	2	192.168.1.128 - 192.168.1.191	26 - 62
	3	192.168.1.192 - 192.168.1.207	28 - 14
	4	192.168.1.208 - 192.168.1.211	30 - 2

Şekil 22: Sınıflı-sınıfsız adreslendirme

İnternet servis sağlayıcıları yönlendiricileri arasında yönlendirilen genel IP adresleri yanında sadece yerel alan ağlarındaki ana bilgisayarların adreslenmesi ve birbirleriyle iletişimi için kullanılmak üzere *özel adres (private address)* blokları da bulunmaktadır. Bu adres blokları İnternet ağı üzerinde kullanılamaz. Fakat dahili ağlarda ihtiyaçlara göre farklı boyutlarda alt ağlara bölünerek ve benzersizlik sağlanarak kullanılabilmektedir. *Ağ adresi dönüştürme (NAT)* içerdeki bir ana bilgisayarın İnternet ortamında iletişim sağlaması için özel ile genel IPv4 adresleri arasında çeviri yapmak için kullanılır. Özel adres blokları A,B,C sınıflarında aşağıda şekilde belirlenmiştir:

- **A sınıfı:** 10.0.0.0 - 10.255.255.255 (10.0.0.0 /8)
- **B sınıfı:** 172.16.0.0 - 172.31.255.255 (172.16.0.0 /12)
- **C sınıfı:** 192.168.0.0 - 192.168.255.255 (192.168.0.0 /16)

IPv6

IPv6 İnternet Protokolünün en son sürümüdür. IETF tarafından IPv4 adresinin tükenmesi sorununun çözümü için geliştirilmiştir. 1990'larda yapılan çalışmalar sonrası IPv6, Aralık 1998'de IETF Taslak Standardına dahil edildi. 1999 yılında IANA tarafından IPv6 blok atamalarına başlandı. IPv6, 14 Temmuz 2017'de İnternet Standardı olarak onaylandı. IPv4'ün 32 bitlik uzunluğuna karşı 128 bitlik bir IPv6 adresi alanıyla artan adres ihtiyacı için kalıcı bir çözüm üretilmiştir. Her iki sürümün bir süre daha birlikte var olacağı gözükmektedir. IPv6 geniş adres aralığıyla birlikte, IPv4 ile ilgili farklı iyileştirmeler de içermektedir: (Solomon & Kim, 2021)

- IP adreslerini atamayı kolaylaştırma
- Ağları yeniden numaralandırmayı kolaylaştırma
- Adresin ana bilgisayar belirleme kısmını standartlaştırma
- Ağ güvenliği unsurlarını içerme
- Çoklu yayının teknik özelliklerin bir parçası olarak tanımlanması

IPv6, IPv4 nokta gösterimi ile 16 sekizli gerektirir. Bunun yerine IPv6 adresleri onaltılık sayı sisteminde 4 basamaklı sayılardan sekiz grup olacak şekilde ifade edilir. Gruplar iki nokta üste üste ile ayrılır. aaaa:aaaa:aaaa:aaaa:bbbb:bbbb:bbbb:bbbb biçiminde a'lar ağ kısmını, b'ler ana bilgisayarı belirleyen kısmı tanımlar.

IPv6 adreslerinin daha kısa bir notasyonda gösterilmesi için iki kural bulunmaktadır:

- Onaltılık gruplar içinde baştaki sıfırlar yazılmayabilir.
- İki veya daha fazla ardışık sıfır grubundan oluşan yalnızca bir grup "::" (iki tane iki nokta üst üste) ile değiştirilebilir.

Şekil 23: IPv6 adresinin kısaltılması

IPv6, IPv4'den farklı olarak broadcast paketleri gönderilmesini desteklememektedir. IPv6, paketleri hedefe göndermek için aşağıdaki yöntemleri içerir:

- **Unicast (Tekli yayın):** Bir paketi tek bir hedefe gönderme.
- **Anycast (Her yöne yayın):** Bir paketi belirli bir düğüm grubundaki en yakın düğüme gönderme.
- **Multicast (Çoklu yayın) :** Bir paketi belirli bir düğüm grubuna gönderme.

IPv6 ve IPv4 sürümleri arasındaki yapısal farklılıklar nedeniyle OSI katman 3'te ikisi de farklı yığınlarda çalışması gerekmektedir. IPv4'ten IPv6'ya geçiş kademeli bir süreçtir ve geçiş sırasında her iki sürüm için de işletim sistemi desteği gerekmektedir. Bu yönde, IPv4 ve IPv6 protokollerinin aynı anda kullanılmasını için işletim sistemlerinin çoğunluğu *ikili IP yığını* (dual stack) desteklemektedir. Uygulamaların bu süreçte özellikle IPv6 uyumlu hale getirilmesi önem arz etmektedir. Çünkü uygulamalar zamanla sadece IPv6 ağlar üzerindeki cihazlara tarafından erişilebilir olması gerekecektir (Solomon & Kim, 2021).

IP protokolünün iki sürümü Şekil 24'te karşılaştırılmaktadır: (Gazi Üniversitesi Bilişim Enstitüsü, 2016)

4.2.6. Ethernet

OSI katman 1 ve 2, *Ethernet* olarak bilinen IEEE 802.3 standardı tarafından tanımlanmaktadır. Katman 2, verilerin fiziksel ortama yerleştirilmesi, hata bildirimleri ve akış kontrolünü içerir. Bu katmandaki protokol veri birimi *çerçevedir*. Çerçevelere ayrıca Katman 2 PDU'lar da denir. Çerçeve başlığına kaynak ve hedef MAC adresleri eklenir. Katman 1'de verilerin bitler halinde fiziksel iletimi

gerçekleşir ve kablolama ve ağ kartlarının uyması gereken gerilimler, hızlar vb. kriterler yer alır. Sosinky fiziksel ortamı aşağıda gibi açıklamaktadır:

"Fiziksel iletim ortamı, bir elektromanyetik sinyali iletebilen herhangi bir ortamı ifade eder. Bir sinyal, belirli bir mesafeye yayılabilen ve bir alıcı tarafından tanınabilen veri biçimindeki bilgileri temsil eden, sinyal genliği, voltajı veya frekansında zamanla değişen bir modeldir. Sinyaller sürekli değişken (analog) olabilir veya ayrık ve belirli durumlarla sınırlı (dijital) olabilir. Analog bilgisayarlar mevcut olsa da, neredeyse tüm durumlarda kullanılan sistemler dijitaldir ve daha spesifik olarak ikili (binary) sistemlerdir. Dijital bilgisayarlar ikili sinyalleri ve boolean mantığını kullanır çünkü sinyal gönderme nispeten basit ve hızlıdır ve ikili sinyaller herhangi bir karakteri temsil edecek veya neredeyse tüm matematiksel denklemleri çözecek şekilde yapılabilir." (2009)

IPv4

- 32 bit adresleme
- 20-60 byte başlık büyüklüğü
- IPSec desteği isteğe bağlı
- Gönderici ve yönlendiricilerde parçalama
- Paket başlığı sağlama toplamı var
- Paket akış tanımlama yok
- IGMP ile multicast üyeliği
- Arp ile adres çözümleme - Broadcast
- Dns A kayıtları
- Yönlendirici keşfi isteğe bağlı
- Adres yapılandırması manuel ve Dhcp
- Broadcast adresi kullanılır
- Loopback adresi 127.0.0.1

IPv6

- 128 bit adresleme
- 40 byte başlık büyüklüğü
- Dahili IPSec desteği
- Sadece istemcide fragmentasyon
- Paket başlığı sağlama toplamı yok
- Başlıkta FlowLabel alanıyla paket akışı tanımlama
- Multicast dinleyici keşfi (MLD)
- Komşu keşfi protokolü - Multicast
- Dns AAA kayıtları
- Yönlendirici keşfi zorunlu ICMPv6
- Adres yapılandırması otomatik, Dhcpv6
- Broadcast adresi kullanılmaz
- Loopback adresi ::1

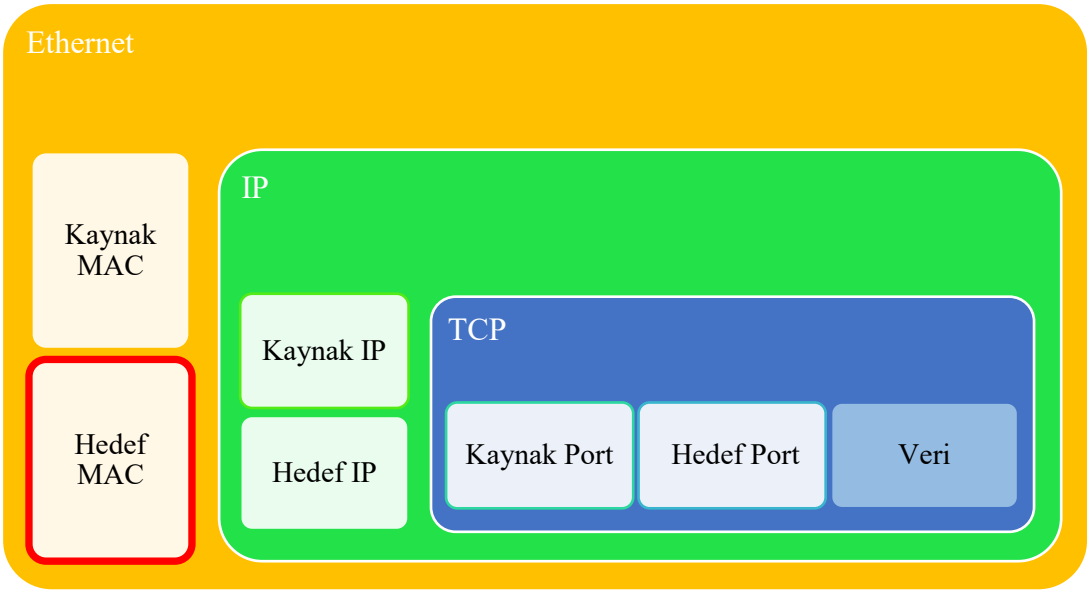
Şekil 24: IPv4-IPv6 Karşılaştırılması

Her iletişim, kaynağı ve hedefi belirlemenin bir yolunu gerektirir. IP protokolü kısmında da ifade edildiği gibi veriler aynı yerel ağ içerisindeki bir ana bilgisayara gidecekse bağlantı o ana bilgisayara olacaktır. Veriler uzak bir ağdaki ana bilgisayara gönderilecekse, bağlantı varsayılan ağ geçidine yapılacaktır. Ağ uygulamaları iletişim için ana bilgisayar isimlerini, alan adlarını ve mantıksal hedef IP adreslerine güvenir. Üst katmanlardan bu bilgiler doldurularak katman 2'ye kadar ulaştırılmakla beraber yerel bir ethernet ağında, fiziksel MAC adresleri üzerinden iletişim gerçekleşir ve bu bilgilerin de çerçeveye yerleştirilmesi gerekir. *MAC (Medya Erişim Kontrolü) adresi*, Ethernet ağ birimleri (NIC) üretilirken her birine farklı olarak atanmış (benzersiz) fiziksel 48 bit adrestir ve ağdaki

ana bilgisayarları tanımlar. O zaman, gönderen ana bilgisayarın çerçeveye yerleştirmesi gerektiği hedef ana bilgisayar veya varsayılan ağ geçidinin MAC adresleri nasıl belirlenecektir? IPv4 protokolünde yerel ağdaki herhangi bir ana bilgisayarın MAC adresini keşfetmek için *Adres Çözümleme Protokolü (ARP)* protokolü kullanılır. IPv6'da ise *komşu keşfi (MLD)* olarak bilinen benzer bir yöntem kullanılır.

Ethernet ağında, bir NIC yalnızca hedef adresin ağ broadcast adresi olması veya kendi MAC adresine karşılık gelmesi durumunda bir çerçeveyi kabul eder. Bu kapsamda ARP protokolünde, IPv4 adresi bilinen yerel ağdaki bir ana bilgisayarın MAC adresini keşfetmek ve depolamak için aşağıdaki süreç takip edilmektedir: (Cisco Networking Academy, 2022)

- Gönderen ana bilgisayar, hedef ana bilgisayarın IP adresini içeren bir çerçeve oluşturarak ağ broadcast adresine gönderir.
- Ağdaki bütün ana bilgisayarlar bu çerçeveyi alır ve IP adreslerini çerçevedeki IP adresiyle karşılaştırır. Yalnızca, söz konusu IP adresine sahip olan ana bilgisayar MAC adresini gönderen ana bilgisayara iletir.
- Gönderen ana bilgisayar, MAC ve IP adresi eşleşmesini ARP tablosunda saklar.



Şekil 25: Kapsülleme

ARP protokolüyle, hedef ana bilgisayarın MAC adresi de öğrenildiğine göre çerçevenin oluşturularak gönderilebilmesi için başka bir engel bulunmamaktadır. Bu manada, ağ yığınında alt katmandaki bir protokolün daha yüksek katmanlı bir protokolden bir mesajı kabul edip bunu kendi protokol veri birimi içerisinde veri kısmına yerleştirmesine *kapsülleme* (encapsulation) denir (ISACA, 2018). Ethernet protokolü kapsamında gönderen tarafından gönderilmeden her bir mesaj çerçeve denilen belirli bir biçimde kapsüllenir. Bu çerçevenin biçimi ve içeriği, gönderilen mesajın türüne ve iletildiği kanala göre belirlenir. Ethernet protokolü standartları, çerçeve formatı, çerçeve boyutu, zamanlama ve kodlama dahil olmak üzere ağ iletişiminin birçok yönünü tanımlar. Temel bir Ethernet çerçevesinde, gönderen ve alıcı MAC adresleriyle birlikte veri türü, verinin kendisi ve çerçeve kontrol dizisi yer alır. Ağ iletişiminde verilerin parçalara ayrılıp çerçevelere yerleştirilerek gönderilmesi birincisi ortamın belirli göndericilerin tekelinde olmasını engeller. İkincisi kaybolan verilerin tekrar gönderilmesini daha verimli hale getirir.

Ethernet ilk sürümlerinde 10 Mbps gibi nispeten yavaş hızlarda çalışırken, teknolojinin gelişmesiyle birlikte *Ethernet (802.3)* yeni sürümleriyle yüksek hız gerektiren uygulamaların ve zamana duyarlı protokollerin çalışmasını destekleyecek hızlarda ve esneklikte standartlar oluşturuldu. Bu yönde, resmi bir yerel alan ağı standardı bulunmamakla birlikte Ethernet tabanlı LAN teknolojilerinin hızlı bir şekilde olgunlaşmasıyla yerel ağların iletişiminde Ethernet diğerlerinden daha yaygın hale geldi. Ethernet'in tarihsel olarak gelişim sürecine aşağıda yer verilmektedir: (Solomon & Kim, 2021)

- 1973 yılında Ethernet, Xerox firması tarafından geliştirildi.
- 1980'lerde Xerox, DEC ve Intel (DIX) birlikte çalışarak 10 Mbps hızında DIX Ethernet standardını çıkardı.
- 1985 yılında IEEE, 802.3 (Ethernet) standardını oluşturdu.
- 1995 yılında 100 Mbps Fast Ethernet standardizasyonu yayınlandı.
- 2001 yılında, Ethernet'in WAN bağlantı çözümü olarak benimsenmesi kapsamında MEF (Metropolitan Ethernet Forum) platformu kuruldu.
- 2006 yılında 1Gbps Ethernet standardı ortaya çıktı.
- 2010, 2011, 2013 ve 2014 yıllarında 100G Ethernet standardizasyonu gerçekleşti.
- 2016 yılında, IEEE tarafından 250Gbps ve 400Gbps Ethernet standartları çıkarıldı.

4.2.7. Ağ Altyapısı Cihazları

Ethernet yerel alan ağlarını (LAN) birbirine bağlamanın birçok yolu vardır. İki veya daha fazla ağ arasındaki iletişim ya da ağ grupları arasında ağ oluşturma uygulama ve teknolojilerine *internetworking* (ağlar arası iletişim) denilmektedir. Düşük maliyetlerde farklı fiziksel ortamlar ve alıcı-vericiler (transceivers) kullanılarak fiziksel olarak Ethernet ağının genişlemesi sağlandı. Yerel alan ağlarının kullanımı arttıkça birimlerin veya çalışma grubu ağlarının birbirine bağlanma ihtiyacı da arttı. Güvenlik, trafik segmentasyonu ve kullanım kolaylığı LAN'ları ayırmak ve ağlar arasında çalışmak için nedenlerdir.

Günümüz ağları kuruluşların istemci-sunucu mimarisine hizmet veren büyük, merkezi olarak yönetilen yüksek hızlı LAN ve WAN ağlarının birbirine bağlı olduğu mimari çözümün bir parçasıdır. Uygulama sunucuları, veritabanları, son kullanıcılar gibi bilgi sistemleri unsurları bu mimaride ağ bölümleri ve blokları altında bir araya getirilmektedir. Bu ortamlarda bilgi kaynaklarını birleştirmek için hızlı erişim yetenekleri sağlanmaktadır. Bunun yanında, bilginin her zaman ve her yerde kullanılabilir olması ve merkezi olarak yönetilmesi gerekliliklerine yönelik mimariler uygulanmaktadır. İş, performans ve güvenlik tasarımı açısından sunulan ağ mimarisi çözümlerini anlamak için telekomünikasyon altyapısının tasarımı ve geliştirilmesiyle ilgili LAN ve WAN gibi bilgi teknolojilerinin teknik özellikleri iyi bilinmelidir (ISACA, 2019:278).

Telekomünikasyon birbirine bağlı uç noktalar arasında veri, ses ve görüntülerin elektronik olarak iletilmesidir. Gönderici ve alıcı uç noktalar iletim ortamına ve ağ cihazlarına ağ birimleri/arayüzleri üzerinden bağlanırlar. Tekrarlayıcı (repeater), hub (merkez), köprü (bridge), anahtar (switch), yönlendirici (router) gibi farklı ağ ortamlarındaki bilgi sistemlerini birbirine bağlamak için kullanılan yaygın ağ cihazlarının açıklamalarına aşağıda yer verilmektedir (Solomon & Kim, 2021).

Tekrarlayıcılar ve Hublar

Tekrarlayıcılar ve hublar, katman 1 yönlendirme cihazlarıdır. Kablolama mesafelerinin fiziksel olarak uzatılması veya farklı bir iletim ortamına dönüştürme işlemleri fiziksel katmanda yapılabilir. Koaksiyel kabloya bağlı Ethernet LAN'larında mesafe sınırlamalarının üstesinde gelinmesi gerekiyordu. Bunun için, bir ağın menzilini genişleten veya iki ayrı ağ segmentini birbirine bağlayan tekrarlayıcılar kullanıldı. Bu cihazlar genellikle, Ethernet bus topolojisinin fiziksel mesafesini genişletmek için bir kablolama türünü diğerine değiştirirken kullanılır. Tekrarlayıcılar iki portludur. Tekrarlayıcı, bir portundan gelen zayıflayan sinyali yeniden oluşturarak yükselten ve diğer portundan gönderen fiziksel katman cihazıdır. Bu sayede, sinyalin daha uzun mesafelere gitmesi sağlanır.

Hub da benzer şekilde çalışır. Tekrarlayıcıdan farkı ikiden fazla porta sahip olması ve birden çok bağlantıyı desteklemesidir. Hub'lar yıldız topolojinin merkezi olarak hizmet verir. Bir porttan gelen çerçeveler, gelen portta dahil olmak üzere bütün portlara tekrar yansıtılır. Ortak veri yolu kullanıldığı için bağlı cihazlar ve ağlar aynı *çarpışma etki alanının* (collision domain) bir parçasıdır. Birden fazla cihaz aynı anda bir ağ segmentinde bir mesaj göndermeye çalıştığında bir ağ çakışması meydana gelir.

Köprüler ve Kenar Anahtarlar

Anahtarların daha üst katmanlarda (katman 3-4) çalışma yeteneği bulunanları mevcut olmakla beraber, köprüler ve anahtarlar temel olarak katman 2 yönlendirme cihazlarıdır. Daha verimli ağlar için çarpışma alanları azaltılmalıdır. Köprüler ve anahtarlar bir ağı birden çok çarpışma alanına bölmek için kullanılır. Bir diğer ifadeyle, bu cihazlardaki her bir port farklı bir çarpışma etki alanındadır. Anahtarlar köprü teknolojisine göre daha hızlı çalıştığı ve daha fazla port sayılarına sahip oldukları için piyasaya çıkınca, köprüler aşamalı olarak kaldırıldı. Katman 1 cihazları trafiği basitçe taşırken, katman 2 cihazları çarpışma alanlarını ayırdığı için trafiği bütün portlara akıtmadan yalnızca hedef aygıtın bulunduğu porttan gönderir. Bu işlemi, kendine gelen bütün trafiği inceleyip çerçevelerde yer alan hedef MAC adreslerini adres tablosunda arayarak sağlar.

Kenar anahtarla bağlı bir Ethernet LAN'ındaki düğümler birbirine broadcast mesajıyla ulaşabilir. Birbirinden broadcast mesajı alabilen bu cihazlar grubu, bir *yayın etki alanı* (broadcast domain) olarak adlandırılır. Cihaz sayısı arttıkça, broadcast mesajları ağdaki cihazlar üzerinde daha fazla işlem yükü oluşturur. Bunun önüne geçmek ve trafiği sınırlandırmak için ayrı broadcast domain'e sahip küçük ağlar oluşturulmalıdır. Fiziksel olarak uç sayısı makul seviyelerde, farklı kenar anahtarlar üzerinde ağlar oluşturulabileceği gibi ağ aynı anahtarlar üzerinde daha küçük VLAN'lara (sanal yerel alan ağı) da bölünebilir. *VLAN*, bir ağdaki bir veya daha fazla anahtardaki bazı portlardan oluşan bir ağdır. Yani, LAN üzerinde mantıksal olarak birbirinden ayrılmış ana bilgisayar grubudur. VLAN sanal bir ağdır ama broadcast mesajlarının VLAN içinde sınırlı olduğu normal bir ağ özelliklerine sahiptir.

Kenar anahtarlar aşağıdaki hizmetleri sağlayarak ağları daha hızlı hale getirmektedir:

- Birçok çarpışma etki alanı oluşturarak, ilgisi olmayan düğümlere giden trafiğin azaltılması
- VLAN'ların etkinleştirilerek trafik izolasyonu sağlanması
- Hasarlı çerçevelerin boşa çıkarılması, düşürülmesi
- Birbiriyle sık iletişim kuran cihazların aynı VLAN içerisinde konumlandırılması

Yönlendiriciler

Yönlendiriciler katman 3 yönlendirme cihazlarıdır. IP paketlerinde ağ adreslerini inceleyerek paketi hedefine yönlendirmek için kararlar verir. Yönlendiriciler, kenar anahtarlara benzer şekilde iki veya daha fazla fiziksel olarak ayrı ağı birbirine bağlar ancak aşağıdaki hususlarda katman 2'de çalışan kenar anahtarlardan ayrılır: (ISACA, 2019: 718)

- Fiziksel değil mantıksal adreslerin kullanılması
- Portlarda farklı adreslerin tanımlanması
- Portlar arası broadcast bilgilerin engellenmesi
- Bilinmeyen adreslere giden trafiğin engellenmesi
- Ağ veya ana bilgisayar bilgilerine bağlı olarak trafiğin filtrelenmesi

4.2.8. Kablosuz Yerel Alan Ağı

Bilindiği üzere, IEEE 802 komitesi ağ oluşturma standartlarını belirlemektedir. IEEE 802.11 alt komitesinde kablosuz yerel alan ağlarının (WLAN) işleyişi, özellikleri ve yapısıyla ilgili standart oluşturma çalışmaları yürütülmektedir. 802.11 standartları arkasındaki teknoloji *Wi-Fi* olarak isimlendirilmektedir. 2,4 GHz veya 5 GHz radyo frekanslarında farklı veri iletim hızlarında geliştirilmiş sürekli genişleyen bir standartlar listesi yer almaktadır. Kablosuz bağlantılar üzerinde güvenliği sağlamak için WEP, WPA, WPA2, WPA3 gibi protokoller bulunmaktadır. Aktarımların şifrelenmesinde ilk kullanılan şifreleme protokolü olan WEP, RC4 algoritmasını kullanılır. WEP, kolaylıkla kırılabilmektedir. Zaman içinde, WEP protokolünün yerini diğer şifreleme teknolojileri almıştır. Bu güvenlik protokolleri, kullanıcılar ve erişim noktaları arasında etkili kimlik doğrulama ve şifreleme sağlamak için açık anahtar şifreleme tekniklerini kullanır. WPA, WEP'te kullanılan RC4

algoritması kullanırken, WPA2 AES şifreleme algoritmasıyla oluşturulmuştur. WPA3, WPA2'nin ardından gelen daha gelişmiş şifreleme teknolojileri kullanan en son sürüm protokoldür.

IEEE 802.11 standardında tanımlanan bazı anahtar terimler aşağıda yer almaktadır: (Anadolu Üniversitesi, 2018:108)

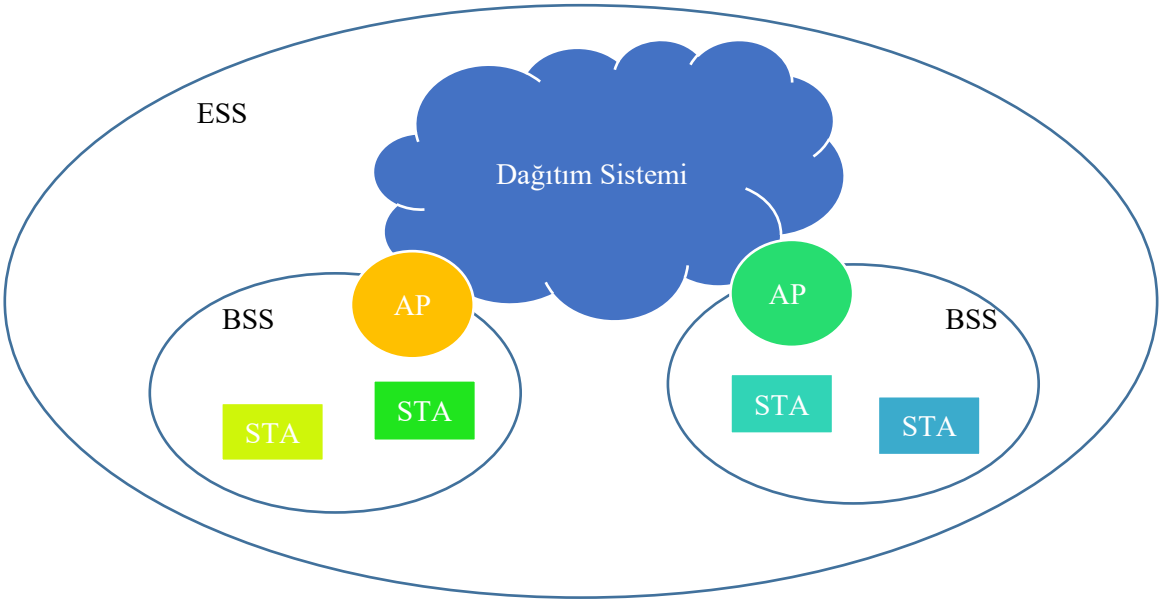
• **İstasyon (Kablosuz istemci - Station):** IEEE 802.11 standardı ile uyumlu çalışan herhangi bir aygıttır.

• **Erişim Noktası (Access Point - AP):** İstasyon işlevine sahip ve ilişkili istasyonlar için kablosuz ortam üzerinden dağıtım sistemine erişim sağlayan herhangi bir öğedir. Erişim noktası BSS ile DS arasında köprü işlevi görür.

• **Eşgüdüm işlevi (Coordination Function):** Bir istasyonun ne zaman veri gönderebileceğine ve alabileceğine karar veren mantıksal işlevdir. Merkezi veya dağıtık olarak gerçekleştirilir.

• **Temel Hizmet Kümesi (Basic Service Set - BSS):** Aynı koordinasyon işlevi tarafından kontrol edilen istasyonların kümesinden oluşur. Her BSS'nin *SSID* (Service Set Identifier – Hizmet Kümesi Tanımlayıcısı) olarak tanımlanan bir ağ adı bulunur. Erişim noktaları tarafından duyurulan SSID'nin benzersiz olması gerekli değildir. Erişim noktalarını benzersiz şekilde tanımlayan erişim noktasının MAC adresidir. Bu *BSSID* olarak adlandırılır. Birçok erişim noktası olan bir ağda erişim noktalarının BSSID'leri farklıdır fakat sorunsuz ve sürekli bir bağlantı için SSID'ler aynıdır.

• **Dağıtım Sistemi (Distribution System - DS):** *Genişletilmiş hizmet kümesi* (Extended Service Set - ESS) oluşturmak için temel servis setlerinin kümesi ile yerel alan ağlarını birbirine bağlamak için kullanılan sistemdir. Dağıtım sistemi kablolu veya kablosuz bir iletişim ağı olabilir.



Şekil 26: Kablosuz Ağ Mimarisi

WLAN mimarisinde kapsama alanları hücre olarak adlandırılan kısımlara bölünür ve her bir hücreden bir erişim noktası sorumludur. Bir kablosuz ağın en küçük yapı taşı *temel hizmet kümesidir*. Bu küme izole kalabileceği gibi, bir erişim noktası kullanarak dağıtım sistemine bağlanabilir. Erişim noktası köprü görevi görür. Temel hizmet kümesi içerisindeki istasyonlar birbiriyle doğrudan iletişim kurmazlar. Erişim noktası üzerinden birbirleriyle iletişime geçerler. İstasyonların erişim noktasına ihtiyacı yoksa birbiriyle doğrudan iletişime geçiyorsa bu hizmet kümesine *bağımsız temel hizmet kümesi (IBSS)* denir. IEEE 802.11i kablosuz yerel alan ağları için kimlik doğrulama, veri bütünlüğü, veri gizliliği ve anahtar yönetimi konularında güvenlik standartlarını belirler. Kablosuz ağlarda verinin iletimi kablo yerine radyo frekansları aracılığıyla atmosfer içerisinde gerçekleştirilir. Kablosuz ağlar iletilen verilerin elde edilmesine veya kurulmak istenen iletişimi bozmaya, verinin değiştirilmesine

yönelik saldırılara maruz kalabilir. Sağladığı hareket esnekliğiyle birlikte aşağıdaki zafiyetleri mevcuttur:

- Yetkisiz kişiler tarafından ağın dinlenmesi.
- Radyo frekanslarının karıştırılması veya kötü amaçlı sinyallerin iletişime eklenmesi.
- Kablosuz istemcilerin yetkisiz erişim noktalarına bağlanması.
- Kablosuz istemcilerin şifreleme algoritmalarını desteklememesi.

Kablosuz yerel alan ağları dışında aşağıdaki özellikleri verilen kablosuz ağ türleri bulunmaktadır: (ISACA, 2019:319)

- **Kablosuz kişisel alan ağları (WPAN):** WPAN'lar 802.15 standardına dayanır. Kablosuz cihazlar kısa menzillerde 2.4 Ghz frekans bandında bağlantı sağlar. Bluetooth ve Zigbee WPAN teknolojileridir.

- **Kablosuz genel alan ağları (WWAN):** Radyo, uydu ve cep telefonu teknolojilerini kullanan WWAN'lar geniş bir coğrafi alan üzerinde farklı ağları birbirine bağlar. Bu geniş kapsama alanı teknolojileri arasında LTE, WiMAX, CDPD, GSM, Mobitex yer alır.

- **Kablosuz tasarsız ağlar (Wireless Adhoc Networks - WANET):** WANET'ler cep telefonları, diz üstü bilgisayar ve tabletler gibi uzak cihazları dinamik olarak bağlarken diğer kablosuz ağ türleri gibi sabit bir ağ altyapısı kullanmaz. Cihazlar arası bağlantılar herhangi bir erişim noktası veya yönlendirici olmadan kurulur ve cihazlar arasında veri transferi arada herhangi bir başka cihaza gerek kalmadan kendi aralarında gerçekleştirilerek karşı cihaza aktarılır. Birbirilerine kablosuz bağlantılarla bağlı gezici yönlendiriciler sistemine dayanması nedeniyle ağların yapılandırmaları düzensizlik arz eder. Yani, cihazlar öngörülemeyen bir şekilde hareket ettikçe bu ağların dinamik topolojiyi yönetebilecek şekilde yeniden yapılandırılması gerekir. Bluetooth ağlar, adhoc ağlar gibi davranabilir. Bluetooth'ta kullanılan yönlendirme protokolü, değişen ağları yönetmesine izin verir. Cihazlara entegre edilen mobil yönlendiriciler, bağlantı ve iletişim akışını kontrol eder.

Wi-Fi Alliance, Wi-Fi ticari markasına sahip kar amacı gütmeyen bir kuruluştur. Bu organizasyon çatısı altında üreticiler 802.11 tabanında oluşturulan ürünlerini test ederek sertifikalandırır. Wi-Fi logusu taşıyan ürünlerin sağlaması gerekli standartları belirtme ve sürümlendirme için *Wi-Fi kuşakları* (generations) isimlendirilmesi kullanılmaktadır. Wi-Fi kuşaklarının özellikleri aşağıdaki tabloda yer almaktadır: ("Wi-Fi Alliance," 2023)

Kuşak	IEEE Standardı	En yüksek hız (Mbit/s)	Yıl	Radyo Frekansı (Ghz)
Wi-Fi 7	802.11be	46120	(2024)	2.4/5/6
Wi-Fi 6E	802.11ax	9608	2020	2.4/5/6
Wi-Fi 6	802.11ax	9608	2019	2.4/5
Wi-Fi 5	802.11ac	6933	2014	5
Wi-Fi 4	802.11n	600	2008	2.4/5
Wi-Fi 3	802.11g	54	2003	2.4
Wi-Fi 2	802.11a	54	1999	5
Wi-Fi 1	802.11b	11	1999	2.4
Wi-Fi 0	802.11	2	1997	2.4

Tablo 1: Wi-Fi Kuşakları

4.3. Bilgi sistemleri Altyapısı Risk Alanları

Bütün kontrollerde benzer şekilde olduğu üzere; etkili bir kontrol tasarımından önce kontrol hedeflerinin ve olası risklerin anlaşılması gerekir. Bu yönde; muhtemel zafiyetlerin olasılığını ve etkisini ele alacak bir kontrol ortamının geliştirilebilmesi için risk altındaki varlıklar belirlenmeli ve varlıklara yönelik tehditler anlaşılmalıdır. Öncelikle ağ güvenliği sağlanamadığı takdirde, bir şirketin karşılaşabileceği en yaygın riskler aşağıdaki gibidir: (Cascarino, 2012)

- İtibar kaybı
- Gizlilik kaybı
- Bilgi bütünlüğü kaybı
- Kullanıcı doğrulama hatası
- Sisteme erişilememesi

Kim and Solomon (2021), bir şirket bünyesinde bilgi sistemleri ve ağ altyapısını yedi alana bölerek incelemektedir. (*Şekil 27*) Bilgi sistemleri altyapısı donanım ve yazılım unsurlarıyla bir şekilde bir ağa veya İnternet'e bağlı bulunmaktadır. Bu durum içeriden ve dışarıdan bilgi sistemlerinin tehditlere açık olması manasını taşımaktadır. Ek olarak, bilgi sistemlerinin tasarım, uygulama veya yazılım kaynaklı zafiyetleri bulunmaktadır. Bilgi sistemleri altyapısının bölümlere ayrıldığı bu çerçeveyle ağ güvenliğinin sağlanması açısından ağ ortamıyla birlikte ağa temas eden bütün alanlarda güvenlik tedbirlerinin alınması sağlanarak katmanlı bir güvenlik yaklaşımı uygulanabilir. Bilgi sistemleri alanları ve bu alanlar özelinde odaklanılması gereken risk, tehdit veya zafiyetler aşağıda açıklanmaktadır:

Şekil 27: Bilgi Sistemleri Altyapısı Risk Alanları

- **Kullanıcılar:** Katmanlı güvenlik yaklaşımının ilk halkası kullanıcılar alanı şirket bilgi sistemlerine erişmek isteyen insanları ve süreçleri tanımlamaktadır. Kullanıcılar kendilerine verilen yetkiler dahilinde sistemlere, uygulamalara ve bilgiye erişmektedir. Kullanıcılar kullandıkları bilgi sistemlerinin güvenliğinden sorumludur. Bu alandaki riskler;
  - Güvenlik konusunda farkındalık eksikliği
  - Kasıtlı kötü amaçlı etkinlikler

- Sosyal mühendislik ve oltalama saldırıları
- Kullanıcı ihmali ve hatası

• **İş istasyonları:** İş istasyonları ağa bağlantı sağlayan masaüstü bilgisayar, dizüstü bilgisayar, akıllı telefon, tablet vb. son kullanıcı cihazlarıdır. İş istasyonları kendi üzerinde kurulu uygulamalara, disk alanlarına sahip olarak verileri yerel olarak işleyip saklayabileceği gibi verilerin işlenmesi ve saklanmasına ilişkin tüm işlemler sunucu kaynakları üzerinde veya bulut ortamlarında da gerçekleştirilebilir. İkinci savunma katmanının olması gereken bu alandaki riskler şu şekildedir;

- Yetkisiz kullanıcı erişimi
- Zararlı yazılımların bulaşması
- İşletim sistemlerinde güvenlik açıklıkları
- Kullanıcıların sahip olduğu cihazlar (BYOD)

• **Yerel alan ağları:** Yerel alan ağında iletişimi sağlayan kenar anahtar, yönlendirici, kablosuz erişim noktaları vasıtasıyla iş istasyonları için kablolu veya kablosuz kurumsal ortak bir bağlantı ortamı oluşturulur. Şirket genelinde sistem, uygulama, servislere erişilebildiği gibi İnternet'e erişim de bu alan üzerinden gerçekleşir. Bu alanda üçüncü savunma katmanı olarak etkili güvenlik ve erişim kontrolleri gerekir. Ağ cihazlarının işletimi ve yönetimi etkin bir şekilde gerçekleştirilmelidir. Yerel alan ağları riskleri aşağıda listelenmektedir;

- Katmansız düz ağ tasarımı
- Yerel alan ağına yetkisiz erişim
- Gizli bilgilerin güvensiz ortamlarda saklanması, şifresiz bir şekilde transferi
- Zararlı yazılımların yayılması

• **Yerel/Uzak Arası Alan:** Bu alan, kurumsal yerel alan ağının, uzak bölgelere veya İnternet'e bağlandığı sınır bölgesidir. Şirketin dış dünyayla erişim ihtiyacı için uzak alan bağlantıları kolaylıkla sağlanmalıdır. Bunun yanında İnternet'e bağlı olmak, İnternet'ten gelebilecek tehlikelere karşı hazır olmayı da gerektirir. Bu alan yönlendiriciler, güvenlik duvarları, saldırı tespit/önleme sistemleri vb. güvenlik çözümleri, İnternet'e açık DMZ bölgeleri, vekil sunucular vb. işletimini ve yönetimini içerir. Ağın çevresel savunma katmanında ele alınması gerekli bazı riskler;

- İç kaynaklara yetkisiz erişim
- Zararlı yazılımlar
- Güvenlik cihazlarındaki zayıflıklar
- Uzak alan bağlantılarında kesinti

• **Uzak Alan Ağları:** Bu alan beşinci güvenlik katmanı olarak, uzak bölgelerin birbirine bağlandığı tüm harici şirketleri ve uç noktaları içeren ağ ortamını temsil eder. Telekomünikasyon hizmet sağlayıcıları, uzak alan bağlantısı ve İnternet üzerinden iletişim hizmeti verirler. Birçok şirket için uzak alan ağı sanal özel ağlar (VPN) ve tünelleme aracılığıyla İnternet üzerinden sağlanmasıyla birlikte noktadan noktaya kiralık hatlar vb. hizmetler de kullanılmaktadır. Uzak alan ağlarının riskleri;

- Kaynağı belirsiz zararlı yazılım saldırıları
- Servis dışı bırakma saldırıları
- Şifresiz transfer edilen bilgi
- Hizmet sağlayıcı ağ altyapısındaki zayıflıklar

• **Uzaktan Erişim:** Uzaktan erişim alanı, sahada veya evde çalışan kullanıcıların şirket kaynaklarına uzaktan erişimini içerir. Bu kapsamda, mahremiyeti sağlamak ve yerel alan ağındaki bilgi sistemlerinin güvenliğini tehlikeye atmamak gerekir. İnternet ortamından kurum içi kaynaklara uzaktan erişimle ilgili gerekli kimlik tanıma, doğrulama, yetkilendirme kontrolleri sağlanmalıdır. Uzaktan

erişimde mobil cihazların kullanımı ve uzaktan erişilen, işlenen veya depolanan bilgiyi korumak için aşağıdaki riskler göz önünde bulundurulmalıdır;

- Mobil cihazların kaybolması
- Bilgi sistemi kaynaklarına yetkisiz erişim
- Zararlı yazılımlar
- Güvensiz İnternet bağlantısı

• **Sistem/Uygulamalar:** Sistem, uygulamalar ve kurumsal verinin bulunduğu alanı temsil eder. Saldırganlar, güvenliğin uygulandığı bu son katmandaki sistem ve uygulamaların kontrolünü ele geçirmek ve bu sayede kurumsal bilgiye erişmek isterler. Ağ güvenliğinin sağlanmasına yönelik uygulanan bütün kontroller esas olarak sistem ve uygulamaları ve üzerlerindeki bilgiyi korumak içindir. Bilgi sistemlerinin geliştirilmesi ve uygulanması, işletimi, operasyonu, sürekliliği bu alandaki kritik hususlar olup bu alandaki belli başlı riskler aşağıdaki gibidir;

- Fiziksel veya mantıksal yetkisiz erişimler
- Yazılımsal veya donanımsal arızalar
- Sistem ve uygulamalarda güncelleme eksikliği
- Konfigürasyon eksikliği

Bilgi sistemleri ve ağ altyapısında görüldüğü üzere birçok risk, tehdit ve zafiyet bulunmaktadır. Kötü amaçlı yazılım, donanım veya yazılım hatası, dahili veya harici saldırgan, hırsızlık, doğal afet, casusluk, terörizm en yaygın tehditlerdir. Bilgi sistemlerindeki zafiyetler risk oluşturmakta tehditler bu zafiyetleri kullanarak bilgi sistemlerinde gizlilik, bütünlük ve erişilebilirlik açısından sorunlara yol açmaktadır. Özellikle kötü niyetli tehditler; şirketler için kritik verilerin kaybı, finansal bilgilerin veya fikri mülkiyetin çalınması gibi daha yaygın sorunlara yol açabilmektedir. Bilgi sistemleri ağ ortamına bağlanması ve İnternet'e erişim sağlaması nedeniyle güvenliği tehlikeye atabilecek ilk saldırılar bu noktalardan olmaktadır. Şimdi önümüzdeki bölümde bu alanda karşımıza çıkabilecek kavramlar üzerinde durulacaktır.

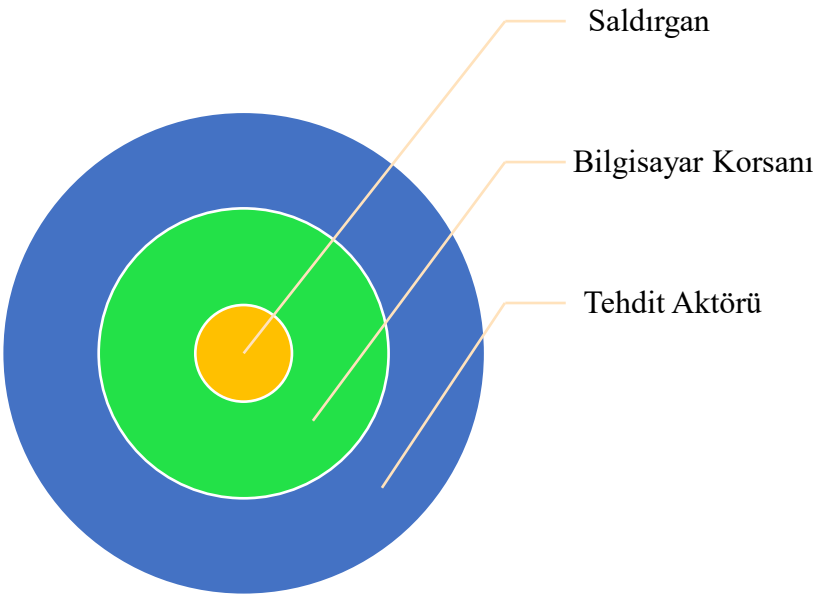
4.4. Tehdit Kişileri

Bilgi sistemlerinin güvenliğini sağlamak için onu tehdit eden kişileri tanımak faydalı olacaktır. Şirketin içinden veya dışından gerçekleştirilebilecek saldırıların failleri fırsatçı veya iyi planlanmış ve hedefli olabilir. Bireyler veya gruplardan oluşabilirler ve motivasyonlarına ve taktiklerine göre hacktivist, terörist, endüstriyel casus, ulus devlet, siber suç sendikası veya bilgisayar korsanı şeklinde adlandırılabilir. Kötü amaçlı faaliyetleri gerçekleştiren bu kişiler için kullanılan kavramlar şu şekildedir:

• **Tehdit aktörü (Threat Actor):** TechTarget'a göre, kötü niyetli aktör olarak da adlandırılan bir tehdit aktörü, bir kuruluşun güvenliğini etkileyen veya etkileme potansiyeli olan bir olaydan kısmen veya tamamen sorumlu olan bir varlıktır.

• **Bilgisayar korsanı (Hacker):** Merriam-Webster'a göre, yasadışı bir şekilde bir bilgisayar sistemindeki bilgilere erişim sağlayan ve bazen bu bilgilere müdahale eden kişi.

• **Saldırgan (Attacker):** Siber güvenlikte saldırgan, kaynaklara, varlıklara veya verilere yok etmeye, ifşa etmeye, değiştirmeye, devre dışı bırakmaya, hizmetleri reddetmeye, çalmaya veya yetkisiz erişim elde etmeye çalışan bir kişi, kuruluş veya yönetilen kötü amaçlı yazılımdır (Haber, 2020)."



Şekil 28: Tehdit Kişileri

Tehdit aktörü; diğerlerini de kapsayan dış ve iç tehditler için kullanılan en geniş terimdir. Teknik bir becerisi olabilir ama olması da gerekmez. Saldırı veya hacking gerçekleştirilmeyen durumlar için de kullanılabilir. Bir şirketin güvenliğini tehlikeye atma misyonu, görevi olan kişi veya kuruluş olabilir. (*Şekil 29*) (Haber, 2020) Bilgisayar korsanı ve saldırgan ise ihlal olayını gerçekleştiren kasıtlı olarak teknolojiyi hedefleyen kişilerdir. Dünyanın herhangi bir yerinde bir işletmeyi, hükümeti istikrarsızlaştırmak, bilgi yaymak veya mali kazanç sağlamak amacıyla hareket edebilirler. Bilgisayar korsanları terimi geleneksel olarak faaliyetlerini yürütmek için bilgi sistemlerindeki güvenlik açıklıklarını ve istismarları kullananlar için kullanılır. Saldırgan da bilgisayar korsanı olabilir ama tahribat yaratmak için herhangi bir yöntem kullanabilir. Mesela, saldırgan olarak içeriden bir çalışan yetkilerini kullanarak hassas dosyaları silebilir veya bir işlemi bozabilir. Bu olayı bilgisayar korsanı yaptığı takdirde bilgi sistemlerindeki güvenlik açıklıklarını, yanlış yapılandırmaları kullanır (Aydın, 2020).

Dışardakiler

- Devlet destekli gruplar
- Siyasi eylemciler
- Organize suç örgütleri
- Fırsatçı kişiler
- Siber teröristler

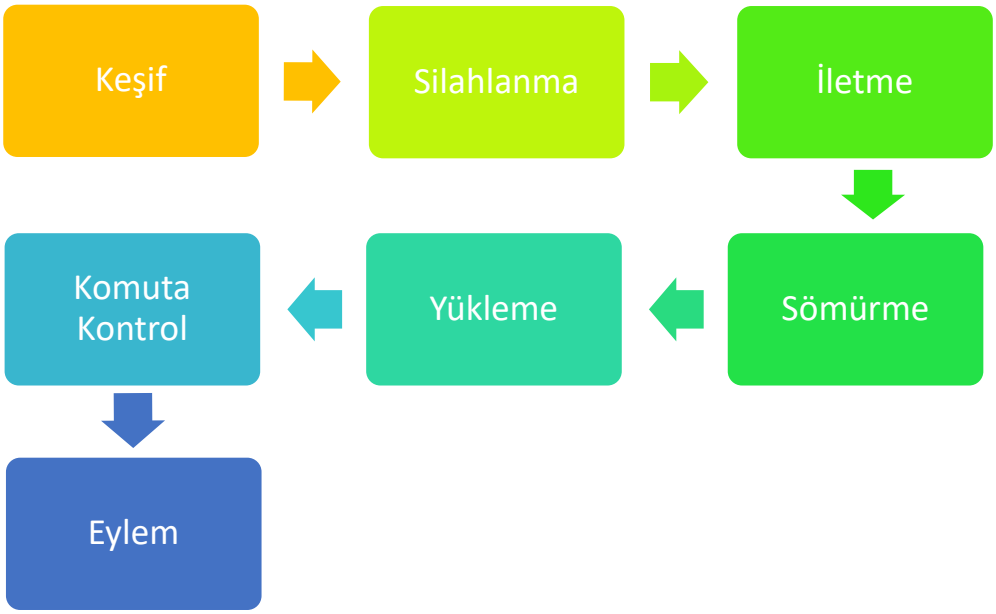
İçerdekiler

- Sistem yöneticileri
- Yazılım geliştiricileri
- Son kullanıcılar
- Veri sahipleri
- Yükleniciler
- Güvenilir üçüncü taraflar

Şekil 29: Tehdit Aktörleri

4.5. Saldırı Aşamaları

Bilgi sistemlerine yapılan saldırıların türleri farklı olsa da takip ettikleri adımlar benzerlik göstermektedir. Bir tehdit aktörünün saldırı geliştirme mantığını ve adımlarını anlamak bilgi sistemlerinin maruz kaldığı tehditlere karşı önlem almak için faydalı olacaktır. *Siber Ölüm Zinciri (Cyber kill chain)* olarak adlandırılan saldırıların nasıl gerçekleştirildiğine dair adımları içeren metodolojinin detaylarına aşağıda yer verilmektedir: (Şeker, 2019)



Şekil 30: Saldırı Aşamaları

- **Keşif (Reconnaissance):** İlk adım olarak, saldırı yapılacak hedefle ilgili ağa bağlı bilgisayarlar, bu bilgisayarlar veya ağdaki zafiyetlerin bilgisi toplanır. Bilgi toplama aktif bilgi toplama veya pasif bilgi toplama şeklinde olabilir. Aktif bilgi toplama esnasında bilgi sistemleri ile etkileşime geçilir. Mesela, açık portları tespit etmek için bir sistem üzerinde port taraması yapılmaktadır. Pasif bilgi toplama da ise keşif sürecinde hedef sistemle herhangi bir etkileşime girilmez. Arama motorları gibi farklı kaynaklardan bilgi toplamaya çalışılır (Diogenes & Ozkaya, 2019).

- **Silahlanma (Weaponization):** Siber ölüm zincirinin ikinci aşamasında, hedefe ulaşmak için nasıl bir yol izleneceği belirlenir. Keşif aşamasında toplanan bilgiye dayanarak tespit edilen zafiyetlere yönelik kötü amaçlı yazılımlar hazırlanır.

- **İletme (Delivery):** Bu aşamada, hedef sistemi sömürmek için hazırlanan zararlı yazılımların/ silahların hedeflenen sisteme ulaştırılması sağlanmaktadır.

- **Sömürme (Exploitation):** Kurban üzerindeki mevcut zafiyetlerin kullanılması için kurbana iletilmiş olan zararlı yazılım uzaktan veya otomatik olarak çalıştırılarak hedef sisteme erişimin sağlanması aşamasıdır.

- **Yükleme (Installation):** Hedef sistemin sömürülmesiyle birlikte zararlı yazılımların sistem üzerinde yüklenmesi sağlanır. Hedef sistemden kendini gizlemek ve iz sürülemez hale gelebilmek için İnternet üzerinden ek güncellemeler indirilerek kullanılmaya çalışılır.

- **Komuta kontrol (Command and control, C2):** Zararlı yazılımın bulaştığı hedef sistemin saldırgan tarafından erişilebildiği ve kontrol merkezi üzerinden kontrol edilebildiği iletişim kanalının oluşturulduğu aşamadır.

• **Eylem (Actions on objectives):** Son aşamada, hedef sistem üzerinden veri çalma, değiştirme, silme, ağ ortamında başka noktalara sıçrama gibi nihai hedefe yönelik işlemler gerçekleştirilir.

Şekil 31: Saldırı Zinciri

Saldırı esnasında bu aşamalar zincirleme birbirine bağlıdır. Haber and Hibbert (2018), *Şekil 31*'de görüldüğü gibi bu saldırı zincirini tanımlamaktadır. Kısacası; bilgi sistemlerine saldırı süreci bilgi sistemlerinin keşif aşaması gerçekleştirilerek zafiyetlerinin bulunması, zafiyetler kullanılarak erişim sağlanması, orada kalıcı olmaya çalışması ve geride iz bırakmayacak şekilde hedeflenin eylemlerin gerçekleştirilmesi ile başarıya ulaşmaktadır. Saldırılar *Şekil 32*'de gösterildiği üzere dört grupta sınıflandırılabilir ve saldırıların dört temel amacı şu şekildedir: (Kim & Solomon, 2021)

• **Erişimi engelleme:** Bilgi sistemlerinin hizmet vermesinin engellenmeye çalışılması.

• **Verileri değiştirme:** Bilgi sistemleri üzerindeki konfigürasyon veya kullanıcı bilgilerinin değiştirilmesi, silinmesi.

• **Veri sızdırma:** Bilgi sistemleri üzerindeki verinin dışarı aktarılması.

• **Başka noktalara sıçramak için başlangıç noktası olarak kullanma:** Hedef bilgi sistemine ulaşmak için başka bilgi sistemlerinin ele geçirilerek kullanılmaya çalışılması.

Şekil 32: Saldırı Tipleri

4.6. Saldırı Vektörleri

Saldırı vektörü Haber (2020) tarafından şu şekilde tanımlanmaktadır:

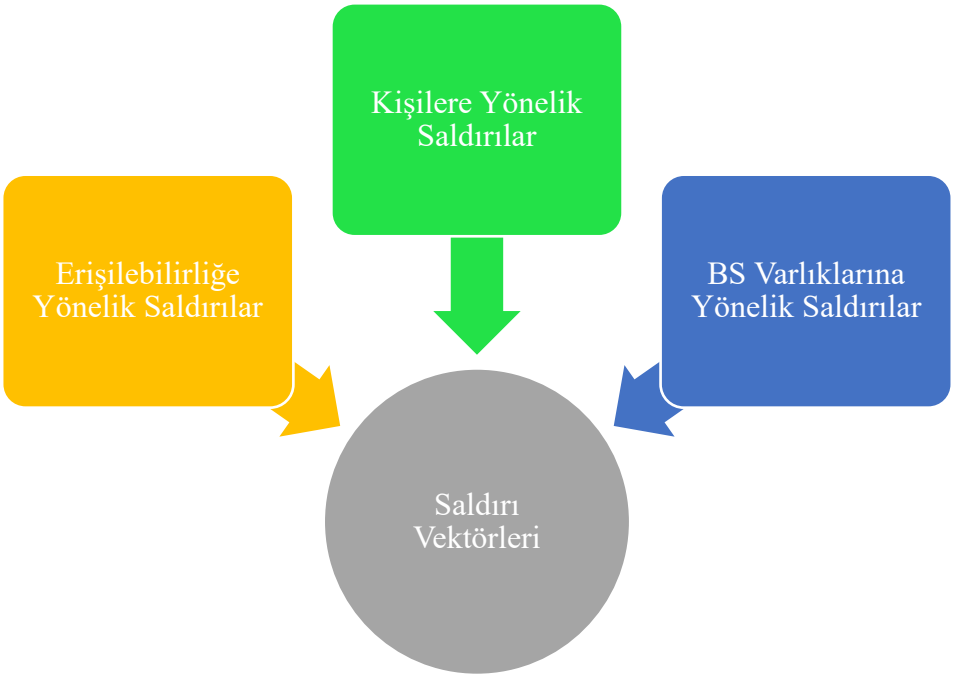
"Saldırı vektörü, bir bilgisayar korsanının, saldırganın veya tehdit aktörünün kötü niyetli bir sonuç işlemek için bir bilgisayara veya ağ kaynağına erişim sağlayabileceği bir yol veya araçtır. Saldırı vektörleri, ayrıcalıklara, varlıklara ve kimliklere (hesaplara) dayalı olarak kaynakların sömürülmesini sağlar ve teknoloji ile insan unsurlarını içerebilir."

Saldırganların amaçlarına göre bilgi sistemlerine tehdit oluşturan birçok saldırı türü bulunmaktadır. Saldırı vektörlerini aşağıdaki gibi 3 kategori altında sınıflandırmak mümkündür:

- **Erişilebilirliğe yönelik saldırılar:** Kritik bir sistem, uygulama veya veriye erişimleri etkileyen saldırılardır.

- **Kişilere yönelik saldırılar:** Bir kişinin zorlama veya aldatma ile istenilen bir eylemi gerçekleştirmesini ve bilgilerini ifşa etmesini sağlamak için kullanılan saldırılardır.

- **Bilgi sistemi varlıklarına yönelik saldırılar:** Sızma testi, yetkisiz erişim, yetki yükseltme, çalınmış parolalar, verilerin silinmesi, veri sızıntısı içeren saldırılardır. (Kim & Solomon, 2021)



Şekil 33: Saldırı Vektörleri

4.7. Sosyal Mühendislik Saldırıları

Sosyal mühendislik "gizli veya hassas bilgileri açığa çıkarmak için hedef bölgedeki kullanıcıları veya yöneticileri aldatmaya dayalı bir saldırı (ISACA, 2018)." olarak tanımlanmaktadır. Sosyal mühendislik saldırılarında güvenliğin en zayıf halkası insan faktörü hedef alınır ve özellikle kimlik hırsızlığına yönelik tehdit aktörleri tarafından kurbanlarının kendileri veya başkaları hakkında sahip olduğu bilgileri vermesi sağlanmaya çalışılmaktadır. Bilgi sistemleri özelinde temel amaç bilgi sistemi kullanıcılarından sisteme giriş için gerekli oturum açma bilgilerini elde edebilmektir. Bu yöntemle, teknik bilgiye ihtiyaç duymadan ikna kabiliyeti ve aldatma yöntemleriyle bilgi sistemlerine erişimle ilgili alınmış tedbirler aşılmış olmaktadır. Sosyal mühendislik saldırı taktiklerinden bazılarına aşağıda yer verilmektedir: (Kim & Solomon, 2021)

- **Otorite (Authority):** Bir otorite konumu kullanılarak bilgiyi ifşa etmeye yönelik bir bireyin ikna edilmesi ve zorlanması.

- **Uzlaşma/Sosyal kanıt (Consensus/social proof):** Bir bireyi yapması istenilen bir hususa ikna etmek için, herkesin gerçekleştirdiği bir şeyi yapabileceği düşüncesinin kullanılması.

- **Çöplük dalışı (Dumpster diving):** Çöpler karıştırılarak bir bireye ait hassas ve özel bilgilerin aranması.

- **Aşinalık/hoşlanma (Familiarity/liking):** Bir bireyle yakınlık oluşturularak bir şey yapmasını sağlamak.

- **Aldatmaca (Hoax):** Yanlış bir algı yaratarak bir bireyin bir şeyi yapması veya bilgiyi ifşa etmesi için inandırılması.

- **Kimliğe bürünme (Impersonation):** Banka temsilcisi, yardım masası personeli gibi başka birisi gibi davranılması.

- **Tehdit (Intimidation):** Bir bireyin bir şeyi yapması ve bilgi ifşası için gözünü korkutma, yıldırma, güç kullanma.

- **Kıtlık (Scarcity):** Bir şeye sahip olamama veya bir şeyi kaybetme korkusuyla istenilen şeylerin baskıyla yaptırılması.

• **Omuzda gezinme (Shoulder surfing):** Bir kişiyi bilgi girişi esnasında izleyerek hassas ve özel bilgilerinin elde edilmesi.

• **Sms oltalama (Smishing):** SMiShing, kısa mesaj (SMS) yoluyla oltalama (Phishing) saldırısı.

• **Yancı geçiş (Tailgating, Piggybacking):** Güvenli bir alana yetkili bir kişiyi yakından takip ederek gizlice girilmesi.

• **Güven (Trust):** Bir insan ile arada kurulan güven bağını istenilen bir şeyi yapması için kullanmak.

• **Saflık (Gullibility):** Geçerli kimlik bilgilerine sahip kullanıcıların yetersiz eğitim, güvenlik farkındalığı eksikliği, kolayca aldatılabilmesinin kullanılması.

• **Aciliyet (Urgency):** Bir aciliyet durumu oluşturarak birinin bir şey yapmasını veya bilgi ifşa etmesinin sağlanması.

• **Sesli oltalama (Vishing):** Sesli oltalama (Voice phishing) telefonla konuşarak sözlü zorlama veya ikna yoluyla bir kimlik avı saldırısı yapılması.

• **Balina avcılığı (Whaling):** Yönetici kullanıcıları veya şirket açısından değerli çalışanların hedef alındığı oltalama saldırısı.

4.8. Kablosuz Ağ Saldırıları

Kablosuz ağlar; bilgi sistemleri altyapısına bir erişim noktası olarak müdahaleci izleme (intrusive monitoring), paket yakalama (packet capturing) ve sızma testi (penetration test) gerçekleştirmeyi kapsayan ataklara maruz kalmaktadır. Bilgisayar korsanları tarafından kablosuz ağlara sızmaya ve saldırmaya yönelik ağ saldırı taktikleri aşağıda kısaca açıklanmaktadır: (Kim & Solomon, 2021)

• **Bluejacking:** Bluetooth cihazlara anonim kısa mesajlar gönderilmesi.

• **Bluesnarfing:** Bluetooth cihazları arasındaki iletişim trafiğini dinleme.

• **Kötü ikiz (Evil twin):** Halka açık bir kablosuz ağa bağlanan cihaz ile erişim noktası arasındaki trafiği dinlemek için gerçek yayını taklit etmek.

• **IV saldırısı (IV attack):** Ortak bir şifreleme anahtarını zamanla çözmek amacıyla transfer edilen şifreli bir IP paketinin ilklendirme vektörünü (Initialization Vector) değiştirme.

• **Frekans bozma/enterferans (Jamming/interference)**: Kablosuz erişim noktalarının yayın yaptığı frekanslarda yayın yapılması neticesinde kablosuz iletişim ortamının bozulması ve kullanıcıların erişiminin engellenmesi.

• **Yakın alan iletişim saldırısı (Near field communication attack):** İki mobil cihazın NFC iletişiminin engellenmesi.

• **Dinleme (Sniffing):** Bir kablosuz ağ üzerinden geçen paketlerin yakalanması ve farklı araçlarla analiz edilmesi.

• **Yeniden oynatma saldırısı (Replay attack):** Kablosuz ağ üzerinden yakalanılan bir IP paketinin sunucuya tekrar gönderilip sunucunun yetkili bir kullanıcıyla iletişim kurduğunu düşünmesi sağlanarak kandırılması.

• **Sahte erişim noktası (Rogue access point):** Yetkisiz bir ağ erişim noktası kullanılarak şüphelenmeyen kullanıcılara kablosuz erişim sağlanması.

• **Savaş tebeşiri (War chalking)**: Kablosuz ağların fiziksel ve coğrafi konumlarının belirlenerek özelliklerine göre işaretlenmesi.

• **Savaş sürüşü (War driving):** Bir arabayla gezerek açık bir kablosuz ağ bağlantısı aranması.

• **Zayıf şifreleme:** Kablosuz erişimde kullanılan WEP, WPA, WPS gibi şifreleme protokollerinin zayıflıklarından yararlanılması.

4.9. Web Uygulama Saldırıları

İnternet üzerinde çalışan herkese açık web uygulamaları, saldırganların bir diğer hedef noktasıdır. Web uygulamalarına sızmaya ve saldırmaya yönelik kullanılan taktikler aşağıda yer almaktadır: (Kim & Solomon, 2021)

• **Uzaktan kod yürütme (Remote code execution):** Sistem yönetim hakları veya ayrıcalıklarıyla erişim sağlanarak istenilen komutların uzak sistem üzerinde çalıştırılması.

• **Bellek taşması (Buffer overflow):** Bir programın veya işlemin beklenenden daha fazla veriyi ara belleğe depolamaya çalışması durumunun hedef sistemde istenilen kodların çalıştırılması için kullanılması.

• **İstemci tarafı saldırısı (Client-side attack):** Bir yerel alan ağındaki iş istasyonlarında veya bilgisayarlarda bulunan zararlı yazılımın İnternet üzerindeki bir sunucu ile birlikte hareket ederek kullanılması.

• **Çerezler ve Ekler (Cookies and attachments):** Web tarayıcılarında tutulan çerezlerin ve zararlı içerik barındıran dosya eklerinin kullanılması.

• **Çapraz site betik saldırısı (Cross-site scripting-XSS):** Bir web uygulama sunucusuna zararlı komut dosyalarının enjekte edilerek web sitesini erişmek isteyen bilgisayarların istismar edilmeye çalışılması.

• **Çapraz site talep sahteciliği (Cross-site request forgery-CSRF):** Hedef web sitesi üzerinde gerçekleştirilmek istenen işlemlere yönelik hazırlanmış zararlı kodların, halihazırda bu sitede kullanıcı oturumu açık durumda bulunan bilgisayarlardan farkında olmadan hedef web sitesine gönderilmesini sağlayacak şekilde kimliği doğrulanmış bir kullanıcının oturumundan yararlanılması.

• **Dizin geçişi/komut yerleştirme (Directory traversal/command injection):** Bir web sunucusunun istismar edilerek kök dosya dizinine erişim elde edilmesi ve istenilen komutların çalıştırılabilmesi.

• **Başlık manipülasyonu (Header manipulation):** Http yanıt başlık bilgilerinin değiştirilerek iletişimin güvenliğinin bozulması.

• **Tam sayı taşması (Integer overflow):** Bir tam sayı değerinin sabit boyutu gereği alabileceği maksimum bir değer vardır. Bu değerin aşılması tamsayı taşması oluşturur ve bu durumlar bir uygulamada kararsızlık veya güvenlik açıklığına neden olabilir.

• **Basit Dizin Erişim Protokolü (LDAP) enjeksiyonu:** Bir web uygulamasının istismar edilerek LDAP sunucusuna gönderilen komutların değiştirilmesi neticesinde hassas kullanıcı bilgilerinin elde edilmesi veya değiştirilmesi.

• **Yerel paylaşılan nesneler (LSO):** Flash çerezleri olarak da bilinen verilerin kullanılması.

• **Zararlı eklentiler (Malicious add-ons):** Meşru programlardaki kötü niyetli yazılım eklentilerinin kullanılması.

• **SQL enjeksiyonu (SQL injection**): Bir web sunucusundan arka uç veritabanlarına gönderilen Structured Query Language (SQL) komutlarını değiştirilmesi.

• **Sulama deliği saldırısı (Watering hole attack):** Bir kişi veya grup tarafından sıklıkça ziyaret edilen sitelere kötü niyetli kod ve yazılımın gizlenerek bu kişilere dolaylı yoldan saldırılması.

• **XML enjeksiyonu (XML injection):** Bir uygulama veya servise Extensible Markup Language (XML) etiketleri ve verileri enjekte edilmeye çalışılması.

• **Sıfır gün (Zero day):** Bir güncelleme veya savunmanın bulunmadığı yeni zafiyet ve yazılım hatalarının kullanılması.

4.10. Zararlı Yazılımlar

Zararlı yazılımın İngilizce karşılığı *malware*, *malicious* ve *software* kelimelerinin kısaltmasıdır. Bilgi sistemlerine gizlice sızmak, hasar vermek veya bilgi sızdırmak için genellikle tehdit aktörleri tarafından tasarlanmış bu kötü amaçlı yazılımların aşağıdaki gibi farklı tür ve kaynakları bulunmaktadır: (Haber, 2020)

- **Yazılım hatası (Bug):** Yazılım hatası tek başına bir zararlı yazılım olmasa da bir yazılım veya uygulamada istismarlara açık zafiyetler oluşturmaktadır. Yazılım hataları zayıf kodlama veya beklenmeyen çalışma koşullarından kaynaklanabilen hatalı ve istenmeyen sonuçlara yol açan kusur, başarısızlık, yanlışlık veya arıza olarak tanımlanabilir.

- **Solucan (Worm):** Solucanlar yazılım açıklıklarını ve zayıflıkları kullanarak kendi kopyalarını başka kaynaklara üzerinde bulunduğu ana bilgisayarın ağ erişimi vasıtasıyla yaymaya çalışır. Bir virüs çeşidi olmakla birlikte bağımsız programlardır, virüsler gibi hayatta kalmak veya yayılmak için ana bilgisayar üzerindeki bir programa ihtiyaç duymazlar. Ana bilgisayara ilk bulaşmaları ekler ve dosya indirmeler üzerinden gerçekleşebilir fakat daha sonra ağ ortamını tarayarak zafiyet içeren sistemler üzerinden yayılabilirler. Bu bağlamda solucan terimi, solucanların ağ üzerinden iletişim kuran ve farklı bilgisayarlar üzerinde çalışan program bölümlerinden oluşmasından kaynaklanmaktadır (Kim & Solomon, 2021). Kendi kendini yayarak farklı sistemlere bulaşabilen fidye yazılımı bir solucan çeşididir.

- **Virüs (Virus):** Bir bilgisayar virüsü farkında olunmadan bir bilgisayara yüklenen "diğer programları, bunların içine kendisinin bir kopyasını içerecek şekilde değiştirerek çoğaltma becerisine sahip bir program (ISACA, 2018)" parçasıdır. Virüsler temel olarak sistemlere, programlara veya dosyalara bulaşabilir. Sistemlere bulaşan virüsler bilgisayar, aygıt donanımlarını ve yazılım başlatma işlevlerini hedef alırken, çalıştırılabilir dosyalara bulaşan virüsler veya ofis dokümanları üzerinde makro gibi çalıştırılabilir özellikleri kullanan virüsler de bulunmaktadır. Virüslerin temel özelliği çoğalması ve çoğunlukla bir kullanıcı eylemi içermeleridir. Virüslerin amaçları çeşitli olabilir, sadece yayılmaya odaklanan virüsler olduğu gibi arka kapı oluşturularak kötü niyetli eylemler için tetiklenmenin beklendiği durumlar da söz konusu olabilir (Kim & Solomon, 2021).

- **Bot:** Botlar, belirli görevleri gerçekleştirmek için tasarlanmış kötü amaçlı yazılım programlarıdır. Tehdit aktörleri tarafından spam e-postalar göndermek veya bilgi sistemlerine hizmet dışı saldırıları gerçekleştirmek için kullanılabilir.

- **Truva Atı (Trojan):** Truva atı kendini normal bir dosya veya uygulama olarak gizler ve kullanıcının indirmesi, açması ve yürütmesi için kandırır. Truva atları kolaylıkla tespit edilemeyebilir, kullanıcı tarafından sürekli kullanılmaya devam edilebilir. Virüslerden ayırt edici özellikleri kendini kopyalamayan zararlı programlar olmalıdır. Bununla birlikte truva atları bulaştığı cihazları ele geçirip arka kapı oluşturarak uzaktan kontrole imkan sağlarlar ve her türlü veri hırsızlığı vb. amaç için kullanılabilir. Virüsler, meşru bir programla birlikte gizlenen ve yayılan bir kod olmaları ve herhangi bir programa bulaşarak programı truva atına dönüştürebilmeleri nedeniyle bir truva atı türü olarak görülebilse de virüs üzerine bulaştığı ana bilgisayardan ziyade sadece bulaşıcı kodu ifade eder. Truva atı terimiyse, kasıtlı olarak yanıltan ve değiştirilmiş ve kendini yeniden oluşturmayan programı ifade eder (Kim & Solomon, 2021).

- **Fidye Yazılımı (Ransomware):** Fidye yazılımlarıyla ele geçirilen bilgi sistemleri üzerindeki veriler şifrelenip söz konusu verilere erişmek için fidye talep edilmektedir.

- **Reklam Yazılımı (Adware):** Reklam yazılımları, genellikle bilgisayara kurulan programlarla birlikte gelir ve istenmeyen reklamları otomatik olarak kullanıcıya gösterirler. Gösterilen reklamlar, kötü amaçlı sitelere yönlendirebileceği gibi kötü amaçlı yazılımların bilgisayara bulaşmasına neden olabilir.

- **Casus Yazılım (Spyware):** Casus yazılımlar da reklam yazılımları gibi genellikle ücretsiz programlarla birlikte yüklenir. Bu zararlı yazılımlarla; bilgisayar üzerinde klavye, ekran, kamera, mikrofon etkinlikleri veya kullanıcının ziyaret ettiği web siteleri bilgileri toplanıp mahremiyet ve gizlilik etkilenmektedir.

4.11. Bilgi sistemleri ve ağ güvenliği tedbirleri

Bilgi sistemleri ve ağ altyapısında görüldüğü üzere birçok risk, tehdit ve zafiyet bulunmaktadır. Bu noktaya kadar bu riskler anlaşılmaya çalışıldı. Önümüzdeki bölümde bu risklerin azaltılmasına ve ağ ve sistem güvenliğinin sağlanmasına yönelik tedbirler üzerinde durulmaktadır.

Tarihsel olarak bakıldığında ağ güvenliği konusunda şöyle bir ayrım vardı: Şirket çalışanları, yükleniciler ve ortaklar genel olarak güvenilir kabul edilirken bunların dışında kalan anonim kişilere güvenilmiyordu. Bu düşünceyi kullanarak saldırganlar tarafından artan biçimde ağlara sızmak için güvenilen kullanıcıları ele geçirme saldırıları gerçekleştirmeye başlandı ve bu nedenle günümüzde ağ güvenliği çözümlerinde sıfır güven yaklaşımı ön plana çıkmaktadır. Asla güvenmeyin, daima doğrulayın yaklaşımıyla birlikte her ağın sıfır güvenilir ağ olarak görülerek önlemlerin alınmasıyla saldırganların bir ağa gizlice sızmasının zorlaştırılması, önüne geçilmesi amaçlanmaktadır (Kim & Solomon, 2021). NIST, sıfır güven ile ilgili aşağıdaki açıklayıcı bilgileri vermektedir: (NIST, 2020a)

"Sıfır güven (ZT), savunmaları statik, ağ tabanlı çevrelerden kullanıcılara, varlıklara ve kaynaklara odaklanmak için hareket ettiren gelişen bir dizi siber güvenlik paradigması için kullanılan terimdir. Sıfır güven mimarisi (ZTA), endüstriyel ve kurumsal altyapı ve iş akışlarını planlamak için sıfır güven ilkelerini kullanır. Sıfır güven, varlıklara veya kullanıcı hesaplarına yalnızca fiziksel konumlarına veya ağ konumlarına (yani internete karşı yerel alan ağlarına) veya varlık sahipliğine (kurumsal veya kişisel olarak sahip olunan) dayalı hiçbir örtülü güven verilmediğini varsayar. Kimlik doğrulama ve yetkilendirme (hem konu hem de cihaz), bir kurumsal kaynağa oturum kurulmadan önce gerçekleştirilen ayrı işlevlerdir. Sıfır güven, uzak kullanıcılar, kendi cihazını getir (BYOD) ve kuruluşa ait ağ sınırı içinde yer almayan bulut tabanlı varlıkları içeren kurumsal ağ eğilimlerine bir yanıttır. Sıfır güven, ağ konumu artık kaynağın güvenlik duruşunun ana bileşeni olarak görülmediğinden, ağ segmentlerine değil, kaynakların (varlıklar, hizmetler, iş akışları, ağ hesapları vb.) korunmasına odaklanır"

İnternet erişiminin vazgeçilmez olduğu günümüzde, ağ güvenliğinin sağlanmasına yönelik belirlenmesi en zor alanın bir ağın tam olarak nerede başlayıp nerede bittiği olduğu söylenebilir. Tek bir şirket tarafından birçok iç ağı, uzak ofislerde bulunan ağlar, uzaktan çalışan ve/veya mobil kullanıcıları, bulut hizmetleri bulunmakta, karmaşık bir ağ ortamı işletilmektedir. Bu karmaşıklık, şirketlerin tek ve kolayca tanımlanabilen bir çevreye sahip olmaması, klasik çevre tabanlı ağ güvenliği yöntemlerini geride bırakılmasına yol açmaktadır (NIST, 2020a). Ağ çevresel savunması; her bir ağın güvenli bir şekilde korunan sınırlı sayıda giriş noktasına sahip olma temeline dayanır. Çoğu ağın artık çok fazla giriş noktasına sahip olması, bunun yanında ağdaki güvenlik kontrol noktası olarak güvenlik duvarlarının yüzde yüz etkili çalıştıkları, tüm tehditlerin dış kaynaklı olduğu varsayımlarının geçersiz olması, çevresel ağ savunmasını yetersiz kılmaktadır (Cascarino, 2012).

Sıfır güven yaklaşımıyla öncelikli olarak veri ve hizmetlerin korunmasına odaklanılmaktadır. Bununla birlikte; şirketin tüm varlıklarını (cihazlar, altyapı bileşenleri, uygulamalar, sanal ve bulut bileşenleri) ve öznelerini (son kullanıcılar, uygulamalar ve diğer bilgi talep eden insan dışı varlıklar) içerecek şekilde koruma genişletilmelidir. Sıfır güven güvenlik modelinde temel varsayım şirkete ait bir ortamın, şirket dışı bir ortamdan farklı veya daha güvenilir olmadığı ve saldırganın ortamda bulunduğu şeklindedir. Yani bu yaklaşımda hiçbir şirket dolaylı olarak güven varsayımında bulunmamalı, varlıklarına ve iş fonksiyonlarına yönelik riskleri sürekli analiz etmeli ve riskleri azaltmak için gerekli korumaları gerçekleştirmelidir. Korumalar genel olarak sadece erişime ihtiyacı olan öznelere ve varlıklara erişim izni verilerek, kaynaklara (veri, bilgi işlem kaynakları, uygulamalar, hizmetler) erişimin en aza indirgenmesini; her erişim isteğinin kimliğinin ve güvenlik durumunun sürekli olarak doğrulanmasını ve yetkilendirilmesini içermektedir (NIST, 2020a).

Şirketler, bilgi sistemleri güvenliğinin sağlanmasına yönelik kontrolleri geliştirmeli ve düzenli olarak bu kontrolleri izlemeli, test etmeli ve iyileştirmelidir. Bilgi sistemlerinin tehdit aktörlerine karşı savunmasında kullanılan en yaygın iki temel savunma stratejisi aşağıda listelenmektedir. Her iki yaklaşım birlikte kullanılarak bilgi sistemleri için dışarıdan veya içeriden tehditlere karşı en yüksek koruma sağlanmaya çalışılmalıdır. (Diogenes & Ozkaya, 2019)

- **Derinliğine savunma (defense in depth):** "Ek koruma sağlamak için katman seviyesinde savunma uygulaması. Derinlemesine savunma, bir saldırıda ihtiyaç duyulan çabayı artırarak güvenliği

arttırır. Bu strateji, bir saldırgan ile bir kuruluşun bilgi işlem ve bilgi kaynakları arasında birden fazla engel barındırır (ISACA, 2018)"

• **Genişliğine savunma (defense in breadth):** "Sistem, ağ veya ürün tasarımı ve geliştirme; imalat; paketleme; montaj; sistem entegrasyonu; dağıtım; operasyon; bakım ve devreden çıkarma dahil olmak üzere sistem, ağ veya alt bileşen yaşam döngüsünün her aşamasında istismar edilebilir zafiyetlerin riskini belirlemeyi, yönetmeyi ve azaltmayı amaçlayan planlı, sistematik çok disiplinli faaliyetler dizisi (NIST, 2020b)."

4.11.1. Derinliğine Savunma

Derinliğine savunma, saldırganların bilgi sistemlerine yetkisiz girişini zorlaştırmak için katmanlı savunma mekanizmalarının kullanılmasıdır. Bir şirketin bilgi sistemlerini, ağları ve verileri koruması için tek bir güvenlik katmanı yeterli değildir ve genel güvenlik düzeyini artırmak için birden çok güvenlik katmanı bir bütünün parçası olarak tasarlanıp devreye alınır. Bu şekilde, bir güvenlik katmanını aşan bir saldırgan başka güvenlik önlemleri ile karşılaşır ve bilgi sistemlerine sızması zorlaştırılır. "Örneğin, dosya sunucusunu korumak isteyen bir kuruluş, ağına izinsiz giriş tespit sistemi ve güvenlik duvarı kurabilir. Ayrıca sunucuya bir uç nokta antivirüs programı yükleyebilir ve içeriğini daha fazla şifreleyebilir. Son olarak, herhangi bir oturum açma girişimi için uzaktan erişimi devre dışı bırakabilir ve iki faktörlü kimlik doğrulamayı kullanabilir. Sunucudaki hassas dosyalara erişmeye çalışan herhangi bir saldırgan, tüm bu güvenlik katmanlarını başarıyla aşmak zorunda kalacaktır. Her güvenlik katmanının kendine özgü bir karmaşıklığı olduğundan başarı şansı çok düşüktür (Diogenes & Ozkaya, 2019)."

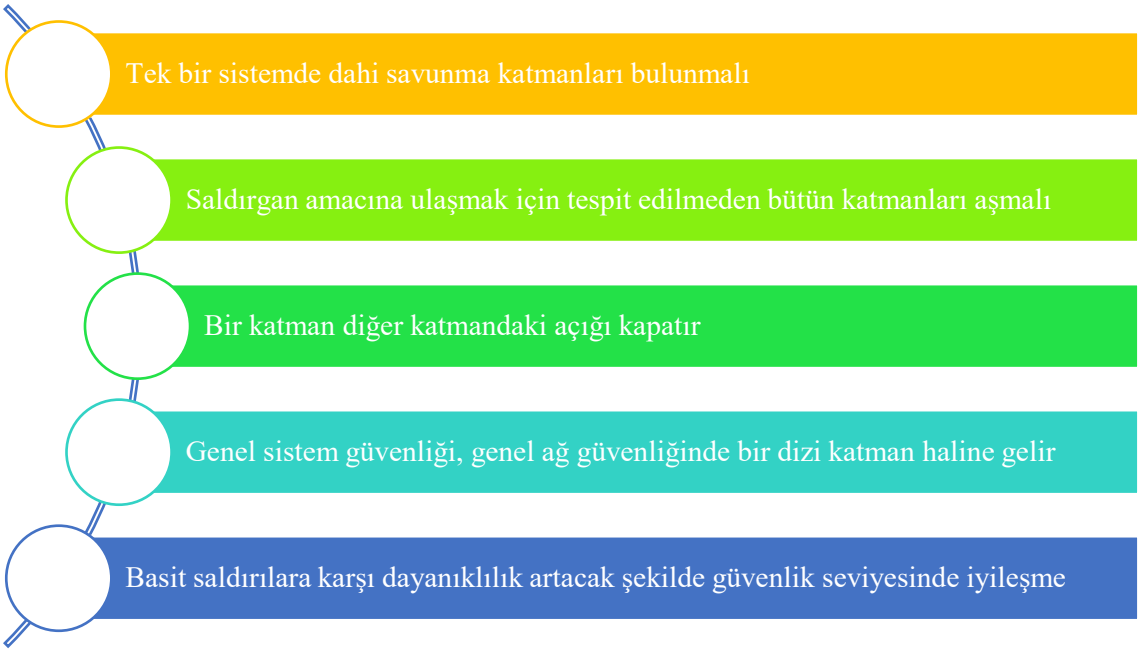
Diogenes & Ozkaya (2019) derinlemesine savunma yaklaşımlarının ortak bileşenlerini aşağıdaki şekilde açıklamaktadır:

• **Ağ güvenliği:** İlk savunma hattı ağlar üzerinde kurulur. Kullanıcıların İnternet üzerinde zararlı sitelere erişmesini ve dış dünyadan içeri yönde gelebilecek zararlı ağ trafiğini engellemek için bir güvenlik duvarı kullanılabilir. Bunun yanında, saldırı tespit sistemleri kullanılarak trafik üzerindeki şüpheli hareketler tespit edilebilir.

• **Antivirüs sistemi:** Zararlı yazılımların bilgi sistemlerine bulaşmasını önlemek için antivirüs programları kullanılabilir. Bu sistemler, sahip olduğu yerleşik güvenlik duvarı özellikleriyle üzerinde çalıştığı ana bilgisayarın korunmasına yönelik ek koruma görevleri gerçekleştirebilir.

• **Şifreleme:** Hassas veriler şifrelenerek, sadece yetkisi olan kişilerin görmesini sağlayacak şekilde bir savunma katmanı oluşturulur. Bu sayede, mesela veriler çalındığında da gizlilikleri şirket açısından korunmuş olacaktır.

• **Erişim kontrolü:** Bir sisteme erişim için fiziksel ve mantıksal erişim kontrolleri uygulanması da bir savunma katmanı oluşturur. Bilgi sistemleri fiziksel olarak güvenli alanlarda muhafaza edilebilir ve kimlik doğrulama ve yetkilendirme süreçleri uygulanarak erişimleri kısıtlanabilir.



Şekil 34: Derinliğine savunma

Kim & Solomon (2021) saldırılara karşı derinliğe savunmanın özelliklerini *Şekil 34*'te görüldüğü gibi açıklamakta olup uygulama, işletim sistemi ve ağ altyapısı şeklinde üç koruma katmanında incelemektedir:

- **Uygulama savunmaları:** Yazılım uygulamaları üzerinden son kullanıcılar tarafından paylaşılan verilere erişim sağlanır. Saldırganların hedefi hassas verilere ulaşmak için uygulama yazılımları olmaktadır. Bilgisayarlar üzerinde çalışan bütün uygulama yazılımlarının korunmasına yönelik bazı kontroller şu şekildedir:
  - Bilgisayar üzerinde antivirüs taramaları
  - Güncel virüs tanımları
  - Taşınabilir ortamların taranması
  - Ana bilgisayar özelinde güvenlik duvarı ve saldırı tespit sistemleri
  - Değişiklik algılama yazılımları ve bütünlük kontrol yazılımları
  - E-posta eklerinin taranması
  - Yazılım yüklemeleri ve güncellemeleri ile ilgili politika
- **İşletim sistemi savunmaları:** İşletim sistemi saldırıları başarılı olduğu takdirde hassas verilerin bulunduğu sistem kaynaklarına erişim mümkün olabilir. İşletim sistemlerinin korumak için aşağıdaki kontroller uygulanmalıdır:
  - İşletim sistemlerinin güncellenmesi
  - Güvenlik açığı oluşturabilecek hizmetlerin devre dışı bırakılması
  - Değişiklik algılama ve bütünlük kontrol yazılımları
- **Ağ altyapısı savunmaları:** Ağ ortamı, saldırganlar için hedeflerine ulaşmasını kolaylaştırır. Zararlı yazılımlar yayılmak için ağ ortamlarını kullanır. Ağların güvenliğini sağlamak için kullanılabilecek kontrollere aşağıda yer verilmektedir:
  - Ağda dar geçit, tıkanma noktası oluşturma
  - Kritik hizmetleri korumak için vekil hizmetler kullanma
  - Tıkanma noktaları üzerinde içerik filtrelemesi yapma

- Saldırı tespit sistemleri güncel veritabanı
- Ağ cihazlarının güncellenmesi
- İhtiyaç olmayan ağ hizmetlerin devre dışı bırakılması
- Gelen/giden ağ trafiği üzerinde filtreleme
- Ağa uzak bağlantıları korumak için erişim kontrol önlemleri uygulanması

4.11.2. Genişliğine Savunma

Geleneksel güvenlik yaklaşımlarını, yeni güvenlik mekanizmalarıyla birleştiren, OSI modelinin her katmanında güvenliği amaçlayan savunma stratejisidir. Saldırganlar, geleneksel güvenlik kontrollerini aşabildikleri takdirde, yine de OSI modelinde daha yüksekteki katmanda engellenebilir durumdadır. OSI modelinde güvenliğin sağlandığı son katman uygulama katmanıdır. Bu katmanda, web uygulama güvenlik duvarları (WAF) kullanılarak uygulamalarda bir açıklık olsa da bu açıklıklara yönelik kurallar uygulanarak saldırıları önlemek mümkündür.

Genel olarak derinliğine savunma ağ seviyesinde güvenliğe odaklanılırken, genişliğine savunmada uygulama seviyesinde güvenlik sağlanmaya çalışıldığı söylenebilir. Web uygulama güvenlik duvarlarının yanında, güvenlik bilincine sahip uygulama geliştiriciler OWASP (Open Web Application Security Project) yöntemleri kullanarak yazılımlarını geliştiriyor. Diğer savunma sistemlerine güvenmeden, güvenli bir şekilde geliştirilen uygulamalar saldırılara karşı durabilecek yeteneğe sahip olacaklardır.

Saldırıları otomatik olarak tespit etme ve kendilerini saldırılara karşı otomatik olarak savunma yeteneklerine sahip şekilde geliştirilen sistemler için kullanılan güvenlik otomasyonu, bu yaklaşımda karşımıza çıkan bir diğer kavramdır. Bu yetenekler, makina öğrenme ile sağlanır ve birçok güvenlik uygulamasında verimliliklerinin artırılması için kullanılmaktadır. İnsan girdisine ihtiyaç duymadan çalışma yetenekleri güvenlik duvarları ve antivirüs programlarına eklenmektedir.

4.11.3. Ağ Güvenlik Riskleri

Bilgi güvenliği unsurları gizlilik, bütünlük ve erişilebilirlik açısından ağ üzerinden taşınan bilgiyi etkileyebilecek risklerin 3 ana kategorisi keşif (reconnaissance), dinleme (eavesdropping), hizmet engelleme (DoS) şeklindedir (Kim & Solomon, 2021).

- **Keşif:** Tehdit aktörleri tarafından, saldırı öncesi ağ ortamıyla ilgili ağda kullanılan IP adresleri, güvenlik duvarları ve diğer güvenlik sistemleri, işletim sistemleri, bilgi sistemlerdeki mevcut zayıflıklar, uzaktan erişim yöntemleri gibi saldırı süreci için gerekli bilgiler toplanmaktadır. Bilgi toplanmasını önlemek için, bilgi sistemleri en az bilgi sağlayacak şekilde ağ ortamında konumlandırılmalı ve yapılandırılmalıdır.

- **Dinleme:** Ağ ortamında açık bir şekilde gönderilen bilgi dinlemeye açıktır. Saldırganlar, ağa fiziksel erişimle birlikte dinleme yapabileceği gibi, ağ ortamındaki bilgisayarlar ele geçirilip trafiğin arasına girilerek de dinleme yapılması mümkündür. Bu risklere karşı uygulanabilecek en temel eylemler şu şekildedir; kablolamaya fiziksel erişimlerin sınırlandırılması, ağ altyapısında kenar anahtarların kullanılması, kablolu/kablosuz ağ ortamlarında transfer edilen bilginin şifrelenmesi.

- **Hizmet Engelleme:** Saldırganlar ağa sızmak yerine ağ üzerinden verilen hizmetlerin kullanılmasını engelleyerek şirketi tamamen çalışmaz hale getirebilir. Ağ üzerinden verilen hizmetleri çok fazla istekle boğarak tamamen durdurmak için iki temel nokta hedeflenir: Ağ trafiğinin kapasitesi, güvenlik sistemlerinin kapasitesi. Hizmet engellemeye karşı ağı koruyabilmek için ağ bant genişliğinin yeterli olması sağlanmalı, saldırıları tespit edip engelleyebilecek kapasitede ve özellikte güvenlik sistemleri kullanılmalıdır.

4.11.4. Temel Ağ Güvenliği Kontrolleri

Ağdaki bilgi sistemleriyle birlikte ağ ortamında transfer edilen bilginin güvenliğinin sağlanması için aşağıdaki güvenlik önlemleri alınabilir: (Gregory, 2019)

Tedbir	Açıklama
Segmentasyon	Kurumsal ağın güvenlik duvarları ve sanal ağlarla farklı güvenlik bölgelerine ayrılması.
Mikrosegmentasyon	Ağ ortamındaki güvenlik duvarları veya ana bilgisayarlar üzerindeki güvenlik duvarlarıyla ana bilgisayar (sunucu veya son kullanıcı cihazları) seviyesinde bölümleme.
Kullanıcı kimlik doğrulama	Kullanıcıların ağ ortamına erişmeden önce kimlik doğrulamasının yapılması.
Makine doğrulama	Ağa bağlanan her bir cihazın ağa doğrulanarak giriş sağlaması.
Kötü amaçlı yazılımlardan korunma	İş istasyonları üzerinde veya ağ üzerinde kötü amaçlı yazılımların engellenmesi için yazılımların kullanılması. Kötü amaçlı yazılımlara karşı uç noktalarda önlem almakla birlikte; ağ tabanlı yazılımlar, e-posta ve web trafiğinde istenmeyen trafiği engellemek için kullanılır.
Şifreleme	Ağ ortamında transfer edilen hassas verilerin dinlemeye karşı şifrelenmesi.
Kenar anahtarlı ağlar	Yerel alan ağında dinlemeye karşı kenar anahtarların kullanılması.
Saldırı tespit ve engelleme	Ağdaki anormal aktiviteleri, saldırı girişimlerini tespit etmek ve engellemek için ağ tabanlı veya ana bilgisayarda çalışan saldırı tespit ve engelleme yazılımlarının kullanılması.
Balküpü (Honeypot)	Bilgi sistemlerinin yetkisiz kullanımını tespit etmek için tuzak sistemlerin kullanılması.
Web içeriği filtreleme	Kötü amaçlı yazılım barındırdığı bilinen İnternet siteleri gibi farklı kategorilerde sitelere erişimi filtreleyen web içeriği filtreleme yazılımlarının kullanımı.
Veri sızıntısı önleme	Hassas bilgilerin şirket ağ ortamında veya şirket dışına iletilmesini tespit etmek ve engellemek için veri sızıntısı önleme sistemlerinin kullanılması.
Kara liste veya beyaz liste kullanımı	Uygulamalar, IP adresleri ve TCP/UDP portları için kara liste/beyaz liste yapısıyla erişim kontrolü uygulanması.

Tablo 2: Ağ güvenliği tedbirleri

4.11.5. Ağ Güvenlik Risk Bölgeleri

Ağ güvenlik bölgeleriyle bilgi sistemleri hizmetlerinin sunumu, ara bağlantı ve birlikte çalışabilirlik için ortak bir ağ altyapısı sağlanarak şirketlerin güvenlik çözümlerini destekleyecek şekilde dengeli ve katmanlı bir güvenlik mimarisinin temeli oluşturulmaktadır. Ağ güvenliğini uygulamak için, bir şirket ağı ayrı ayrı kontrol edilebilen, izlenen ve korunabilen aşağıdaki ayrı bölgelere ayrılabilir: (Canadian Centre for Cyber Security, 2021)

- **Kamusal bölge (Public zone):** İnternet gibi tamamen herkese açık ağları içermektedir. Şirket tarafından herhangi bir kontrolün olmadığı için son derece düşmanca bir ortam olarak varsayılmaktadır. Tehdit düzeyi yüksek olan bu ortam içinde olan veya bu ortama temas eden bütün bilgi sistemleri saldırılara karşı güçlendirilmelidir.

- **Kamusal erişim bölgesi (Public access zone):** Kamusal bölge tehditlerinden şirketin iç ağının ve uygulamaların korunması, dahili kaynakların dış ortamdan gizlenmesi ve açığa çıkmasının sınırlanması amacıyla kamusal bölge ile çalışma bölgesi arasındaki erişim bu bölge üzerinden sağlanır. Şirket çalışanlarının İnternet erişimine izin veren proxy sunucular, harici e-posta, uzaktan erişim ve dış ağ geçitleri ve çevrimiçi bütün hizmetler bu bölge üzerinde bulundurulmalıdır. Kamusal erişim bölgesi üzerinden bağlanılan dış ağlar ile kısıtlı dış ağ bölgesi üzerinden bağlanılanlar arasında duyulan güven açısından farklılık bulunmaktadır. Kısıtlı dış ağ iş ortakları güvenilirliği sebebiyle doğrudan şirket içi ağına bağlanabilir.

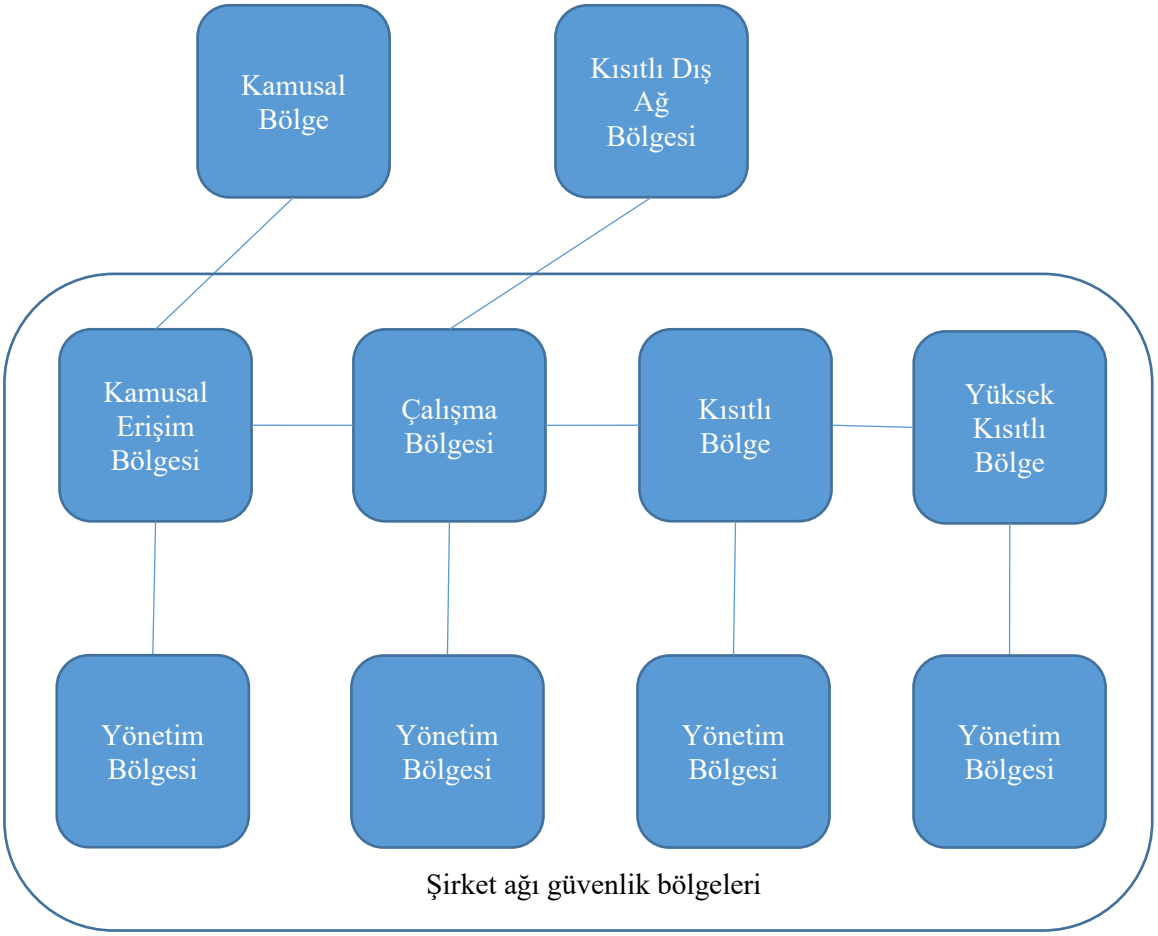
- **Çalışma bölgesi (Operations zone):** Şirketin son kullanıcı sistemlerinin; uygulama, dosya, yazdırma sunucularının bulunduğu rutin operasyonların yürütüldüğü ortamdır. Uygun güvenlik kontrolleriyle bu ortamda hassas bilgilerin işlenmesi sağlanabilir fakat genel olarak büyük hassas veri depoları ve kritik uygulamalar için uygun değildir. Bu bölgede trafik; şirket içi bölgelerden dahili olarak veya kamusal erişim ve kısıtlı dış ağ bölgeleri üzerinden uzaktan erişim, mobil erişim ve dış ağlardan kaynaklanabilir ve erişim genellikle sınırsızdır. Bu bölgede kötü niyetli trafik içerdeki düşmanlardan (insiders), kamusal bölge üzerinden gelen zararlı yazılımlardan, ağda ele geçirilmiş iş istasyonlarından veya iş istasyonlarına yetkisiz kablosuz bağlantılarından kaynaklanabilir.

- **Kısıtlı bölge:** Orta düzeyde bütünlük ve erişilebilirlik gereksinimli, güvenliği ihlal edildiğinde işin kesintiye uğramasına neden olabilecek bir şirket için kritik bilgi sistemleri hizmetlerine ve hassas bilgi depolarına uygun kontrollü bir ağ ortamı sağlanır. Kısıtlı bölgeye kurumsal bölgeden erişimler, çalışma bölgesi ve kamusal erişim bölgesi aracılığıyla gerçekleşir. Kısıtlı bölgedeki ağ seviyesindeki varlıkların kimlik doğrulaması yapılır. İçerdeki düşmanlardan gelen tehditleri azaltmak için kısıtlı bölgeye erişim sınırlanır. Kısıtlı bölge içerisinde yetkisiz kişilerin dinleme yapmasını önlemek için veri gizliliği hizmetleri uygulanır ve gelebilecek tehlikelere karşı yönetimsel olarak izleme mekanizmaları kurulur.

- **Yüksek kısıtlı bölge:** Yüksek seviyede bütünlük ve erişilebilirlik gereksinimli, güvenlik ihlallerinin insan sağlığını ve emniyetini tehlikeye atabilecek seviyede risk barındırdığı kritik uygulamalar ve yoğun hassas bilgi depoları için sıkı şekilde kontrol edilen bir ağ ortamı sağlanır. Bu bölgeye kamusal bölge üzerinden erişim sağlanamaz sadece başka kuruluşların kontrollü bölgeleri üzerinden erişim sağlanabilir. Yüksek kısıtlı bölgedeki ağ seviyesindeki varlıkların da kimlik doğrulaması yapılır. İçerdeki düşmanlardan gelebilecek tehditlere karşı kısıtlı bölgeden daha sıkı kontroller uygulanır. Hassas bilgilerin gizliliğinin sağlanmasına yönelik fiziksel ve ağ katmanında gerekli güvenlik kontrolleri sağlanır.

- **Kısıtlı dış ağ bölgesi:** Güvenilirlik seviyesi yüksek iş ortaklarıyla doğrudan bağlantılı dış ağ hizmetlerini destekleyen ortamdır. Kısıtlı dış ağ bölgesi kamusal erişim bölgesiyle bağlanması gerekmez. Bu bölge için gereksinimler ve uygulamalar duruma göre belirlenmeli ve iş ortaklarıyla yapılan anlaşmalar çerçevesinde uygulanmalıdır.

- **Yönetim bölgesi:** Kısıtlı bölgeye benzer şekilde sağlamlığa sahip; ağ ve sistem yöneticilerinin bilgi sistemleri ve ağ yapısını yapılandırma ve izleme işlemlerini, müdahale veya güvenlik riski azaltılarak, gerçekleştirebilecekleri ayrı ve yalıtılmış bir yönetim ağ ortamı sağlanır. Uzaktan yönetim için kullanılacak iş istasyonlarının kimlik doğrulaması yapılmalıdır.



Şekil 35: Ağ güvenlik bölgeleri

Ağ güvenlik bölgeleri güvenlik politikası kapsamında tanımlanmalıdır. Her bir bölge için trafik yönetimi, güvenlik duvarlarının kullanımı, VPN bağlantısı, sistemlerin sağlamlaştırılması, kötü niyetli kod taraması vb. güvenlik gereksinimleri iyi belirlenmelidir (Stewart & Kinsey, 2021). Bir bölgede risk ne kadar büyükse, o bölgede daha fazla güvenlik tedbiri alınması gerekir veya tam tersi de geçerlidir. Bölgeler güven hususunda birbirine karıştırıldığında, ağ güvenliğinin sağlanması karmaşık hale gelmektedir. Bölgelerin birbiri ile bağlantısında bir şüphe olduğunda bağlantının geldiği bölge düşük güvenlikte (yüksek riskte) olduğu varsayılarak bağlanılan bölge için gerekli güvenlik tedbirleri uygulanmalıdır. Ağ güvenliği en zayıf halkası kadar güçlüdür ve ağa bağlanan bütün iş istasyonlarının güvenli bir işletim sistemi kullanması gerekmektedir. Genel olarak işletim sistemleri güvenlik sıkılaştırmaları yapılmadan kullanılmaktadır ve daha fazla riske sahip olan bu ağ bölgelerinde işletim ortamlarının güçlendirilmesi gerekir.

Genel olarak ağların; verilerin ele geçirilmesi, iletişimin sağlanabiliyor olması ve giriş noktaları aracılığıyla yetkisiz erişim hususlarında zafiyetlere sahip olduğu söylenebilir. Bilgi sistemleri denetiminde ağın fiziksel güvenliğiyle birlikte ağ trafiğinin şifrelenmesi ile ilgili kontrollere bakılmalıdır. İletişimin erişilebilirliği açısından ilk kontrol etkili bir ağ mimarisi ile ağ yönetim yazılımıyla uygun izleme olmalıdır. Ağ yönetim yazılımıyla bant genişliğinin kullanımı izlenerek ağ üzerindeki dar boğazların önüne geçilebilir. Ağ erişimi, yönlendiriciler üzerinde erişim kontrol listeleri ve uygun güvenlik duvarı çözümlerinin kullanılmasıyla yalnızca izin verilen trafiği sağlayacak şekilde kısıtlanmalıdır (Cascarino, 2012).

4.11.6. Güvenlik Duvarları

Ağ güvenliği risk bölgeleri açık ve net şekilde birbirinden izole edilmelidir ve bölgeleri ayırmak için kullanılan birincil araç güvenlik duvarları olmaktadır. Güvenlik duvarları sağladığı erişim ve güvenlik kontrolleriyle bir ağ ortamının dışarıdan gelen saldırılara karşı ilk savunma hattıdır. Güvenlik duvarlarının şirket içinde konumlandırılmasında ve kullanılmasında aşağıdaki güvenlik stratejilerinden faydalanılmaktadır (Stewart & Kinsey, 2021).

- **Belirsizlik yoluyla güvenlik:** Güvenlik önlemi olarak temel yapılandırma ayarlarının değiştirilmesi ve normal dışı konfigürasyonlar yapılmasıdır. Belirli bir portta çalışan hizmeti farklı bir portta çalıştırarak; bilgi sistemlerine ilişkin isim, ağ adresi, ağ boyutu, alt ağlar veya belirli başlıklar değiştirilerek temel saldırılara karşı bir miktar korunma sağlasa da gerçek anlamda bir güvenlik sağlamaz. Bu değişikliklerin birçoğu ağ tarama teknikleri ile aşılabilir ve atlanabilir. Belirsizlik yoluyla gerçek güvenlik, belirsiz ve standart olmayan teknolojilerin kullanılmasına dayanır. En yaygın ve en popüler işletim sistemi veya yazılımın güvensiz olduğu biliniyorsa, farklı bir ürün kullanmakla bilinen bir istismara karşı bir güvenlik iyileştirmesi yapılabilir. Sonuç olarak belirsizlik yoluyla güvenlik, saldırganlar tarafından kullanılan teknolojinin bilinememesiyle sağlanabilir. Bilgi sistemleri ile ilgili bilgileri gizlemek, saldırganların daha az şey öğrenmesine neden olur. Bu sayede saldırıların başarılı olma ihtimali azaltılmış olur.

- **En az ayrıcalık:** Kullanıcılara görevlerini gerçekleştirirken en düşük erişim düzeyinde izin verilmesine dayanan ağ güvenliğinin temel kavramlarından birisidir. Kullanıcıların her sisteme, kaynağa, dosyaya, hizmete, İnternet üzerinde bütün noktalara erişim ihtiyacı yoktur. Gereğinden fazla yetenek, erişim ve ayrıcalığa sahip olmak, bilgi sistemlerinin ele geçirilmesi ve güvenliğin bozulması riskini artırır.

Erişim denetim kapsamında şirketler varsayılan reddet veya tümüne izin ver erişim denetim politikalarına sahip olabilir. Varsayılan reddet politikasında, tüm kaynaklara erişim engellenir ve en az ayrıcalık ilkesiyle, hem kullanıcıların iş tanımlarına hem de sistemlerin ihtiyacına göre gerektiğinde izin verilen istisnalar kapsamında erişim sağlanır. Tümüne izin ver politikası kapsamında önceden belirlenmiş kısıtlı erişim dışında bütün erişime izin verilir. İnternet gibi harici bir kaynağa erişmek için güvenilir bir kaynaktan geldiği durumlarda kullanılır, isteğe bağlı erişim kontrolü olarak da bilinir. Varsayılan reddet politikası ise güvenilir olmayan bir kaynaktan güvenli bir ortama erişim sağlandığı durumlarda daha yaygındır. Daha katı ve sağlam olduğu için varsayılan reddet politikasının uygulanması önerilir (Doshi, 2020).

En az ayrıcalığın sağlanmasında her kullanıcının ayrı ayrı kontrol edilmesi kullanıcı yönetiminde yük oluşturur. Bu yüzden en az ayrıcalık şirketlerde genellikle kısmen uygulanır. Yaygın bir uygulama kullanıcıları benzer güvenlik düzeylerinde gruplayıp, bir bütün olarak gruplara izinler verilmesidir. Kullanıcılara gereğinden fazla ayrıcalık sağlanarak güvenlik riskinde bir artış olmakla birlikte, yönetimsel anlamda kolaylıklar getirmektedir.

Özellikle yönetici kullanıcıları için en az ayrıcalık ilkesinin bir uzantısı olarak görevler ayrılığı uygulanır. Görevler ayrılığı kapsamında yöneticilere sınırlı bir sorumluluk alanında yetki verilmesi sonucu bilgi sistemlerinin tümü genelinde yöneticiler ortadan kaldırılmış olmaktadır. Bu şekilde de güvenlik riskleri azaltılabilir.

- **Basitlik:** Güvenliğin önemli bir parçası olarak işlerin basit tutulması sistemlerin anlaşılmasını, yönetilmesini ve sorun gidermeyi kolaylaştırır. Bir çözüm ne kadar karmaşıksa; hataların, kusurların artması ve gözden kaçması o kadar muhtemeldir. Karmaşık bir sistemin güvenliği sağladığının doğrulanması da o kadar zordur. Ağ altyapılarında basitlik her zaman mümkün olmasa da, güvenlikten ödün vermeden basit çözümlerin uygulanması tercih sebebi olmalıdır.

- **Derinlemesine Savunma:** Güvenlik duvarları, güvenlik altyapısının bir parçasıdır, tek başına tam bir güvenlik sağlayamaz. Bir şirketin uygun bir güvenlik altyapısı birbirine kenetlenmiş ve katmanlar halinde konumlandırılmış bileşenlerden oluşmalıdır. Güvenlik bileşenlerinden herhangi birisinin atlatılması durumunda bir alternatif ve tamamlayıcı bileşen devrede olmalıdır. Bu derinlemesine savunma olarak bilinir. Örneğin, şifreleme, antivirüs yazılımları, güvenlik duvarı, saldırı tespit sistemleri, fiziksel erişim kimlik doğrulaması. Derinlemesine savunmanın bir diğer yönü de, özel

kaynakları, halka açık ortamlardan ayırmak için birden çok alt ağın seri olarak konuşlandırılmasıdır. N-katmanlı mimari olarak bilinen bu yapı; sunum, uygulama ve veri katmanlarından oluşan geleneksel istemci-sunucu uygulamaları için kullanılan başlıca yazılım uygulaması mimarisidir. Derinlemesine savunmanın uygun bir şekilde uygulanmasıyla, sadece dış dünyadan gelecek saldırılar için değil şirket içinden güvenliği tehlikeye atmaya yönelik girişimler için de korunma seviyesi artmış olacaktır.

- **Savunma Çeşitliliği:** Derinlemesine savunmayla benzer şekilde birden çok güvenlik katmanı desteklenir fakat savunma çeşitliliği çoğu katmanda farklı güvenlik mekanizmaları kullanılarak sağlanır. Yani, birden çok güvenlik duvarının kullanılması derinlemesine savunma sağlar fakat savunma çeşitliliği olmaz. Bu durumda monolitik bir derinleme savunması yerine, saldırı tespit sistemi, antivirüs, güçlü kimlik doğrulama, sanal özel ağ, ayrıntılı erişim kontrolü vb. araçlar eklenerek katmanlı ve çeşitli bir savunma gerçekleştirilebilir.

Savunma çeşitliliği uygulanırken; tüm güvenlik tasarımları ve algıları test ve incelemelerin sonuçlarına dayandırılarak gerçekten çeşitliliği arttıran güvenlik kullanıldığından emin olunmalıdır. Bunun için; güvenlik ürünleri farklı isme ve markaya sahip olsa da arka planda aynı ürünlerin olması, farklı güvenlik uzmanlarıyla tüm yapılandırmaların kontrol edilmesi, pek çok ürünün aynı ortak açık kaynaklı kodları kullanması, aynı türden birçok sistemin temel teknoloji, tasarım ve güvenlik açısından aynı zayıflıklara sahip olması gibi hususlar göz önünde bulundurulmalıdır.

Savunma çeşitliliği; teknoloji çeşitliliğiyle birlikte satıcı ve kontrol türünün çeşitliliği göz önünde bulundurularak oluşturulabilir. Örneğin, satıcı çeşitliliği için; farklı üreticilerin güvenlik duvarları veya antivirüs programları kullanılabilir ve bir üreticiden kaynaklanabilecek riskler azaltılabilir. Ancak, birden çok satıcının ürünlerinin kullanılmasıyla ağ yönetiminin karmaşıklığı artacak, yönetim zorluğu oluşturacaktır. Bununla birlikte, genel altyapı tasarımları ve yedeklilik hususları da göz önünde bulundurulmalıdır. Güvenlik duvarlarını seri bağlamak birindeki zafiyet durumunda diğerinin devreye girmesi anlamına gelecekken, güvenlik duvarları paralel bağlıyken iki güvenlik duvarında da bulunan farklı zafiyetler nedeniyle şirketin saldırı yüzeyi artmış olacaktır. Kontrol türünün çeşitliliği kapsamında, önleyici, tespit edici ve düzeltici kontrolleri şeklinde işlevlerin farklılıkları değerlendirilmelidir.

- **Dar geçit:** Kontrol noktası, filtre yolu veya dar boğaz olarak adlandırılabilir. Herhangi bir kontrolsüz trafik, kullanıcı veya veri geçişi olmayacak şekilde bütün trafiğin, iletişimin veya eylemlerin tek bir yol veya kanal üzerinden geçmesi zorlanarak içeriği filtrelemek, kimlik doğrulama ve yetkilendirmeyi zorlamak, bant genişliğini kontrol etmek vb. güvenlik kontrollerinin gerçekleştirilmesi amaçlanmaktadır. Bir bilgi sistemleri altyapısının sınırları boyunca ve ağ güvenlik risk bölgeleri arasında geçiş noktaları kullanılarak ağ trafiğinin kötü niyetli girişimlere karşı filtrelenmesi sağlanabilir. Bir darboğaz atlatılamıyorsa, o filtre yolu üzerindeki güvenlik kontrolleri geçerli olacaktır. Bir saldırgan, tesis edilen dar geçitlerin yerine alternatif yollardan hedefe ulaşabiliyorsa dar geçitin bir önemi yoktur. Bu yüzden alternatif yollar göz önünde bulundurulmalıdır. Örneğin: bir geçit noktası bir ağ trafiğini ağ erişim kontrolü, antivirüs, saldırı tespit sistemi, güvenlik duvarı gibi güvenlik cihazlarıyla izlenip filtrelenecek bir yol boyunca zorlayabilir. Fakat saldırgan hedef sisteme fiziksel olarak veya başka bir ağ ortamından erişebiliyorsa bu mekanizmalar devre dışı kalacaktır.

- **En zayıf halka:** Bir güvenlik altyapısında en zayıf halkanın bulunup onunla ilgili güvenlik önlemleri alınması önemlidir çünkü saldırganlar da güvenlik açıklıkları ararken en zayıf halkayı keşfedip kullanmak ve istismar etmek isterler. En yaygın saldırıları ve izinsiz girişimleri engelleyebilecek bir güvenlik yapısına ulaşmak için saldırganlara benzer bir yaklaşımla sürekli olarak bir altyapıdaki en zayıf ögeyi bulup güvence altına almayı içerecek şekilde devam eden bir süreç uygulanmalıdır. En zayıf halkalar kaçınılmaz olsa da böyle bir en zayıf halka güvenlik duruşu güvenlikli bir altyapı oluşturmaya yardımcı olacaktır.

- **Bozulmaya dayanıklı: "**Bir bilgisayar sistemine saldırmak veya bunu atlamak için yapılan aktif girişimlere sistemin direnmesine izin veren tasarım özelliklerini açıklar (ISACA, 2018)." Bozulmaya dayanıklılıkla ilgili fail-safe (fail-open), fail-secure (fail-closed) kavramları sadece güvenlik duvarlarının ve diğer güvenlik kontrollerinin tasarım ögeleri değildir, aynı zamanda bir şirketin güvenliğini sağlamak için kapsamlı bir güvenlik duruşudur. Bir başka deyişle; yalnızca bozulmaya dayanıklı güvenlik ürünleri kullanmak değil, bütün altyapıyı güvenlik açısından bozulmaya dayanıklı

tasarlamakla ilgilidir. Güvenliğin herhangi bir yönü göçüp çalışamadığı durumda, temel güvenlik korumaları desteklenmeye ve sürdürülmeye devam edilmelidir. Bu durumda genellikle gizlilik ve bütünlük korumaları sürdürülmeye çalışırken erişilebilirlik koruması feda edilmektedir. Şirketin politika ve hedeflerine göre, erişilebilirlik öncelik hedeflerdense diğer güvenlik kontrollerini desteklemek için erişilebilirlikten de kolaylıkla vazgeçilemeyecektir.

- **Zorunlu ortak katılım:** Bir şirketin güvenliğinin sağlanması, şirket güvenlik politikası kapsamında herkesin kurallara uymasına bağlıdır. Herkesin kurallara uyması için çalışanların güvenlik çabalarının kendi çıkarları için olduğuna inanması gerekir. Bazı çalışanların diğerlerinden farklı kurallara tabi olduğu bir ortamda çalışanlar arasında hoşnutsuzlar olur ve çalışanların güvenlik çabalarını desteklemesini, gönüllü katılımını zorlaştırır. Bunun için güvenlik politikalarında tutarlı uygulama önemlidir. Sonuç olarak güvenlikle ilgili kontrollerde istisnalar olacaktır fakat istisnalar kural olarak benimsenmeye başladıysa sadece bir güvenlik varsayımımız olur, gerçek bir güvenliğin varlığından bahsedilemez.

Güvenlik Duvarı Yönetimi En İyi Uygulamaları

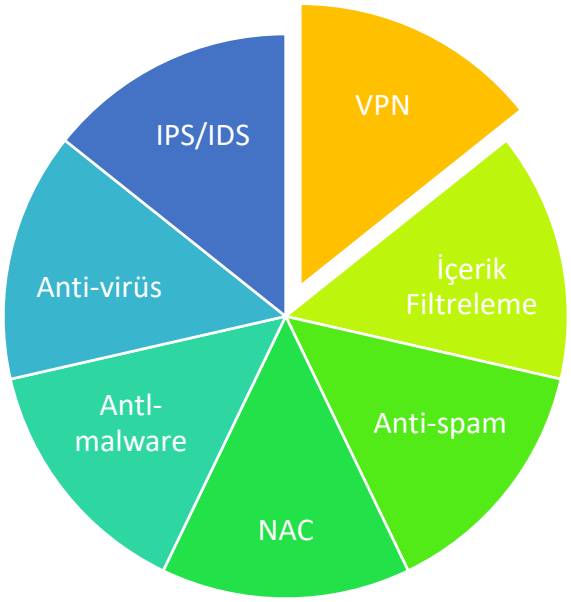
Güvenlik duvarı güvenliğinde güvenilirliği sağlamak için bazılarının genel olarak ağ güvenliği için de geçerli olduğu önerileri, ilkeleri ve standart işletim prosedürleri içeren en iyi uygulamalar aşağıda yer almaktadır: (Stewart & Kinsey, 2021)

- Yazılı bir güvenlik duvarı politikasına sahip olun.
- Güvenlik duvarı uygulanmasına yönelik bir plana sahip olun.
- Bilgi sistemleri ve ağ altyapısını anlayın.
- Güvenlik duvarlarının gerekli olduğu alanlara karar verin.
- Ortam ve iletişim tehditlerini belirleyebilmek için bir risk değerlendirmesi yapın.
- Politikayı düzenli olarak gözden geçirin.
- Her hizmet, işlem ve iletişimin filtrelenerek geçtiği istisnasız bir politika oluşturun.
- Tümünü izin ver yerine varsayılan reddet politikası tercihinde bulun.
- Fiziksel erişimi koruyun.
- İnternet erişimlerini kısıtlayın ve filtreleyin.
- Tek bir güvenlik duvarına güvenmeyin, derinlemesine savunma uygulayın.
- IPsec, VPN vd. şifreli trafiği kontrol ederek uygun olan yerlerde izin verin.
- Güvenlik duvarı tasarım ve yapılandırmalarını basit tutun.
- Güvenlik duvarı erişim kurallarını düzenli olarak gözden geçirmeye öncelik verin.
- Hem ağ üzerindeki hem de ana bilgisayarlar üzerindeki güvenlik duvarlarını sıkılaştırın.
- Güvenlik duvarı güncellemelerini takip edin, uygulamadan önce test edin.
- Her zaman farklı bir ortama güvenlik duvarı yapılandırma yedeklerini alın.
- Güvenlik ihlallerine karşı güvenlik duvarını sürekli izleyin.
- Karşılaşılabilecek tehditlere karşı bir olay müdahale planı oluşturun.
- Güvenlikle kullanılabilirlik arasında kullanıcılara en az güçlük oluşturacak şekilde denge kurmaya çalışın.
- Günlük, haftalık kontrollerin yer aldığı bir güvenlik duvarı kontrol listesi geliştirin.
- Düzenli olarak zafiyet taraması ve sızma testi gerçekleştirin.

Güvenlik Duvarına Ek Güvenlik Önlemleri

Güvenlik duvarları güvenlik altyapılarının en önemli parçasıdır. Ana bilgisayarlar üzerinde güvenlik duvarı ihtiyacı vardır, bir ağ ortamında çevresel güvenlik için sınır güvenlik duvarlarına ihtiyaç vardır. Bunun yanında, en uygun şekilde tasarlanmış bir güvenlik altyapısı için tek başlarına güvenlik duvarları sağladığı güvenlik kontrolleriyle eksik bir güvenlik çözümü olarak kalacaklardır. Şirketlerin ağ ortamlarındaki belirli riskleri ele almak için güvenlik duvarlarıyla birlikte *Şekil 36:* 'da görüldüğü üzere daha farklı unsurları içeren güvenlik sistemlerine ihtiyaç bulunmaktadır: (Stewart & Kinsey, 2021)

- Anti-virüs yazılımı
- Anti-malware yazılımı
- Anti-spam yazılımı
- Web içerik filtreleme
- Veri sızıntısı önleme (DLP)
- Saldırı tespit ve önleme sistemleri (IDS/IPS)
- Ağ erişim kontrolü (NAC)
- Uzaktan erişim (VPN)



Şekil 36: Ağ güvenlik sistemi bileşenleri

Bu bağlamda, farklı amaçlarla kullanılmakta olan bazı özel güvenlik duvarı türlerine ve özelliklerine aşağıda yer verilmektedir: (Stewart & Kinsey, 2021)

- **Hibrit:** Tek bir güvenlik sistemi üzerinde bütünleşik bir şekilde VPN erişimi, güvenlik açıklığı yönetimi, IDS/IPS, antivirüs, antimalware, antispam, DLP, içerik filtreleme vb. ağ güvenliğiyle ilgili özellikler sağlanmaktadır. Bu şekilde, gelişen farklı tehditlere karşı tek bir sistem üzerinden bir şirketin güvenlik ihtiyaçları karşılanabilmektedir. Tek bir güvenlik sistemi üzerinde çok fazla işlevin gerçekleştirilmesiyle performans açısından risklerin artacağı göz önünde bulundurulmalıdır.

- **Web uygulama:** Web uygulamalarına giriş, çıkış ve erişimi kontrol etmek için tasarlanmış web uygulama güvenlik duvarları (WAF) bulunmaktadır. Web uygulama güvenlik duvarları, web uygulamalarındaki zafiyetleri hedef alan arabellek taşması, SQL enjeksiyonu saldırısı vb. saldırıları engelleyebilecek yeteneklere sahip olmaktadır.

• **Veritabanı:** Veritabanı özelinde ayrıntılı bir şekilde güvenlik sunan, veritabanına yapılan giriş, çıkış ve sistem çağrılarını kontrol etmek için tasarlanmış veritabanı güvenlik duvarları mevcuttur. Bu sayede veritabanına gelen her bir sorgu üzerinde gerekli kontroller yapılarak özellikle SQL enjeksiyonu gibi saldırıların önüne geçilmektedir.

4.11.7. Saldırı Tespit ve Engelleme Sistemleri

Güvenlik duvarları, ağ ortamına gelen ve giden trafik erişimini kontrol eder. Bununla birlikte, derinlemesine savunma yaklaşımının bir parçası olarak izin verilen ağ trafiği üzerinden ağ güvenliğini ihlal edebilecek girişimleri tespit edebilecek ve engelleyebilecek mekanizmalar oluşturulmalıdır. Güvenlik duvarlarıyla birlikte saldırı tespit ve engelleme sistemleri etkili savunma mekanizmalarıdır. Saldırı tespit ve engelleme sistemleri ağ ortamında konumlandırmayla birlikte bilgisayar tabanlı olarak da düşünülmeli; hem imza hem de anormallik algılama özelliklerini kullanacak şekilde uygulanmalıdır. Anormallik tespiti, servis dışı bırakma veya sürekli oturum açma girişimleri gibi saldırıları tespit etmek için faydalı olabilir. Bunun için sistemin normal veya kabul edilebilir aktiviteyi öğrenmesi ve ön yapılandırması süreci gerekir (Stewart & Kinsey, 2021).

4.11.8. Sanal Özel Ağlar (VPN) ve Uzaktan Erişim

Günümüzde birçok şirket, çalışanlarına ofis ortamında çalışmanın yanında uzaktan çalışma imkanı da sunuyor. Uzaktan çalışma için çalışanların ofis ortamında erişim sağladığı uygulama ve sistemlere uzaktan erişim ihtiyaçları bulunmaktadır. Uzaktan erişim, "harici bir ağ aracılığıyla iletişim kuran bir kullanıcı (veya bir kullanıcı adına hareket eden bir süreç) tarafından bir kurumsal sisteme erişim" şeklinde tanımlanmaktadır (NIST, 2020c). Kullanıcıların iç ağ ortamındaki kurumsal kaynaklara uzaktan erişimiyle ilgili potansiyel tehditlere karşı güvenlik tedbirlerinin alınması gerekmektedir.

Sanal özel ağ (VPN), uzaktan erişim esnasında İnternet gibi halka açık ağlar üzerinden kullanıcılar ile şirket iç ağı arasında iletilen verinin şifreleme kullanılarak gizlilik ve bütünlük açısından güvenlik düzeyini iyileştirmenin bir yoludur. Buna ek olarak, iki taraf arasında erişim sağlamak için noktadan noktaya özel bir bağlantıdan ziyade hali hazırda mevcut olan İnternet gibi ortamlar üzerinden VPN ile erişim uygun maliyetli olmaktadır. VPN erişimi yönlendiriciler, güvenlik duvarları veya ayrı VPN cihazları üzerinde sonlandırılabilmektedir (Kim & Solomon, 2021).

VPN kullanımıyla ilgili bazı riskler aşağıda yer almaktadır: (Stewart & Kinsey, 2021)

- VPN çözümü yanlış yapılandırması
- İşletim sistemi güvenlik açıkları
- İşletim sistemi yanlış yapılandırması
- Virüsler ve kötü amaçlı yazılımlar
- DoS saldırıları
- Eksik yamalar
- Arka kapı saldırıları
- Zayıf istemci güvenliği
- Zayıf kimlik doğrulama
- Kimlik bilgisi paylaşımı

VPN yönetiminin en iyi uygulamaları aşağıda listelenmektedir: (Stewart & Kinsey, 2021)

- Yedekli bir yapı oluşturun.
- Ortamınız için doğru VPN çözümünü belirleyin.
- Aşağıdaki hususları içerecek şekilde bir VPN politikası oluşturun.
  - Uzaktan erişim sağlayacak kişileri, grupları belirleyin.

o Bağlantı türlerini ve şifreleme düzeylerini belirleyin.

o Kimlik doğrulama yöntemlerini belirleyin.

o Son kullanıcı bilgisayarları için antivirüs, güvenlik duvarı, antimalware gibi yapılandırma gereksinimleri belirleyin.

o Bireysel cihazlara izin verilecekse bu bağlantılar için standartları belirleyin.

o Farklı şirketlerle ağlar arası VPN bağlantılar için onay süreci ve kriterleri belirleyin.

- Son kullanıcı bilgisayarı güvenliğini sağlayın.
- Eksik yamalar, yapılandırma sorunları, güvenlik açıklıklarını test eden araçlar kullanın.
- Çok faktörlü kimlik doğrulama kullanın.
- VPN uygulama planınızı yazılı hale getirin.
- VPN hizmetini kesintilere karşı izleyin.
- Düzenli incele, yedekle ve güncelle.

4.11.9. Ağ Erişim Denetimi (NAC)

Uzaktan erişime benzer şekilde, bir şirketin kablolu veya kablosuz ağlarına bağlantıların kontrol altında tutulması gerekir. Bunun için şirket iç ağına ve kablosuz ağ ortamına bağlantı noktalarında kimlik denetimi yapılması, sadece yetkilendirilmiş kullanıcı ve cihazların bağlanması sağlanmalıdır. Ağ erişim denetimi (NAC) sistemleri bir cihazın bir ağa bağlanmadan önce kimlik doğrulaması ve duruş kontrolü görevlerini yerine getirir.

Genel olarak, ağa giriş yapabilmek uç noktadaki cihazlar IEEE 802.1.x standardı kullanarak NAC sistemi ile etkileşimde bulunur. Kimlik doğrulama yanında ağa erişim izni vermek için NAC sistemi istemciler için duruş kontrolü de sağlar. Bu yönde, istemcilerin güncel antivirüs yazılımı kurulu olması, güvenlik duvarının etkin olması, işletim sistemi sürümleri ve güncelliği benzeri yapılandırmaları kontrol ederek bu hususlar karşılandığı durumda ağa erişim izni verilir. İstemciler tarafından güvenlik kontrolleri sağlanmadığı takdirde, cihazlar ağa bağlanmadan engellenebilir ya da bir karantina ağına alınabilir (Kim & Solomon, 2021).

4.11.10. IP Üzerinden Ses (VoIP)

TCP/IP ağlarının ve İnternet'in yaygınlaşmasıyla, geleneksel telefon sistemlerinin yerini IP üzerinden iletişim kurabilen sistemler aldı. Şirketler mevcut ağ altyapısı üzerinden ses ve görüntülü aramalar için IP üzerinden ses (VoIP) sistemlerini kullanarak maliyetleri azaltabilmektedir. IP telefonlar ağ ortamına bağlandığı için diğer ağ trafiğiyle ilgili aynı saldırılara maruz kalabilir. VoIP güvenliğini sağlamak için en iyi uygulamalardan bazıları şunlardır: (Kim & Solomon, 2021)

- IP telefon sistemi yazılımlarını güncel tutun.
- İş istasyonları trafiğiyle IP telefon trafiğini ayrı VLAN'lar kullanarak birbirinden izole edin.
- Ses ve video trafiğini şifreleyin.
- Kullanıcılar için kimlik doğrulaması uygulayın.
- Uzaktan erişimler için VPN kullanın.
- IP telefon sistemini güvenlik duvarı ile koruyun.
- IP telefon sistemi cihazlarını ve yazılımlarını sıkılaştırın.

4.11.11. Kablosuz Ağ Güvenlik Kontrolleri

Şirket çalışanları için kablosuz ağ ortamında kablo bağlantısına ihtiyaç duymadan iletişim esneklik sağlamasıyla birlikte iletişimin kolayca dinlenebilmesi nedeniyle kablosuz ağlar saldırganların ana hedeflerinden birisi olmaktadır. Kablosuz ağlarla ilgili dinlemenin (eavesdropping) yanı sıra zayıf şifreleme (weak encryption), kimlik sahtekarlığı (spoofing), oturum ele geçirme (session hijacking), savaşta sürüş ve savaş tedbirleri (war driving and war chalking) gibi tehditler ve güvenlik açıklıkları risklerini azaltmak için aşağıdaki önlemler alınabilir: (Gregory, 2019)

- Bilinmeyen bir SSID kullanın.
- SSID yayınlamayı kapatın.
- Kapsama alanını sınırlayacak şekilde iletişim gücünü azaltın.
- MAC adresi filtreleme gerçekleştirin.
- WPA2 veya WPA3 şifrelemesi kullanın.
- İç ağ erişimleri için VPN kullanın.
- Kablosuz ağ altyapısı cihazlarında varsayılan kullanıcı adı ve şifreleri kullanmayın.
- Kablosuz ağ altyapısı cihazlarının güncellemesini yapın.
- Halka açık kablosuz erişim noktaları yerine mobil ağlara bağlanan kişisel kablosuz erişim noktası kullanın.

4.11.12. İşletim Sistemi Güvenliği

Sınırsız erişimin olduğu ortamlarda veya varlık değeri yüksek bilgi varlıklarının söz konusu olduğu durumlarda özellikle işletim ortamlarındaki güvensizliklere dikkat edilmelidir. İşletim sistemleri birçok güvenlik yeteneğine sahiptir ve bunların etkili kontroller haline gelmesi için işletim sistemi sıkılaştırma tedbirleri uygulanmalıdır (Cascarino, 2012). Bu kapsamda, aşağıda bazı işletim sistemi sıkılaştırmalarına yer verilmektedir: (DDO, 2020)

- Sadece gerekli olan servisler ve portların açık olması.
- Servislerin ihtiyaçları olan en az yetki ile çalışması.
- Servislerin versiyon vb. bilgilerin ifşasına yol açmayacak şekilde başlık bilgileri dönmesi.
- Güvenlik güncelleme yamalarının yüklenmesi.
- Güvenlik desteği devam eden işletim sistemlerinin kullanılması.
- Şifresiz iletişim kuran uygulama ve servis çalıştırılmaması, şifreli muadillerinin kullanılması.
- Kullanıcı parolaları için güçlü bir parola politikası belirlenmesi, ilk giriş esnasında parolaların değiştirilmesi, parolaların belirli sürelerde yenilenmesi, hatalı giriş denemelerinde hesaplar kilitlenmesi.
- Son kullanıcı bilgisayarlarında uzaktan erişimin kısıtlanması.
- Hata ve sorun bilgilerinin üretici ile otomatik olarak paylaşılmaması.
- Düzenli olarak zafiyet taraması yapılması.
- Kullanılmayan uygulamaların kaldırılması.
- Bilgisayar tabanlı saldırı tespit ve engelleme sistemi kullanılması.
- Virüsten korunma ve kötü amaçlı yazılımlardan korunma için yazılımların kullanılması ve güncel tutulması.
- Yerel güvenlik duvarı ayarlarının yapılması.
- Disk seviyesinde şifreleme yapılması.

- Tüm sistemlerde ortak zaman kullanımı için NTP sunucuları üzerinden zaman senkronizasyonu yapılması.

- Sistem zaman ve tarih ayarları, kullanıcı hesapları, ağ yapılandırması, erişim kontrolleri üzerinde yapılan değişikliklerin, giriş/çıkış bilgilerinin, yetkisiz dosya okuma denemelerinin, dosya silme işlemlerinin, sistem yöneticisi işlemlerinin kayıt altına alınması ve değiştirilemeyecek şekilde saklanması.

4.11.13. Mobil Cihaz Güvenliği

Mobil iletişim teknolojileriyle sağlanan mobilite, şirketler için büyük fırsatlar sunduğu kadar bilgi sistemleri altyapısı risk alanlarından kullanıcı alanındaki değişimlerle birlikte kontrol edilmesi gereken riskler de oluşturmaktadır. Şirketler verimlilik, çalışan memnuniyeti ve maliyet avantajları nedeniyle daha çok *kendi cihazını getir* (BYOD) stratejisini benimsiyor. BYOD; dizüstü bilgisayar, akıllı telefon, tablet gibi çalışanların kendi cihazlarını kişisel işlerinin yanısıra iş için de kullanabilmesiyle ilgili bir kurumsal politika olarak tanımlanmaktadır. Bu kişisel cihazların iş amaçları için kullanımı, bilgi sistemleri güvenliği açısından farklı riskleri, tehditleri ve güvenlik açıklıkları beraberinde getirmektedir.

Bir şirket, kişisel cihaz yönetiminde daha kontrol edici ve aktif rol alabilir. Daha az cihaz seçeneği, daha kolay cihaz yönetimi düşüncesini içeren *kendi cihazını seç* (CYOD) yaklaşımıyla çalışanlara arasında seçebileceği birkaç cihaz seçeneği sunulabilir. BYOD'a benzer şekilde bu yaklaşımda da çalışan cihazı kullanmakta özgürdür. Daha fazla kontrol için *şirkete ait/kişisel olarak etkinleştirilmiş* (COPE) cihazlar veya *yalnızca iş* (COBO) cihazları tercih edilebilir. Her durumda, mobil cihaz kullanımıyla ilgili politikaların belirlenmesi ve gerekli güvenlik tedbirlerinin uygulanması gerekir (Kim & Solomon, 2021). Mobil cihaz kullanımına ilişkin bazı güvenlik tedbirlerine aşağıda yer verilmektedir: (DDO, 2020)

- Mobil cihaz kullanımı için aşağıdaki hususları içeren bir politika hazırlanması ve kullanılması.
  - Fiziksel koruma
  - Parola tanımlama
  - Uygulama güncellemeleri
  - Uygulama kısıtlamaları
  - Uzaktan yönetim
  - Yedekleme
  - Bulut hizmetlerinin kullanımı
  - Kablosuz ağların kullanımı
  - El değiştirme ve imha
- Kullanıcılara mobil cihaz kullanımı ile ilgili eğitim verilmesi.
- Zararlı yazılımları tespit eden ve önleyen güvenlik uygulamaları kullanımı.
- Taşınabilir cihazlar uzaktan yönetilmesi, izlenmesi.
- Güncel olmayan sistemlerin bilgi sistemlerine erişiminin engellenmesi.
- Disk şifrelemesi.
- Ekran kilitlerinin kullanılması.
- Kişisel ve iş verilerinin birbirinden ayrılması.

Örnek Sorular

Soru 1: Aşağıdaki zararlı yazılım türlerinden hangisi, yazılım açıklıklarını ve zayıflıkları kullanarak kendi kopyalarını başka kaynaklara üzerinde bulunduğu ana bilgisayarın ağ erişimi vasıtasıyla yaymaya çalışır?

A) Solucan

B) Virüs

C) Bot

D) Truva atı

E) Fidye yazılımı

Cevap: A

Soru 2:

I- Segmentasyon

II- Şifreleme

III- Saldırı tespit ve engelleme

IV- Kullanıcı kimlik doğrulama

V- Veri sızıntısı önleme

Yukarıdakilerden hangisi/hangileri temel ağ güvenliği kontrolleri arasındadır?

A) I, II, III

B) II, III, IV

C) III, IV, V

D) I, II, V

E) Hepsi

Cevap: E

5. ERİŞİM GÜVENLİĞİ

Bu bölümde, kimlik ve erişim yönetimi kapsamında kimlik tanımlama, kimlik doğrulama, yetkilendirme kavramları üzerinde durulmakta mantıksal erişim ve mantıksal erişim kontrolleri konularına yer verilmektedir.

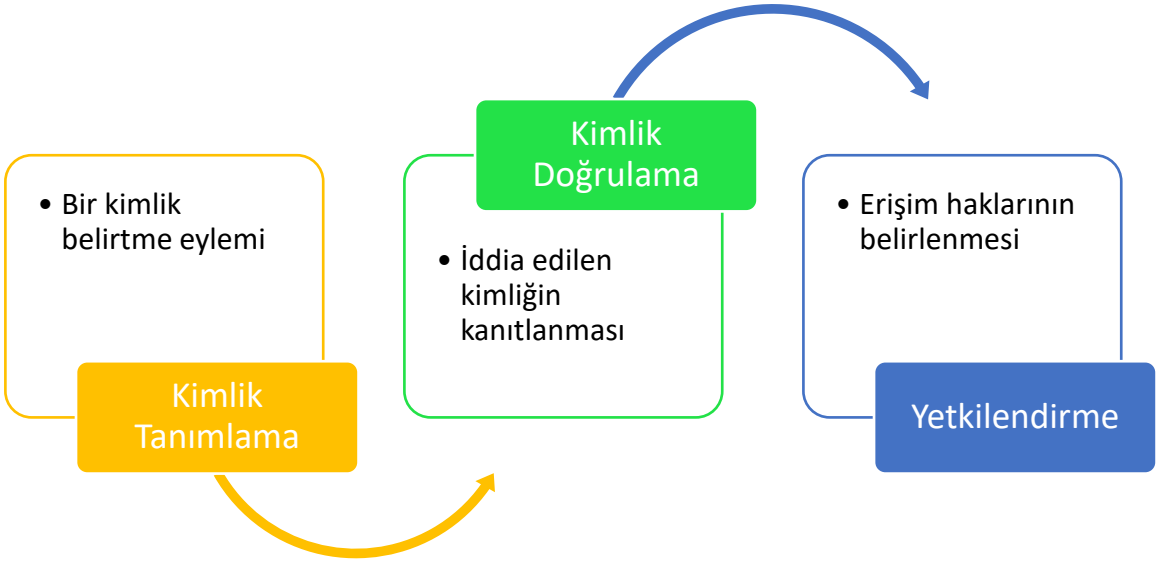
5.1. Erişim Kontrolü Kavramları

Erişim; bilgi sistemlerinden yararlanabilme, bu kaynaklar üzerinde bir program çalıştırma, okuma, yazma, silme ve değiştirme veya bağlantı kurma benzeri işlemleri gerçekleştirebilme yeteneğidir. Erişim kontrolü ise aşağıdaki gibi tanımlanmaktadır:

"Bilgi ve ilgili bilgi işleme hizmetlerinin elde edilmesine ve kullanılmasına veya fiziksel olarak bir binaya, tesise girilmesine yönelik taleplere izin verilmesi veya reddedilmesi süreci" (NIST, 2017: 59).

Erişim kontrolü tanımdan anlaşılacağı üzere bilgi sistemleri kaynaklarına erişimi kontrol etmenin teknoloji tabanlı yöntemleri olarak fiziksel ve mantıksal olmak üzere iki başlık altında ele alınmaktadır (Gregory, 2019). Fiziksel erişim ve kontrollerine fiziksel ve çevresel güvenlik bölümünde yer verilmekte, bu kısımda mantıksal erişim konusu üzerinde durulmaktadır.

Mantıksal erişim, "kimlik tanımlama, kimlik doğrulama ve yetkilendirme vasıtasıyla erişim izni verilen bilişim kaynaklarıyla etkileşim kurabilmek" şeklinde ifade edilmektedir (ISACA, 2018). Mantıksal erişimi oluşturan kimlik tanımlama, kimlik doğrulama ve yetkilendirme kavramları aşağıda açıklanmaktadır. (Şekil 37)



Şekil 37: Mantıksal Erişim Unsurları

Mantıksal erişim kapsamında doğrulama ve yetkilendirme süreçlerinin gerçekleştirilmesinden önce birincil olarak kimlik tanımlamanın yapılması gerekmektedir. Kimlik tanımlaması, bir kişinin veya nesnenin kendini tanımlayan kullanıcı kimliğinin belirtilmesi eylemidir (Drozhzhin, 2020). Sıklıkla, kişinin adı ve soyadı birleşimiyle bir kullanıcı ismi veya e-posta adresi kullanılmaktadır. Örneğin, Emre Kalkan için emre.kalkan kullanıcı ismi. Kimlik doğrulaması ise, kimlik tanımı iddiasının geçerliliğini belirlemenin yoludur. Örneğin, Emre Kalkan tarafından bilenen ve gizli olarak tutulan bir parola. Kimlik tanımlaması olmadan doğrulamanın, kimlik doğrulaması yapılmadan kimliğin tanımlamasının bir anlamı olmayacağı için kimlik tanımlaması, kimlik doğrulaması ile genel olarak birlikte ele alınmakta ve birçok sistem açısından erişim güvenliğinin ilk savunma hattını oluşturmaktadır. Bu bağlamda, bilgi sistemlerine yetkisiz kişilerin girmesini ve yetkisi olunmayan işlemlerin gerçekleştirilmesini önleyen

teknik bir önlem olarak bilgi sistemleri güvenliğinin kritik bir yapı taşı olarak yer almaktadır. (NIST, 1995).

Kimlik tanımlama ve doğrulama işlemleri gerçekleştirildikten sonra bilgi sistemlerinde herkesin her bilgiye erişme ve her işlemi yapma yetkisi olmayacaktır. Yetkilendirme süreciyle kimin, hangi bilgi sistemi kaynaklarına nasıl bir erişim hakkına sahip olduğunun belirlenmesi gerekmektedir. Bu yönde kullanıcılara verilen yetkiyle birlikte bilgi sistemi kaynakları üzerinde okuma, yazma, silme, değiştirme, program çalıştırma veya bağlantı kurma olanağına sahip olunacaktır. Bu süreç kapsamında, öznenin (bir şeye erişmek isteyen kişi, program, cihaz veya bilgisayar) nesneye (dosya, veritabanına kaydı, uygulama, bilgisayar vb. erişilmek istenen kaynak) erişimine izin verilip verilmeyeceğine karar verilebilmesi için bir yetki tablosunda arama yapılması veya yetkilendirmeye ilişkin bir kuralın onaylanması sağlanacaktır (Gregory, 2019).

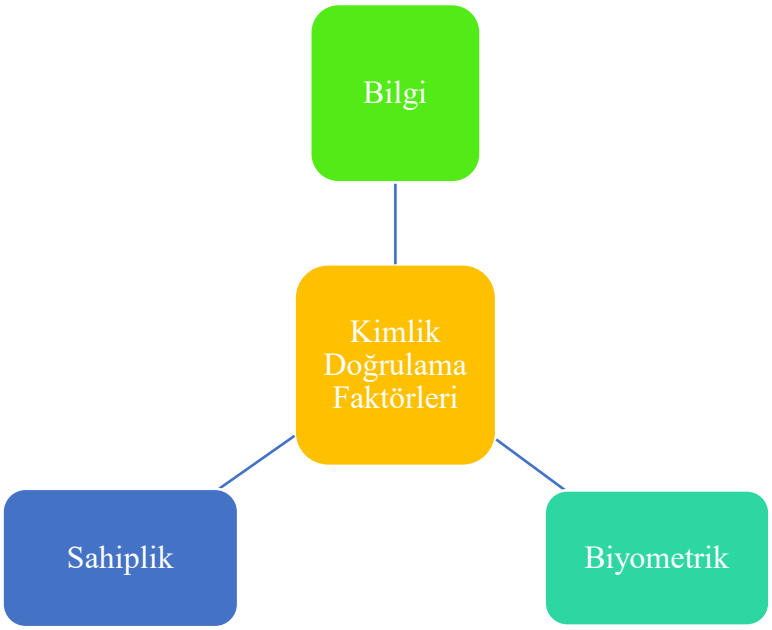
5.2. Kimlik Doğrulama Yöntemleri

Bilgi sistemlerine erişim güvenliği önemli ölçüde mantıksal erişim sürecinde kullanılan kimlik doğrulama yönteminin gücüne bağlıdır. Kimlik doğrulama yöntemleri kullanılan doğrulama faktörüne göre aşağıdaki gibi 3 kategori altında yer almaktadır:

- **Kişinin bildiği bir şey (Something you know):** Kimlik doğrulamasında parola, PIN(kişisel kimlik numarası), güvenlik soruları vb. bilgi faktörünün kullanımıdır.

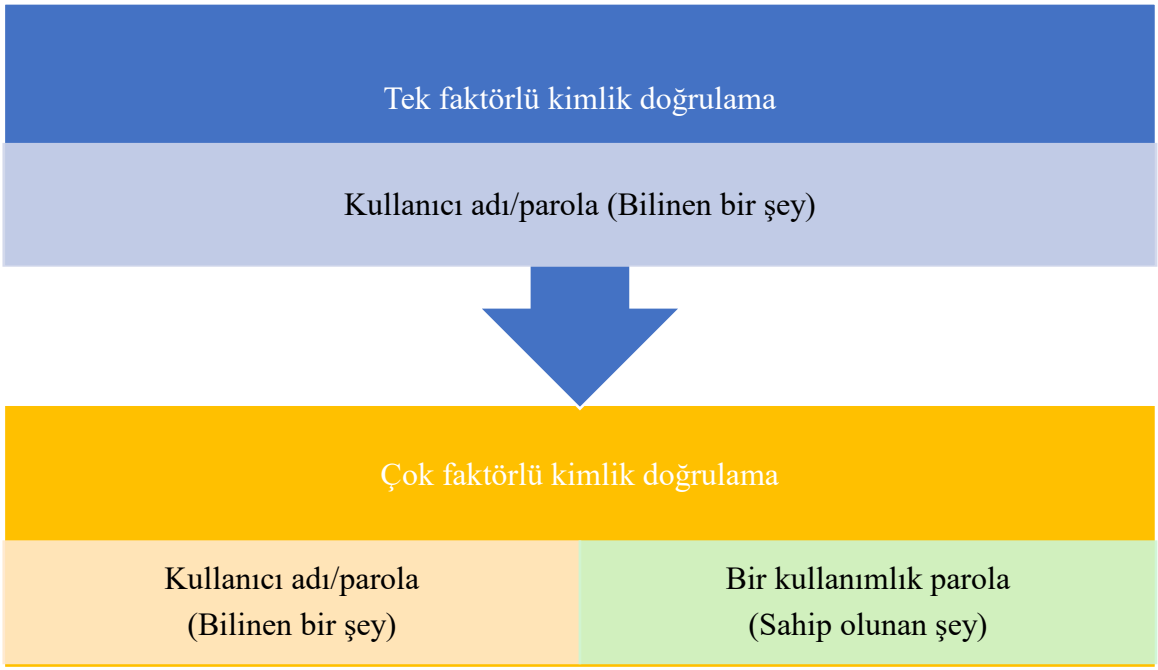
- **Kişinin sahip olduğu bir şey (Something you have):** Kullanıcının sahip olduğu token, akıllı kart, bir kullanımlık parola gibi doğrulama esnasında kullanıcının yanında bulunması gereken faktörleri içermektedir.

- **Kişinin olduğu bir şey (Something you are):** Kişinin kendine has biyometrik faktörler olarak parmak izi, iris, yüz, ses, yürüyüş, imza, klavye tuşlarına basma şekli benzeri fiziksel veya davranışsal özelliklerin tanınmasına dayanmaktadır (“Kimlik doğrulama,” 2022).



Şekil 38: Kimlik Doğrulama Faktörleri

Bilgi sistemlerine erişmek için kullanıcı adı ve parola çifti kullanımı en yaygın ve kolay uygulanabilen bilgiye dayalı kimlik doğrulama yöntemi olarak *tek faktörlü kimlik doğrulamaya* örnek verilebilir. Erişim güvenliğini daha iyi sağlamak adına birden fazla faktörün aynı anda kullanılarak kimlik doğrulama işlemi gerçekleştirilmesi durumu *çok faktörlü kimlik doğrulama* olarak adlandırılmaktadır (Anadolu Üniversitesi, 2018:88).



Şekil 39: Çok Faktörlü Kimlik Doğrulama

Kullanıcı adı ve parola kullanımı üzerine oluşturulmuş Lokal depolama, Merkezi depolama, Kerberos şeklinde değişik kimlik doğrulama uygulamaları bulunmaktadır. Kullanıcı adları ve parolaların bilgi sistemleri üzerinde lokal olarak saklandığı durumlarda parolaların dosyalarda açık olarak saklanması nedeniyle kolaylıkla ulaşılması, şifreli olarak saklandığı durumlarda şifreleme algoritmalarının çok güçlü olmamasından kaynaklı kaba kuvvet ve sözlük saldırısı yöntemleriyle parolaların elde edilebilmesi mümkün olmaktadır. Bu bağlamda, parolaların fiziksel olarak korunmasının ve güvenliğin arttırılmasının merkezi depolama ile sağlanmaya çalışıldığı görülmektedir. Merkezi depolamada ise kullanıcının girmiş olduğu parolanın ağ üzerinde açık veya şifreli iletilmesiyle ilgili güvenlik sorunları ortaya çıkmaktadır. Kullanıcının girmiş olduğu parolanın ağ üzerinden merkezi sunucuya güvenli bir şekilde iletilmesi için hem kullanıcının hem de sunucunun doğrulanması gerektiği için bu yönde geliştirilmiş kimlik doğrulama yöntemleri olarak CHAP ve MS-CHAP protokolleri bulunmaktadır (Anadolu Üniversitesi, 2018:89).

Kerberos, MIT (Massachusetts Institute of Technology) tarafından geliştirilen bilet-tabanlı ağ kimlik doğrulama yöntemi, standardında parolayla birlikte sertifikalar da kullanılarak kimlik doğrulama yapılabilmektedir. Kerberos protokolünde dağıtık mimariye sahip bilgisayar sistemlerinde (DCE) hem kullanıcıların hem de sunucular ve üzerinde sunulan hizmetlerin merkezi olarak kimlik doğrulaması gerçekleştirilmektedir. Kimlik doğrulaması sürecinde iki farklı aşama bulunmaktadır. Birinci aşamada uzaktaki sistem kaynaklarına erişmek isteyen kullanıcının ilk oturum sürecinde kimliğinin doğrulanması sağlanmakta ve kullanıcıya bir bilet sağlanmaktadır. Bu süreçten sonra kullanıcının oturum süresi sona erene kadar parolasını tekrar girmesi istenmemekte, sunucular üzerindeki servislere erişim için kimlik doğrulamaları bu bilet bilgisi üzerinden devam etmektedir (Anadolu Üniversitesi, 2018:90).

Kerberos, bir tek kullanıcı adı ve parolayla bir tek oturum açarak birden çok sunucu ve hizmetlere tekrar oturum açmadan erişmeyi açıklayan *tek oturum açma (SSO)* kavramına bir örnektir. SSO bir kuruluşun platform tabanlı bütün yönetim, kimlik doğrulama ve yetkilendirme işlevlerinin tek bir merkezi yönetim işlevinde birleştirme süreci olarak tanımlanmaktadır. Bu yönde; bir kuruluşun istemci-sunucu ve dağıtık sistemlerine, uzaktan erişim mekanizmaları dahil ağ güvenliğine yönelik uygun arayüzler SSO ile sağlanmaktadır. SSO'nun, birçok sistem için tek bir kimlik doğrulama noktası olması nedeniyle tek bir hata noktası riski oluşturması, çok farklı sistemlere uyumunun zorluğu ve geliştirmesiyle ilgili maliyetleri dezavantajları olarak sıralanabilir. Bununla birlikte kullanıcıya tek bir kullanıcı/parola çifti yeterli olduğu için kullanıcıların bu tek şifreyi daha güçlü belirlemesine yönlendirmesi, yöneticiler tarafından kullanıcı hesaplarının yönetilme becerisini iyileştirmesi, unutulan

parolaların sıfırlanması için destek talebinin azalması ve farklı uygulamalara oturum açma için gerekli sürenin kullanıcıya kalması gibi avantajları içermektedir. (ISACA, 2019:270)

Şekil 40: Tek Oturum Açma'nın(SSO) Avantajları

Kullanıcıların çoğunlukla kolay tahmin edilebilir parolalar oluşturma, sahip olduğu parolaların güvenliği konusunda farkındalık eksikliğiyle birlikte oluşturdukları parolaları unutmamak için farklı bilgi sistemlerinde aynı parolayı kullanma eğilimi bulunmaktadır. Bu durum saldırganlar tarafından bilgi sistemleri üzerinde kötü niyetli yazılımlar vasıtasıyla kullanılmasına yol açmaktadır. Karşılaşılan bu tarz sorunları ortadan kaldırabilmek için kullanıcı tarafından oluşturulan parolaların yerine kimlik doğrulamasında belirli bir protokole göre üretilen *bir kullanımlık parolaların* kullanımı çözümleri geliştirilmiştir. Bu yöntemlerde, bir kullanımlık parolaların hem kullanıcı tarafında hem de sunucu üzerinde benzer şekilde oluşturulması gerekmektedir. Kullanıcılar akıllı kart, token, cep telefonu kullanarak donanım veya yazılım tabanlı bir kullanımlık parola üretebilmektedir. Bunun yanında kullanıcılar tarafından, bilgi sistemlerine erişim esnasında kullanıcı adı ve parolaya ek olarak bir kullanımlık parolanın girilmesi de istenerek kullanıcının bildiği ve sahip olduğu bir şey faktörlerinin ikisi de sağlanarak iki (çok) faktörlü kimlik doğrulama gerçekleştirilmektedir. Bu şekilde; saldırganlar kullanıcı parolasını ele geçirmiş olsa dahi bilgi sistemlerine erişim imkanına sahip olamayacaktır (Anadolu Üniversitesi, 2018:91).

Şekil 41: Biyometrik Özellikler

Bir kullanıcının kimliğinin doğrulanmasında biyometrik faktörler de kullanılmaktadır. Biyometrik kimlik doğrulama insanların fiziksel ve davranışsal özelliklerinin ölçülmesine dayanmaktadır. Bu şekilde kullanılacak özelliklerin kişiye özgü ve eşsiz olması, farklı kişileri birbirinden ayırt edebilecek özellikler olması gerekmektedir. Şekil 41'de kimlik doğrulamasında kullanılan biyometrik özelliklerden bazıları yer almaktadır. Kullanıcıların bu özelliklerinin kimlik doğrulama sistemlerinde öncelikle uygun donanımlarla alınması ve kaydedilmesi aşamasının gerçekleştirilmesi gerekmektedir. Daha sonra; kimlik doğrulama aşamasında kullanıcıdan alınan değerler ile saklanan biyometrik verilerin her bir özelliğe göre değişik algoritmalarla karşılaştırması sağlanır. Biyometrik tanıma cihazları arasında parmak izi tanıma ve yüz okuma yaygın olarak kullanılmaktadır (Anadolu Üniversitesi, 2018:93). Biyometrik cihazların performansının belirlenmesi için kullanılan aşağıda açıklanmakta olan doğruluk ölçümleri biyometrik sistemlerin başarı faktörünü belirlemektedir (Doshi, 2020).

- **Yanlış kabul oranı (FAR):** Bir bilgi sistemini kullanma yetkisi olmayan kişilerin yanlışlıkla kabul edilmesini belirten orandır. Sistemlere yetkisiz giriş riskini gösterdiği için bu gösterge önemlidir.

- **Yanlış reddetme oranı (FRR):** Bir bilgi sistemini kullanma yetkisi olan doğru bir kişinin reddedilmesi oranıdır.

- **Çapraz hata oranı (CER) veya eşit hata oranı (EER):** Biyometrik cihazlar FAR ve FER oranlarını düşürmek için ayarlanır ve bu iki oranın eşit olduğu değer çapraz hata oranını belirler. Düşük CER veya EER'ye sahip biyometrik cihazlar daha etkili sistemler olacağı için bu değerler üzerinden cihazların performansı değerlendirilmektedir.

5.3. Erişim Kontrol Türleri

Erişim kontrolü ile ilgili iki ana kategori *zorunlu erişim kontrolü (MAC), isteğe bağlı erişim kontrolü (DAC)* aşağıda açıklanmaktadır:

Zorunlu erişim kontrolü nesnelere erişimi (dosya, dizin, veritabanı, sistem, ağ vb.) öznelere (kişiler, programlar, bilgisayarlar vb.) göre kontrol etmek için kullanılır. Erişim kontrol kuralları onaylanmış bir politikaya bağlı olarak merkezi olarak sistem yöneticileri tarafından yönetilir ve kullanıcılar veya veri sahipleri erişime izin verilip verilmeyeceğini değiştiremez. Erişim kontrolü öznenin ve nesnenin erişim özellikleri incelenerek sağlanır. İsteğe bağlı erişim kontrolünde, bir nesnenin sahibi nesneye nasıl ve kim tarafından erişilebileceğini belirleyebilmekte ve değiştirebilmektedir. (Doshi, 2020; Gregory, 2019).

Şekil 42: Erişim Kontrol Türleri

5.4. Erişim Kontrol Prensipleri

Mantıksal erişim kontrolleri; "bilgisayar yazılımına ve veri dosyalarına erişimi kısıtlamak için tasarlanan politikalar, prosedürler, organizasyon yapısı ve elektronik erişim kontrolleri" (ISACA, 2018) şeklinde ifade edilmektedir. Mantıksal erişim kontrolleri kimin bir sistem kaynağına erişeceğini belirlemekle birlikte izin verilen erişim türünü de belirleyebilir. Sistem erişim izinleri, bilgi sistemlerinden yararlanabilme, bu kaynaklar üzerinde bir program çalıştırma, okuma, yazma, silme ve değiştirme veya bağlantı kurma benzeri işlemleri gerçekleştirebilme ayrıcalıklarını içermektedir. Mantıksal erişim kontrolleri korunması gereken bilgi sistemlerinde dahili veya harici olarak uygulanabilir; işletim sistemine yerleştirilebilir, uygulama programlarına, veritabanlarına, ağ kontrol cihazlarına ve diğer yardımcı programlara dahil edilebilir (NIST, 2017:59).

Mantıksal erişim kontrollerini uygulamak için aşağıdaki süreç izlenmelidir: (Doshi, 2020)

- Bilgi sistemleri kaynaklarının envanterinin oluşturulması.
- Bilgi sistemleri kaynaklarının sınıflandırılması.
- Bilgi sistemleri kaynaklarının gruplandırılması/etiketlenmesi.
- Bir erişim kontrol listesinin oluşturulması.

Mantıksal güvenlik altındaki bilgi sistemleri ağlar, platformlar/işletim sistemleri, veritabanları ve uygulamalar olmak üzere dört katmanda gruplanabilir. Erişim güvenliğini sağlamak için bütün bilgi sistemleri katmanlarına erişim kontrolleri uygulamak gerekir. Bu süreçte genel olarak kimlik tanıma, kimlik doğrulama, yetkilendirme ve bu işlevlerin günlüğe kaydedilip raporlanması gerçekleşir. Erişim kontrol yazılımları içerden veya dışardan kullanıcıların yetkisiz erişimine karşı uygulanarak özellikle ağ ve platform seviyesinde korunmayı sağlar. Bu iki katman birlikte genel destek sistemleri olarak adlandırılır ve uygulama ve veritabanı katmanlarının altyapısını oluştururlar. Kısacası, erişim kontrol yazılımları bilgi sistemleri içerisinde farklı seviyelerde güvenliğin sağlanması için kullanılır. Üst katmanlar genel sistem kaynaklarının korunması noktasında alt katmanlara bağımlıdır ve görevlerin fonksiyon bazında ayrılması açısından uygulama seviyesinde ihtiyaç duyulan detaylandırmayı sağlar. (ISACA, 2019:263) Bu kapsamda uygulanabilecek mantıksal erişim kontrolleri ve prensiplerine aşağıdaki bölümde yer verilmektedir: (DDO, 2020; TSE, 2013)

- Erişim kontrol politikası oluşturulmalı, uygulanmalı ve güncelliği sağlanmalıdır. Mantıksal erişim yetenekleri, bilgi sistemleri yöneticileri tarafından bir dizi erişim kuralı dahilinde uygulanmaktadır. Bu kuralların belirlendiği doküman olan erişim kontrol politikası çerçevesinde

kullanıcı hesap yönetimi ve erişim talepleri bir süreç olarak takip edilmeli ve kayıt altına alınmalıdır. Kurumsal kaynaklara erişen kuruluş dışı kişiler de dahil erişim politikalarına uyum sağlanmalıdır.

- Kuruluş kaynaklarına erişimde merkezi kimlik doğrulama mekanizmaları kullanılmalıdır. Kuruluş ağına İnternet üzerinden yapılan erişimler için çok faktörlü kimlik doğrulama seçenekleri göz önünde bulundurulmalıdır.

- Hesap verme sorumluluğu; belirli bir faaliyeti veya olayı sorumlu tarafa geri döndürme becerisi olarak tanımlanmaktadır (ISACA, 2018). Kullanıcıların yaptığı işlemlerden sorumlu olmasını sağlayacak şekilde kullanıcıları tanımlayan eşsiz/benzersiz kullanıcı adları belirlenmeli ve parolaları oluşturulmalıdır. Kullanıcı adları belirlenirken belirli bir adlandırma kuralı uygulanmalıdır. Guest, Admin, Administrator vb. varsayılan kullanıcı adı ve parolalar kullanılmamalı, devre dışı bırakılmalı veya mümkün olduğu durumlarda yeniden adlandırılmalıdır. Kuruluştan ayrılan kullanıcı hesapları veya önceden belirlenmiş bir süre boyunca kullanılmayan hesaplar devre dışı bırakılmalıdır.

- Kullanıcı oturumları belirli bir süre sonra sonlandırılmalı ve işlem yapılmadığı, aktif olunmadığı zamanlarda otomatik olarak kilitlenmelidir.

- Kullanıcılar tarafından parolalar oluşturulurken dikkat edilmesi gereken kurallar belirlenmeli ve uygulanmalıdır. Örneğin, en az parola uzunluğunun belirlenmesi, rakam/harf/özel karakter kombinasyonlarının kullanımının zorlanması, parolanın kolay tahmin edilebilir olmaması, kişisel bilgileri içermemesi, belirli sürelerde değiştirilmesi, eski parolalardan farklı parolalar oluşturulması vb.

- Bilgi sistemlerine erişim yetkileri bilmesi gereken (need to know), en az ayrıcalık (least privilege), görevler ayrılığı (SoD) ilkeleri dahilinde verilmeli, onaylanmalı, kaydı tutulmalı ve düzenli aralıklarla verilen erişim yetkileri gözden geçirilmelidir. Bu ilkeler aşağıdaki şekilde açıklanmaktadır:

Bilmesi gereken prensibi: Yetkilendirmelerin, görev ve sorumluluklar çerçevesinde belirlenmesini ifade eder. "Herhangi bir konu veya işi ancak görev ve sorumlulukları gereği öğrenmekle, incelemekle, gereğini yerine getirmekle ve korumakla sorumlu bulunanların; yetkisi düzeyinde bilgi sahibi olması ve nüfuz etmesidir." (Milli Savunma Bakanlığı, 2010)

En az ayrıcalık prensibi: Bu prensiple, bir kullanıcının görev ve sorumluluklarını gerçekleştirmesi için minimum erişim seviyesinin kullanıcıya sağlanması amaçlanmaktadır. Bir diğer deyişle; yetkinin işin amaçlarından geniş olmaması, bilgi sistemleri kapsamında kullanıcılara aşırı yetkilendirme yapılmasının önüne geçilmesi ve kullanıcılara işlerini yapabilmeleri için yeterli yetkiyi vermek anlamına gelir (Kim & Solomon, 2021). Mesela, betik dosyası oluşturma araçlarına (powershell, python) sadece iş amaçları doğrultusunda erişmesi gerekenlere izin verilmelidir.

Görevler ayrılığı: Görevler ayrılığı ilkesi, ISACA terimler sözlüğünde (2018); "ayrı şahıslara, işlemlerin başlatılması ve kayıt altına alınması ve varlıkların gözetimi için sorumluluk üstlenerek hata ve usulsüzlükleri önleyen veya tespit eden temel bir iç kontrol. Görevlerin ayrıştırılması / ayrılması, büyük kuruluşlarda yaygın olarak kullanılır, böylece hiçbir kişi, tespit edilmeksizin hileli veya kötü niyetli kodları tanıtamaz." şeklinde tanımlanmaktadır. Bilgi sistemleri kapsamında sistem, ağ, veritabanı ve uygulamaların geliştirilmesinde, test edilmesinde ve işletilmesinde kritik işlemlerin tek bir personele ve hizmet sağlayan kuruluşa bağımlı olmaması göz önünde bulundurularak görevler ayrılığı prensibi uygulanmalıdır (SPK, 2018).

- Yüksek seviyede haklar gerektiren yönetici hesaplarının kullanımı kısıtlanmalı, gerekli durumlarda onay mekanizmasıyla verilmeli ve kaydı tutulmalıdır. Sistem yöneticileri için normal işlerde kullandıkları hesaplardan ayrı sistem hesapları oluşturulmalı ve bu hesaplarla yapılan işlemler kayıt altına alınmalıdır.

- Erişim saldırılarına karşı önlemler alınmalı, uyarı mekanizmaları oluşturulmalıdır. Oturum açma saldırılarına karşı başarısız oturum açma sayısı belirleyerek hesabı kilitleme, IP bloklama, Captcha kullanımı benzeri güvenlik önlemleri alınmalıdır. Bu kapsamda işletim sistemlerine, veritabanı sistemlerine, dosyalara ve dizinlere vb. başarılı/başarısız erişim girişimleri kayıt altına alınmalı ve bütünlüğü sağlanmalıdır (Gregory, 2019).

Örnek Sorular

Soru 1: Aşağıdaki özelliklerden hangisi isteğe bağlı erişim kontrolü özellikleri arasında değildir?

A) Nesne sahibinin erişim haklarını belirleyebilme esnekliği

B) Yetkilerin transfer edilebilmesi

C) Katı ve sağlam olması

D) Kötüye kullanım ve hassas bilgilerin açığa çıkma riski

E) Hiçbiri

Cevap: C

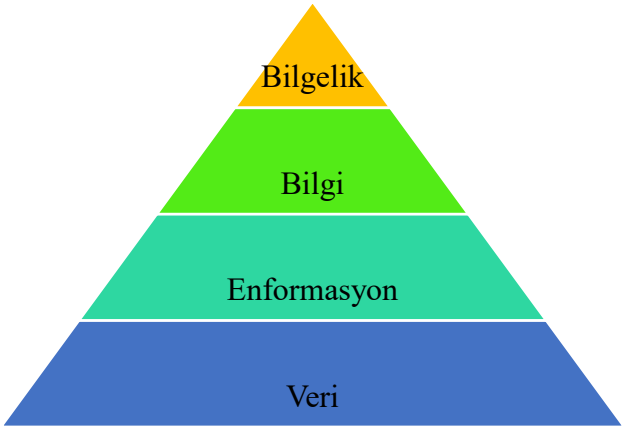
6. VERİ VE İZ KAYITLARININ GÜVENLİĞİ

6.1. Veri ve İz Kayıtlarının Güvenliği

Bu bölümde, iz kayıt (log) sistemlerine ilişkin kavramlar ile verinin oluşturulma, taşınma, saklanma ve imha sürecinde izlenmesi gereken süreçlere yer verilmektedir. Bununla birlikte veri şifrelemeye ilişkin teknolojilerden de bahsedilecektir.

6.2. Veri ve Veriye İlişkin Kavramlar

Veri üzerine konuşmadan önce, verinin tanımı ve bilgi güvenliği kapsamında veriye bakış açısının açıklığa kavuşturulması gerekmektedir. Veri, (Latince Datum'dan türetilmiş, İngilizce Data) "Olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi." (TDK Sözlük) olarak tanımlanmakta olup İngilizcede çoğul kullanımı (datas) bulunmamaktadır. Bilgi sistemleri kapsamında birçok farklı teorik hiyerarşi içerisinde değerlendirilmekte olup bu hiyerarşilerden en bilineni olan DIKW piramiti yaklaşımında, veri'yi hiyerarşinin en alt basamağında "ham" olarak değerlendirmekte ve işlemler sonrasında bir üst basamağa çıkartmaktadır.



Şekil 43: DIKW Piramidi

DIKW yaklaşımına göre, veri ham bir durumu ifade etmekte, kurulan ilişkiler sayesinde anlamlı olduğunda enformasyon halini almakta, kullanılabilir haline bilgi (knowledge), icraata dönüşmüş haline de bilgelik denilmektedir. Kısaca, Veri: "Gerçek", Enformasyon: "Ne olduğunu bilme", Bilgi: "Nasılı bilme" ve Bilgelik: "Nedenini bilme" şeklinde ifade edilebilir. (Anadolu Üniversitesi)

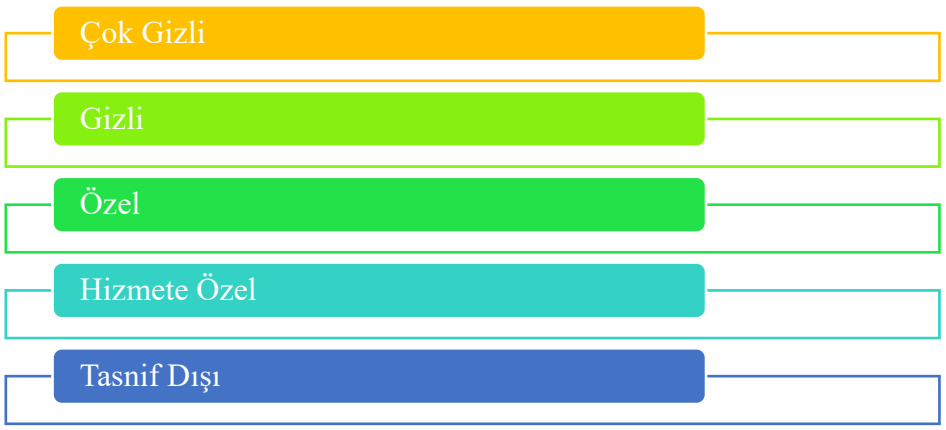
Veriye ilişkin bir diğer teorik altyapı ise verinin durumuna ilişkin yaklaşımdır. Bu kapsamda verinin 5 farklı durumu söz konusudur; verinin üretimi, kullanımı, saklanması, taşınması ve nihayetinde imhası. Her bir aşama için gerekli kontrollerin yapılması ve bu aşamada veriye ilişkin değerlendirme için CIA üçlüsünün değerlendirilmesi mümkündür.

Veri ile ilişkili bir diğer tanım da metaveri (İng. metadata) olup, veri hakkında veri olarak ifade edilebilir. Metaveri de veri hakkında sağladığı bilgiler dolayısıyla veya diğer metaveriler ile bir araya gelerek anlamlı bir veri kümesi haline gelebilir.

Kişisel veri ise, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi (KVKK) ifade eder. Verilerin kişisel oluşu, söz konusu verilere ilişkin farklı kısıtlar getirmekte ve uygulamada değişikliklere gidilmesini gerektirebilmektedir.

6.3. Veri Sınıflandırılması

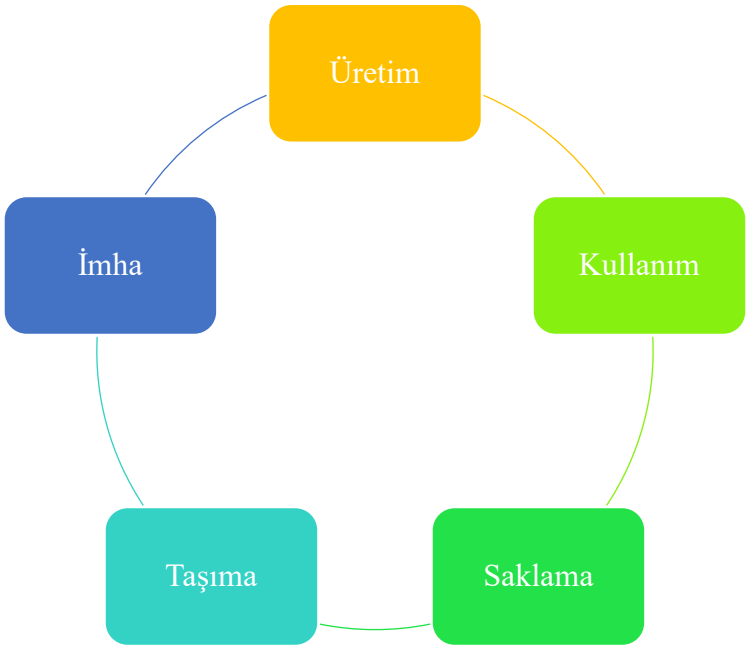
Veriye ilişkin kontrollerin gerçekleştirilmesi sırasında farklı güvenlik seviyeleri tanımlanması mümkündür. Her bir varlık aynı önem seviyesine sahip olmadığı için yapılacak kontrollerin ve erişim tanımlarının da bu durumu yansıtır şekilde yapılmasının ön şartı önem derecesine göre sınıflandırılma yapılmasıdır. Bu kapsamda Varlık Sınıflandırması bölümünde anlatıldığı üzere veri için de varlık sınıflandırılması yapılması gerekmektedir. İş gereklerine göre gerçekleştirilebilecek bu sınıflandırmaya örnek olarak; DDO Rehber'de yer aldığı üzere "Bilmesi gereken kişiler dışındakilere açıklanması veya verilmesi, millî güvenlik ve ülke menfaatleri bakımından sakıncalı görülen ve haiz olduğu önem derecelerine göre "çok gizli", "gizli", "özel" veya "hizmete özel" şeklinde sınıflandırılma yapılması mümkündür. Oluşturulacak kontroller ve denetim de bu çerçeve bağlamında gerçekleştirilebilir.



Şekil 44: Örnek sınıflandırma tablosu

6.4. Veri Yaşam Döngüsü

Veri yaşam döngüsü 5 durumdan oluşmaktadır; verinin üretimi, kullanımı, saklanması, taşınması ve nihayetinde imhası. Her bir aşama için gerekli kontrollerin yapılması ve bu aşamada veriye ilişkin değerlendirme için CIA üçlüsünün değerlendirilmesi mümkündür.



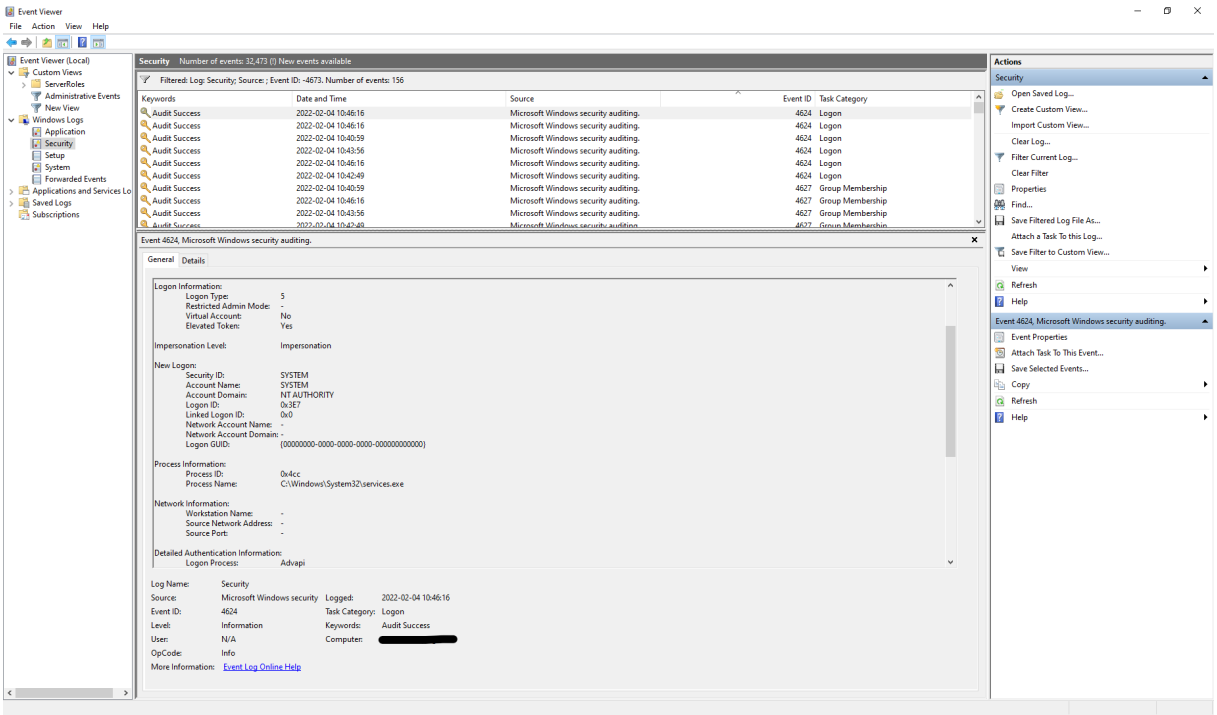
Şekil 45: Veri Yaşam Döngüsü

6.5. İz Kayıtları

İz kayıtları veya günlükler (İng. Log) bir kuruluşun sistemleri ve ağları içerisinde meydana gelen olaylara ilişkin kayıtları ifade eder. Her bir "satır" meydana gelen bir olaya ilişkin belirli bilgileri içerir. Aslen problem takibi için kullanılan log kayıtları, günümüzde birçok alanda ve karar mekanizmalarında veri kaynağı olarak da kullanılmakta, belirli şartları sağladığında hukuki süreçlerde kanıt olarak değerlendirilmektedir.

Bilgi sistemlerinde yapılan her bir işlem tüm sürecin herhangi bir evresinde yapılan işlemin başarılı ya da başarısız olduğu veya herhangi bir erişim işleminde taraflara ilişkin adres, port, saat, fiziksel cihaz bilgileri gibi sürece ilişkin bir iz kaydı oluşturabilir. Bilgi Sitemleri Yönetimi Tebliğine göre asgari olarak yapılan işlemin türü ve niteliği, işlemi gerçekleştiren uygulama ve/veya kişi, tarih ve saat bilgilerini içermelidir.

İz kayıtlarına örnek olarak, bilgisayar güvenlik kayıtları (security logs) veya bina giriş-çıkış sistemleri kayıtları verilebilir.



Şekil 46: Örnek Log Kaydı

Artan tehditler ve saldırılar karşısında, iz kayıtları sadece işlemleri değil, sistemlere yönelik yetkisiz erişimleri de kayıt altına almaktadır. Veriler için geçerli olan, üretim, kullanım, saklama, taşınma ve imha süreçleri, iz kayıtları için de gerçeklidir. İz kayıtlarının üretimi, düzenli olabileceği gibi, farklı periyotlarda gerçekleşmesi de mümkündür. Her halükarda, iz kayıtlarına ilişkin en önemli nokta, iz kayıtlarını üreten ve toplayan sistemlerde ağ zaman protokolü (Network Time Protocol – NTP) ile tarih ve zaman değerlerinin merkezi bir sistemden referans alınarak (Örn: pool.ntp.org) tüm iz kayıtlarının zaman damgalarının eşleşmesini sağlamaktır.

İz kayıtlarının oluşturulduktan kısa bir zaman içinde bozulmasını, değiştirilmesini, tahrip edilmesini engellenmesine yönelik bir takım tedbirler alınabilir. Bu işlemler hem dosyaların değişmediğinin göstergesi olarak bütünlük sağlamaya yönelik olarak yapılabileceği gibi, inkar edilemezlik (non-repudiation) de sağlayabilirler. Bunu sağlamanın yöntemleri arasında kriptografik yöntemler kullanılarak özet (hash) değerinin oluşturulması ve 3. taraflar kullanılarak dijital imzalama işleminin gerçekleştirilmesi sayılabilir.

Zaman damgası olarak adlandırılan bu işlemler ile üretilen kayıtlar, 5070 sayılı e-imza Kanunu'na göre "bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve/veya

kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kaydı" ifade eder.

Üretilen iz kaydının veya herhangi bir verinin belirtilen tarihte var olduğunun kanıtlanması denetim faaliyetleri için büyük önem arz etmektedir.

6.6. İz Kaydı Saklama Süreleri

Denetim iz kayıtlarının saklanması, belirlenmiş süreler kapsamında yapılmalıdır. Kişisel bilgi içeren denetim iz kayıtları için saklanma süreleri KVKK ile belirlenmiş olup söz konusu sürenin bitiminde imha işlemlerinin gerçekleştirilmesi gerekmektedir. Bunun dışında, şirketlerin iş süreçlerini göz önünde bulundurarak iz kaydı saklama süresi belirlemeleri gerekmektedir.

6.7. İz Kaydı Kaynakları Yönetimi

İz kayıtları, iz kaydı üreten sistemler üzerinde incelenebileceği gibi, harici bir sisteme taşınabilir veya merkezi bir sistem üzerinde toplanıp, diğer iz kayıtları ile ilişki kurulması sağlanabilir. Güvenlik bilgi ve olay yönetimi sistemleri (Security Information and Event Management – SIEM) tüm kaynak sistemlerden gelen iz kayıtlarını bir araya getirerek iz kayıtlarının birbiri ile ilişkini inceleyerek yeni bir veri oluşturulmasını da sağlamaktadır. Örneğin, bina girişi sistemlerinden gelen iz kayıtları ile Windows oturum açma iz kayıtlarını karşılaştırarak ele geçirilmiş bir bilgisayarın tespiti SIEM sistemleri ile mümkündür. Ayrıca, çeşitli algoritmik yöntemler ve yapay zeka kullanılarak da iz kayıtlarında normal dışı gerçekleşen olayların tespit edilmesi ve bunlara ilişkin bildirimlerin yapılması mümkündür.

Çoğunlukla basit metin dosyası olarak oluşturulan iz kayıtları, tek bir standart yapıya sahip değildir. Her bir sistem, kendine özgü olarak iz kaydı oluşturabilmekte ve farklı metotlar kullanabilmektedir. Bu farklılığı ortadan kaldırmak için syslog protokolü geliştirilmiş ve iz kaydı oluşturulması ve iletilmesi konusunda standartlar ve dokümanlar (RFC 5424 The Syslog Protocol) ortaya çıkmıştır.

Seviye	Önem Derecesi	Açıklama
0	Emergency	Sistemin kullanım dışı olduğuna ilişkin mesajlar.
1	Alert	Sisteme acil müdahalenin gerekli olduğuna ilişkin mesajlar.
2	Critical	Sisteme acil müdahale gerekli durumun gerçekleşmek üzere olduğunu ifade ede mesajlar.
3	Eror	Acil olmayan hatalara ilişkin mesajlar.
4	Warning	Düzeltilmemesi durumunda hataya yol açabilecek durumlara ilişkin uyarı mesajları.
5	Notice	Normal işleyiş dışında olup müdahale gerektirmeyen durumlara ilişkin bildirim mesajları.
6	Informational	Normal işleyişe ilişkin bilgilendirme mesajları.
7	Debug	Hata ayıklama mesajları.

Tablo 3: Syslog Mesajları Önem Seviyeleri

İz kayıtlarına yönelik olarak bildirimler oluşturulması mümkün olup, bu bildirimlerin anlamlı olması ve doğru taraflara iletilmesi önem arz etmektedir. Bununla birlikte, aşırı miktarda üretilen uyarı mesajları iz kaydı yorgunluğuna yol açıp etkili müdahale yapılmasına engel olabilmektedir.

6.8. Şifreleme

Kriptografi ve kriptoloji günümüzde birbirinin yerine kullanılan terimler olup latince gizli anlamına gelen kryptos kelimesinden türetilmiştir. Kriptoloji, kısaca, güvensiz ağlarda güvenli bir şekilde iletişim yapılması olarak tanımlanabilir. Bilgi güvenliğini sağlamak için kullanılan kriptoloji, çeşitli matematiksel yöntemler kullanılarak açık metin (plain-text) bir verinin şifreli metin (cipher-text) haline getirilmesi olarak da ifade edilebilir.

Şifreleme işlemleri ile birden çok güvenlik probleminin çözülmesi mümkündür. Herhangi bir verinin gizliliği ve bütünlüğünü sağlamak için kullanılabileceği gibi, kimlik doğrulama (authentication) ve inkar-edilemezlik kriptografik yöntemler ile sağlanabilir.

Şifre sisteminde, açık metin şifreli metin haline getirilirken bir algoritma kullanılması gerekmektedir. İlk şifreleme sistemleri çoğunlukla doğrudan harf değişimi şeklinde yapılmakta ve kağıt kalem kullanılarak çözülebilecek basitlikte olup, en bilinen örneği Sezar şifreleme yöntemidir. Sezar şifrelemesinde her bir harfin alfabede belirli bir sayı kadar ileri pozisyondaki harf ile değiştirilmesi ile şifreli metin elde edilmektedir. Harf değiştirme şeklinde algoritma ile çalışan şifreleme sistemleri, frekans analizi gibi yöntemler ile kolaylıkla çözülebildiği için çoklu harf değiştirme yöntemlerine yol açmış, bu algoritmalar da blok-şifreleme yöntemlerinin geliştirilmesine ön ayak olmuştur.

Teknik/algoritmik yöntemler ile çözüm sunan kriptografik işlemlerin çeşitli açıkları da bulunmakta, kriptografik sistemlere yönelik saldırılar, doğrudan algoritmaya yönelik olarak yapılmakla beraber, insan faktörü ile (hırsızlık, şantaj, rüşvet vs.) alt edilebildikleri gibi, yan-kanal (side-channel) saldırıları ile algoritmanın uygulama şekline yönelik açıklıklar kullanılabilmektedir. Bu kapsamda, bilinen bir algoritmanın doğru şekilde uygulanması, yeni bir algoritma üretilmesinden daha güvenli olduğu kriptografi araştırmacıları arasında yaygın bir kanaat olup, "never roll your own crypto" sözü ile halihazırda var olan açık kaynak sistemlerin kullanılmasının daha güvenli olacağı ifade edilmektedir.

Çeşitli saldırı yöntemlerine karşı dayanıklı olması için, kriptografik sistem ile elde edilen şifreli-metin rasgele (rassal/random) "görünümlü" (psuedo-random) olmalı, tekrar eden kısımlar bulunmamalıdır. Hiçbir saldırı ile kırılması mümkün olmayan bir kriptografik yapı, tek kullanımlık şerit (one-time pad) mümkün olmakla beraber, böyle bir yapının yaygınlaştırılması ve şifre dağıtımı kolay olmadığı için PKI gibi farklı kriptografik yöntemler geliştirilmiştir.

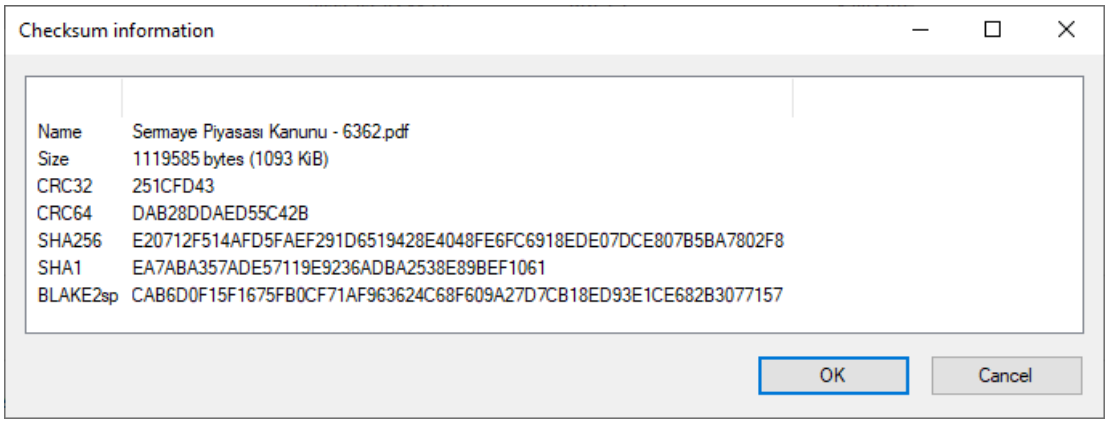
Modern kriptografik sistemler, anahtar kullanan sistemler olan simetrik ve asimetrik olarak iki grup altında incelenebilir. Herhangi bir anahtarın kullanılmadığı veri özeti (hash) de kriptografik yöntemler arasında sayılmaktadır.

6.8.1. Kriptografik Özet

Kriptografik yöntemler kullanılarak herhangi açık bir metin, daha sonra deşifre edilebilecek şekilde şifrelenebileceği gibi, benzer kriptografik yöntemler kullanılarak, herhangi bir uzunluktaki metne ait "metin özeti" elde edilebilir. Özet fonksiyonu olarak adlandırılan bu yöntem ile metin boyutundan bağımsız olarak, sabit uzunlukta (karakter sayısında) bir özet bulunabilir.

Şekil 47'de gösterilen grafikte, Sermaye Piyasası Kanunu'nun pdf uzantılı şekilde düzenlenmiş dosyasının özeti alınmış olup, dosya değişmediği sürece aynı özet değeri bulunacaktır.

Benzer şekilde, "SERMAYE PİYASASI KURULU" ifadesinin SHA1 algoritması ile özeti alındığında ise, "E4EF68375AD2E5CD00ECADE34B3A9C90413D0114" değeri bulunacak, boşluklar olmadan, "SERMAYEPİYASASIKURULU" ifadesinin özeti alındığında ise, "1982F9DD7AD55FAFC073AF5B93079DE4B1FAC392" değeri elde edilecektir. Görüldüğü üzere, sayfalar süren bir dosyanın özeti alınabileceği gibi birkaç karakterlik bir metinin de özeti alınabilir. Üç kelimelik bir metnin sadece boşluklarının değişmesi ile elde edilen özet tamamen farklı olmaktadır.



Şekil 47: Hash

Birçok kullanım alanı olan özet fonksiyonlarının kullanımına örnek olarak, dosya bütünlük kontrolü verilebilir. Özet fonksiyonun rasgele bir sayı üretilmesinde kullanılması da mümkündür. Mesaj doğrulama kodlarında (message-authentication-codes) ve dijital imzalarda da özet fonksiyonları kullanılmaktadır. Ayrıca, güvenli parola saklanması uygulamaları da özet fonksiyonları kullanmakta, açık metin olarak saklanan kullanıcı adı-parola çiftinin ele geçirilmesi durumunda parolaların elde edilmesini zorlaştırmaktadır.

Özet fonksiyonlarının sözde rassal (pseudo-random) olmaları gerekmekte, özetlenecek metindeki herhangi bir değişikliğin tüm özeti değiştirmesi beklenmektedir. Özet fonksiyonların birbirleri ile çakışmaması (collision) ve buna yönelik olarak 3 farklı özelliğe sahip olması gerekmektedir:

- **Öngörüntü direnci:** verilen özeti kullanarak özetlenen metnin bulunmasının zor olmalıdır.
- **İkinci Öngörüntü direnci**: verilen bir metin ve özeti kullanarak aynı özete sahip başka bir metnin bulunması zor olmalıdır.
- **Çakışma direnci**: aynı özete sahip iki farklı metinin bulunması zor olmalıdır.

Bu özelliklere sahip özet fonksiyonu, her bir özetin "dijital parmak izi" olarak kullanılabilmesini, yüksek olasılıkla birbirinden farklı olmalarını sağlar.

En bilinen özet fonksiyonları, MD5 ve SHA serisi olmakla birlikte, MD5 ve SHA1 özet fonksiyonlarının çakışmaları bulunduğu için kritik işlemlerde kullanılmaması tavsiye edilmektedir. 2022 yılı itibariyle, güncel ve yaygın olarak kullanımda olan özet fonksiyonu SHA-256 (SHA-2) ve SHA-3 fonksiyonlarıdır.

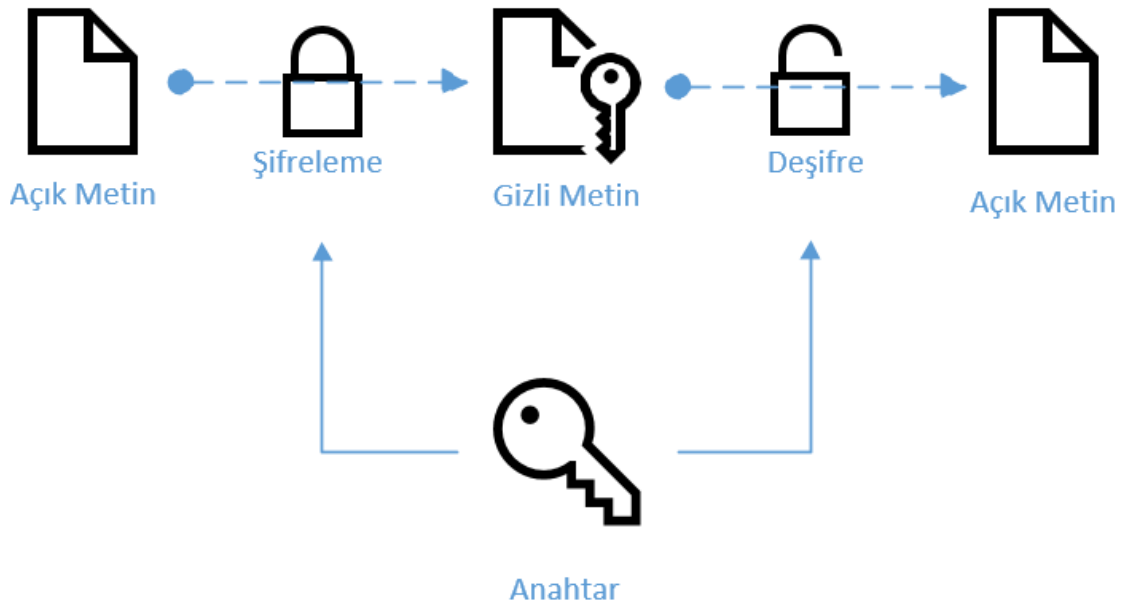
6.8.2. Simetrik Şifreleme

Anahtar kullanılan şifreleme yöntemlerinden birincisi olan simetrik şifreleme, aynı (veya yakın ya da kolayca türetilebilir) anahtar kullanılarak şifreleme ve şifre çözme (deşifre) işleminin yapılması işlemi olup, hem şifrelemede hem de şifre çözmede aynı işlemin uygulanması dolayısıyla "simetrik" olarak adlandırılmaktadırlar. Simetrik şifreleme, kullanılan anahtarın sadece taraflarca bilinmesi (gizlenmesi) gerektiği için gizli anahtar şifreleme olarak da isimlendirilmektedir.

Simetrik şifreleme kripto sisteminde, şifrelenmek istenen açık bir metin, belirli bir algoritma ve anahtar kullanılarak rassal görünümlü (psuedo-random) şifreli metin haline getirilir. Şifreli metin aynı algoritma ve anahtar kullanılarak deşifre edilerek açık metin elde edilir.

Blok (block) ve akış (stream) olarak ikiye ayrılan simetrik şifreleme algoritmaları bulunmaktadır. En bilinen simetrik blok şifreleme algoritmalarından biri olan DES'in (Data Encryption Standart) çeşitli saldırı yöntemleri ile "kırılabildiği" anlaşıldıktan sonra, eski sistemlerle uyum sağlamaya devam edecek şekilde uç-uca eklenmiş 3 adet DES şifreleme algoritması olan 3DES kullanılmaya başlanmış olup 3DES'in de kullanılmasına son verilmesi tavsiye edilmektedir. Güncel ve

yaygın olarak kullanılan simetrik şifreleme metodu ise AES olup, iletişim, arşivleme, dosya sistemi ve parola yönetim araçlarında yaygın olarak kullanılmaktadır.



Şekil 48: Simetrik Şifreleme

Bunlar dışında diğer yaygın olarak bilinen simetrik şifreleme yöntemleri Twofish, Blowfish ve Serpent şifreleme algoritmalarıdır.

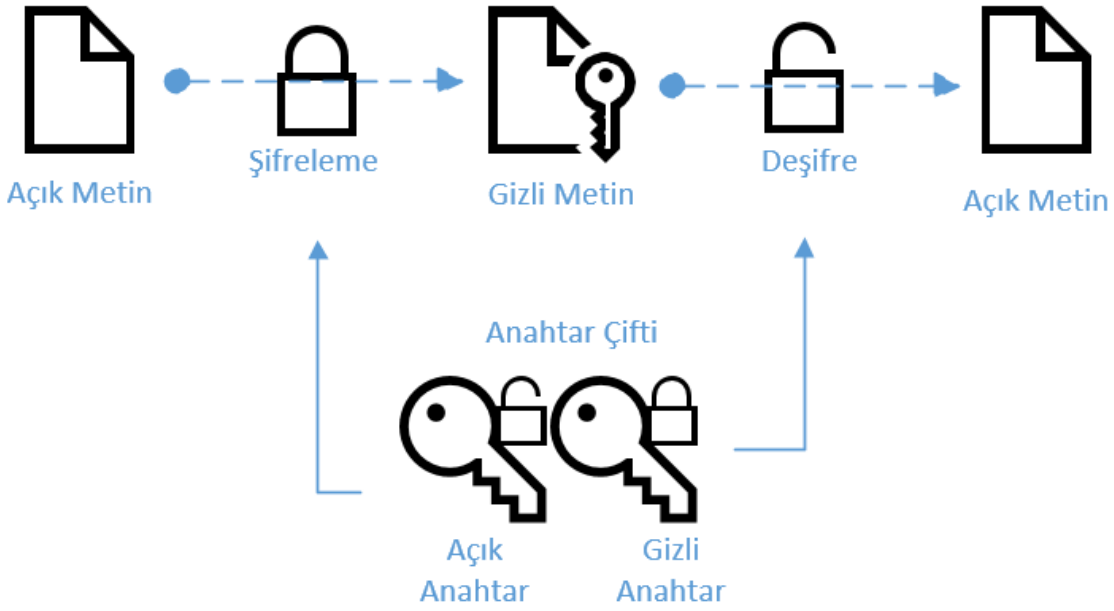
Simetrik şifrelemede kullanılan anahtar, mümkün olan tüm anahtarların denendiği kaba kuvvet saldırısı (brute-force attack) ile tespit edilebileceği gibi, diferansiyel veya lineer kriptoanaliz yöntemleri ile de tespit edilebilir. Önceden bilinen bir açık metnin kullanıldığı veya seçilen bir açık metnin kullanıldığı saldırılar da parola tespiti için kullanılmaktadır. Örneğin, önceden bilinen bir metnin tüm anahtarlar ile şifrelenmesi ile elde edilen tablolar (rainbow table) kullanılarak da anahtar elde edilebilir. Algoritmanın işleyişine yönelik olarak, geçen süre, harcanan enerji, yayılan manyetik alan gibi yan kanal (side-channel) yöntemleri de saldırı yöntemleri arasında yer almaktadır.

Simetrik şifrelemenin yapısından kaynaklı bir takım problemler de bulunmaktadır. Anahtar ile alakalı olarak, anahtarın doğru şekilde (tahmin edilemez) üretilmesi, doğru şekilde (gizlilik ve erişilebilirlik) saklanması ve doğru şekilde (sadece taraflar arasında) paylaşılması gerekmektedir. Ayrıca, yapısı itibariyle, simetrik şifreleme yapılan bir açık metnin uzunluğu yaklaşık olarak şifreli metnin uzunluğuna eşit olması da metne ilişkin entropi kaybına neden olmaktadır.

6.8.3. Asimetrik Şifreleme

Anahtar kullanılan şifreleme yöntemlerinden ikincisi olan asimetrik şifreleme, açık bir anahtar kullanılarak şifreleme ve gizli bir anahtar kullanılarak şifre çözme (deşifre) işleminin yapılması işlemi olup, şifrelemede ayrı, şifre çözmede ayrı anahtarın kullanılması dolayısıyla "asimetrik" olarak adlandırılmaktadırlar. Asimetrik şifreleme, şifrelemede kullanılan anahtarın herkesçe bilinir olması dolayısıyla açık anahtar şifreleme olarak da isimlendirilmektedir.

Asimetrik şifreleme kriptosisteminde, şifrelenmek istenen açık bir metin, belirli bir algoritma ve herkesçe bilinen anahtar (açık anahtar) kullanılarak rassal görünümlü (psuedo-random) şifreli metin haline getirilir. Şifreli metin aynı algoritma ve sadece anahtar kullanılarak deşifre edilerek açık metin elde edilir.



Şekil 49: Asimetrik Şifreleme - 1

İnternet gibi güvensiz ortamlarda, simetrik şifrelemede var olan anahtarın taraflar arasında paylaşılmasının zorluğu nedeniyle geliştirilen asimetrik şifrelemede, anahtar dağıtımı, anahtar değişimi (yenilenmesi) ve uçtan-uca bağımsız anahtar oluşturulması zorluklarını ortadan kaldırmıştır. Anahtar çiftinden açık anahtarın paylaşılması ve gizli anahtarın saklanması ile açık anahtar ile şifrelenen mesajların sadece gizli anahtar ile deşifre edilebildiği yöntem ile mesaj güvenliği sağlanmaktadır.

Benzer şekilde, dijital imzalama işlemi de herhangi bir metnin gizli anahtarla imzalanması ve açık anahtar kullanılarak imzanın doğruluğunun teyidi yapılabilmektedir. Bu yöntem ile mesajı gönderenin gizli anahtara sahip olduğunu ve mesaj içeriğinde değişiklik yapılmadığı anlaşılmaktadır.

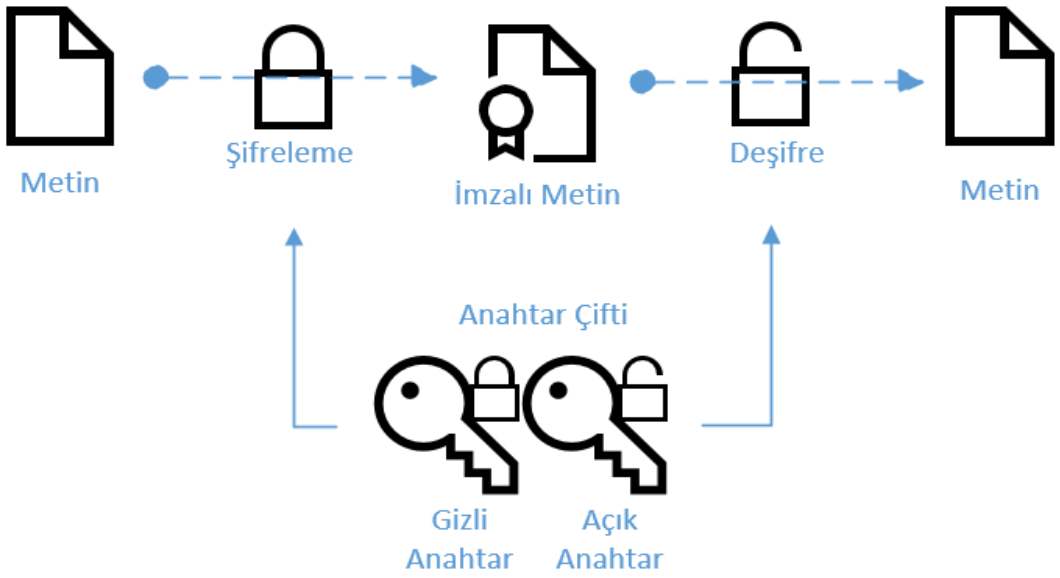
Asimetrik şifrelemede açık anahtarın dağıtımı gerekli olup, bunun için birkaç yöntem kullanılmaktadır. Sertifika yayıncıları ile gerçekleştirilen yöntemin adı Açık Anahtar Altyapısı (Public Key Infrastructure – PKI) olup, bu sistem içerisinde güvenilir 3. taraflarca üretilen sertifika zincirlerine ilişkin detaylar bir sonraki bölümde yer almaktadır.

Bir diğer anahtar paylaşım yöntemi ise, güven-ağı yöntemi olup, PGP/GPG anahtarlarının dağıtımı (örneğin pgp.mit.edu) veya mail işletme altyapısında kullanılan DKIM bu yöntem ile açık anahtar dağıtımı gerçekleştirmektedir. Tarafların birbirine doğrudan anahtar iletimi gerçekleştirmesi de mümkündür.

Güncel ve yaygın olarak kullanılan asimetrik şifreleme metodu Ron Rivest, Adi Shamir and Leonard Adleman tarafından geliştirilen RSA algoritmasıdır. RSA algoritması, geniş bir kullanım alanına sahip olmakla beraber, anahtar uzunluğunun fazla olması gibi problemler dolayısıyla, daha kısa anahtar boyutu ile benzer güvenlik sağlayan eliptik eğri kriptografisi (ECC) gibi algoritmalar geliştirilmektedir.

Ayrıca, güncel kriptografik yapıların quantum bilgisayarlar ile kolaylıkla kırılabileceği öngörüsüyle, quantum bilgisayarlar ile kolaylıkla kırılamayacak kriptografik algoritmalar da geliştirilmektedir.

Asimetrik şifreleme sadece şifreleme işlemleri için değil, anahtar değişimi ve dijital imza işlemleri için de kullanılmaktadır.



Şekil 50: Asimetrik Şifreleme - 2

Anahtar değişimi

İnternet gibi güvensiz ortamlarda, asimetrik şifreleme kullanılarak anahtar değişimi yapılması ve bu değişim sonrasında elde edilen yeni bir (asimetrik şifrelemeye göre daha hızlı olan) simetrik şifre ile işlem yapılması mümkündür. Bu kapsamda en bilinen yöntem, Diffie-Hellman Anahtar Değişimi (Diffie-Hellman Key Exchange) metodudur. Bu yöntem, TLS altyapısında kullanılan anahtar değişim metotlarından bir tanesi olup, TLS 1.3 versiyonunda sadece RSA veya önceden paylaşılmış anahtar (pre-shared-key) ile kullanılmaktadır.

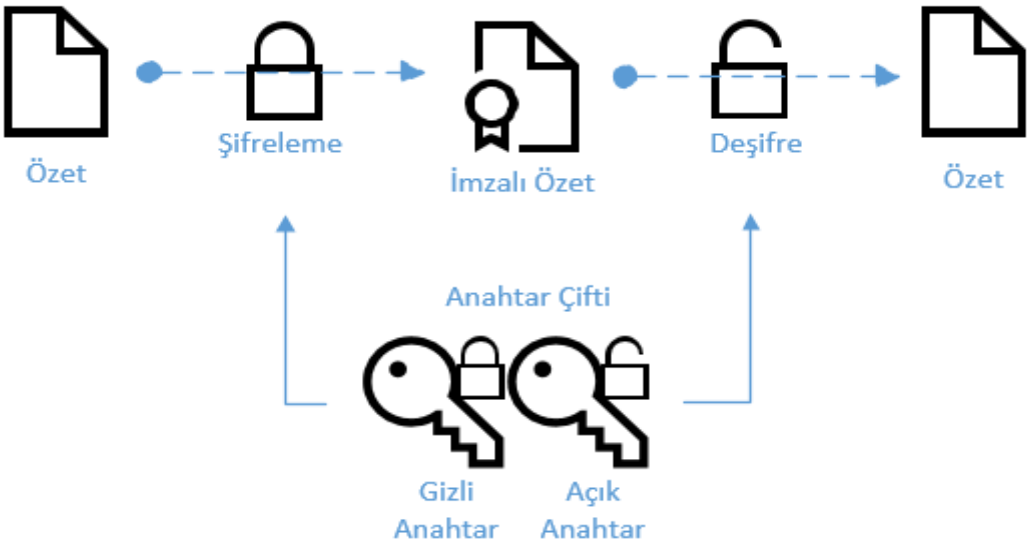
Dijital İmza

Asimetrik şifreleme yöntemi ile gizli anahtar ile şifrelenen metinin, açık anahtar ile deşifre edilmesi de mümkündür. Bu sayede, belirli bir mesajın gizli anahtar sahibince şifrelendiği anlaşılarak inkar-edilemezlik sağlanabilir. Dijital imza uygulamaları, genellikte tüm metne değil, belirli bir metne ait özetin gizli anahtar ile şifrelenmesi ve metnin özet ile beraber dağıtılması şeklinde uygulanmaktadır. E-imza ile belgelerin imzalanması işlemi de bir dijital imza uygulamasıdır.

Asimetrik şifreleme birçok sistemde kullanılmaktadır. Bunlar arasında, güvenli internet erişimi için kritik olan TLS protokolü, e-posta güvenliği sağlayaan S/MIME, PGP ve GPG, VPN gibi güvenli ağların oluşturulması sırasında kullanılan IPSec ve güvenli iletişim için SSH erişim sistemlerinde yer almaktadır. Asimetrik kriptografinin bir diğer önemli kullanım alanı ise bitcoin ve diğer kripto para sistemleridir.

6.8.4. Açık Anahtar Altyapısı

Açık anahtar altyapısı (Public Key Infrastructure - PKI), sertifika otoriteleri olarak adlandırılan üçüncü taraflarca anahtar çiftlerinin (açık-gizli) sahipliğine ilişkin kayıtların işlendiği sistemlerdir. Sertifika oluşturulması, yönetilmesi, dağıtılması, kullanılması ve iptal edilmesi süreçlerini kapsamaktadır. PKI'lar ile güvensiz internet ortamında güvenli iletişim yapılması mümkündür. PKI sayesinde bütünlük, gizlilik, kimlik doğrulama ve inkar edilemezlik sağlanabilmektedir.



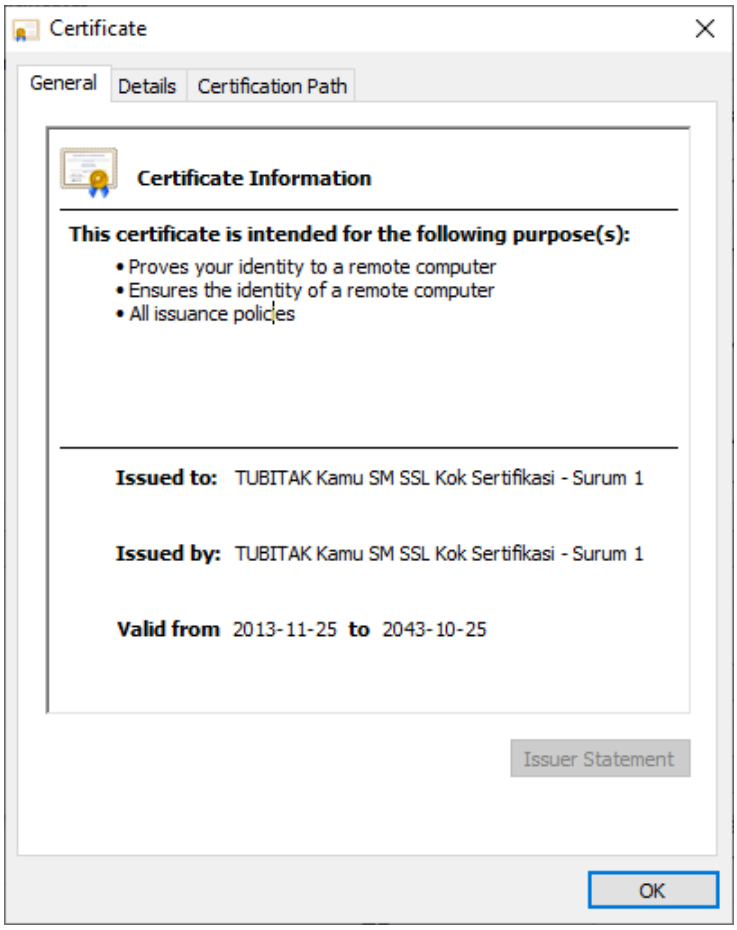
Şekil 51: Dijital İmza

PKI sisteminde, sertifikaların saklanması, üretilmesi ve imzalanması işlemlerini gerçekleştiren bir merkezi otorite (Certificate Authority – CA) ile merkezi otoritede sertifika oluşturulmasını isteyen tarafların kimliğini doğrulayan kayıt otoritesi (Registration Authority – RA) bulunmaktadır. Bunlar dışında, Sertifika sunucusu, Sertifika Deposu (Repository), Zaman sunucusu ve İmza Sunucusu da PKI altyapısının parçalarıdır. Anahtarlara ilişkin olarak ise süreç içerisinde üretim, dağıtım, saklama, kullanım, kurtarılma, sonlandırılma ve arşivlenme işlemleri yer almaktadır.

Örnek bir sertifika üretilmesi ve doğrulama aşaması aşağıdaki sıralamada yer almaktadır:

- A Şirketi, RA'ya sertifika üretilmesi isteğini iletir
- RA, A Şirketinden gerekli bilgileri talep eder, A şirketinin kimliğini doğrular
- RA, CA'ya A Şirketi için sertifika üretilmesi talebini iletir
- CA, üretilen sertifikayı A Şirketine güvenli bir şekilde iletir
- A Şirketi, sertifikasını kullanıma alır
- B kullanıcısı, A şirketinin web sitesini ziyaret edip sertifikasını talep eder
- A Şirketi B kullanıcısına sertifikasını gönderir
- B kullanıcısı, sertifikanın doğruluğu CA sertifikasını kullanarak teyit eder

PKI sertifikaları X.509 olarak isimlendirilen standarda uygun şekilde üretilmektedirler. Bu standart kapsamında sertifikaların belirli bilgileri içermesi zorunludur. Kullanılan algoritma, sertifika sağlayan ve talep edene ilişkin bilgiler, sertifika geçerlilik süresi bu bilgiler arasındadır. X.509 sertifikaları zincir olarak birbirini doğrulayan sertifikalar üretilmesini mümkün kılmakta olup, Kök otoriteye (Root CA) bağlı Alt otorite (Subordinate CA) sertifikaları tanımlanabilmektedir. Bu işlem, sertifika yönetim süreçlerini (aynı parolaların kullanılmaması, sertifika zincir iptalleri, fonksiyon ayrımları vd.) kolaylaştırmaktadır.



Şekil 52: Sertifika

PKI problemleri

Güveni merkezi bir otoriteye teslim eden PKI sistemi, tüm tarafların kullanılan yazılım ve donanım ile yönetim süreçlerine güvenmesini gerektirmektedir. Bu kapsamda, gerekli denetim ve gözetimin gerçekleştirilmesi gereklidir. PKI güven problemi dışında bir takım teknik problemlere de sahiptir. Örneğin, sertifika iptal işlemi, sertifika iptal listeleri (Certificate Revocation Lists – CRL) ile yapılmakta olup, CRL'in tüm son kullanıcıları dağıtılması her zaman mümkün olamamaktadır. Bu problemler dışında teknik altyapı, kullanılan kriptografik algoritmalar ve çakışmalar, zincir güvenliği, uygulama karmaşıklığı gibi çeşitli problemler bulunmaktadır.

6.8.5. Kriptografik Kontroller

Kriptografik sistemlere ilişkin olarak, genel kontrollere ek bir takım kontrollerin de gerçekleştirilmesi gerekmektedir. Bu kapsamda;

Kriptografik süreçler içerisinde yer alan anahtar üretim, dağıtım, saklama, kullanım, kurtarılma, sonlandırılma ve arşivlenme aşamaları yetkili kullanıcılar tarafından ve gerekli iz kayıtları oluşturularak gerçekleştirilmelidir.

Anahtar ve parolaların değiştirilebilir olması yanında, güvenli kriptografik algoritmalar ve rassal sayı üreteçleri kullanılmalıdır. Verinin önemine göre algoritma ve anahtar uzunluğu seçilmelidir.

Örnek Sorular

Soru 1: Aşağıdakilerden hangisi özet fonksiyonu değildir?

A) MD4

B) MD5

C) MD6

D) SHA-256

E) SHA-1

Cevap: C

Soru 2: Aşağıdakilerden hangisi veri yaşam döngüsünün aşamalarından biri değildir?

A) Üretim

B) Saklama

C) Taşıma

D) Değiştirme

E) İmha

Cevap: D

7. ÜÇÜNCÜ TARAFLARLA İLETİŞİM GÜVENLİĞİ

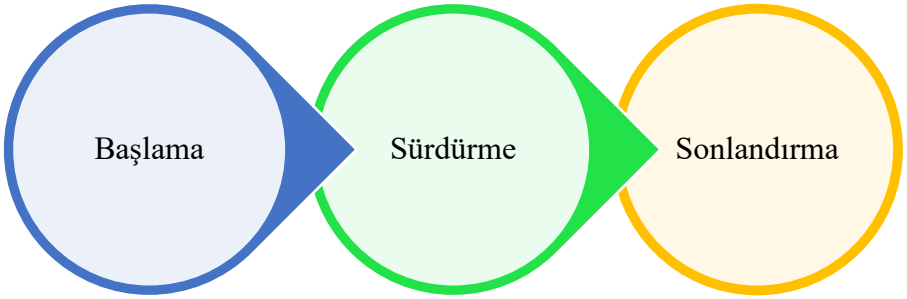
Bilgi güvenliği, verilerin erişim yetkisi olanlarla sınırlı (gizli) kalmasını, bütünlüğünün değiştirilmemesi için korunmasını ve erişmesine izin verilenler tarafından erişilebilir olmasını gerektirmektedir. Bu kapsamda, doğrudan ilişki içerisinde bulunan paydaşlara ek olarak, dolaylı olarak ilişki kurulan paydaşlara ilişkin kontrol ve denetimlerin de gerçekleştirilmesi gerekmektedir. Söz konusu taraflar, üçüncü taraf olarak ifade edilmekte ve Sermaye Piyasası Kurulu Bilgi Sistemleri Yönetimi Tebliği'nde (Tebliğ), "Kurum, Kuruluş ve Ortaklıklar ile müşteriler dışında kalan gerçek veya tüzel kişiler" şeklinde tanımlanmaktadır.

Şirketler, üçüncü taraflarla ilişkilerine ilişkin yönetim süreçlerini oluşturmalı ve üçüncü taraflarla paylaşılan verilerin uygun şekilde korunmasını sağlamalıdırlar. Tebliğ'in "Üçüncü taraflarla bilgi değişimi" başlıklı 21 nci maddesinde, üçüncü taraflara erişim hakkı verilmeden önce gerekli güvenlik gereksinimlerinin tanımlanması ve uygulanması gerektiği ve bilgi aktarımları sırasında gerçekleşebilecek kötüye kullanım veya bozulmaya karşı korunması gerektiği ifade edilmektedir.

İşlenen verilerin kişisel veri kapsamında olması durumunda kişisel verilerin saklanması, transferi, işlenmesi ve imhasına yönelik gerekli tedbirleri alınmalıdır. Bu çerçevede, varlık ve veri sınıflandırılmasının tamamlanmış olması gerekmektedir.

Üçüncü taraf ilişkileri bir yaşam döngüsü olarak değerlendirilebilir. Bu kapsamda, gerçekleştirilmesi gerekmektedir.

Üçüncü taraflarla kurulan ilişkiler, bir yaşam döngüsü olarak değerlendirilip, başlama, sürdürme ve sonlandırma aşamaları olarak incelenebilir. Bu çerçevede döngünün her bir basamağında ilgili kontrollerin tanımlanması, süreçlerin işletilmesi ve denetim ve değerlendirme işlemlerinin gerçekleştirilmesi gerekmektedir.



Şekil 53: Onboard-Ongoing-Offboard Cycle

7.1. Başlama

Üçüncü taraflarla anlaşmalar yapılmadan önce bir takım gereksinimlerin kontrol edilmesi gereklidir. Bu kapsamda veri gizliliği, erişim ve hizmet seviyeleri konularının belirlenmiş olmalıdır.

Veri gizliliği

Veri gizliliğini sağlamak adına, üçüncü taraflardan verinin işlenme, depolanma, transfer ve imha süreçlerine ilişkin bilgi alınabilir. Müşteri verilerinin şifrelenmesi, KVKK uyumu, diğer standart ve mevzuata uyum (BDDK vs.) ile veri sınıflandırmasına ve güvenliğine yönelik iç yönetmelikler bu kapsamda incelenebilecek başlıklar arasındadır.

Veri gizliliğine ilişkin bir diğer önemli konu ise veri konumudur. Tebliğ kapsamında birincil ve ikincil sistemlerin yurt içerisinde barındırılması zorunludur. Üçüncü taraf verilerinin nerede saklandığı, yedeklerin nerede tutulduğu ve üçüncü tarafların ilişkili taraflarıyla veri paylaşım anlaşmaları kontrol edilmelidir.

Fiziksel Güvenlik

Fiziksel ve çevresel güvenlik konularına ilişkin yeterli önlemlerin üçüncü taraflarca alınması gerekmektedir. Paylaşımlı ortamlarda gerekli fiziksel ve mantıksal ayrımların yapıldığından emin olunması gerekmektedir. Kamera ve diğer görüntüleme sistemleri, güvenlik görevlileri, iklimlendirme sistemleri, güç kaynakları ve yedek güç kaynakları, afet hazırlığı, yangın söndürme sistemleri fiziksel güvenlik kapsamındadır.

Siber Güvenlik

Üçüncü taraflardan siber güvenliğe yönelik süreçlere ilişkin bilgi alınabilir. Bu kapsamda iç ve dış taraflarca gerçekleştirilen sızma testleri, mavi ve kırmızı takım çalışmaları talep edilebileceği gibi, olay yönetimi süreçleri ile aktif sertifikasyonlar talep edilebilir.

Erişim/Bağlantı

Şirket ile üçüncü taraflar arasında gerçekleştirilecek bağlantıların ne şekilde gerçekleşeceği tespit edilerek, internet gibi güvensiz ağlarda şifrelemelerin sağlandığından, yetkisiz erişimlerin engellendiğinden ve ilgili iz kayıt mekanizmasının bulunduğundan emin olunmalıdır. Uzaktan erişim yapılacaksa, buna ilişkin güvenlik önlemleri alınmalıdır.

Hizmet Seviyesi Anlaşmaları (Service Level Aggreements – SLA)

Hizmet seviyesi anlaşmaları, üçüncü tarafın işlemlerine ilişkin hedeflerin belirlendiği sözleşmelerdir. Bu kapsamda hizmetlerde aksamaların ne kadar süre içerisinde giderileceği veya ne kadar sürede taleplere cevap verildiği gibi gereksinimler takip edilmektedir. SLA'lar yasal yaptırımları da içerebilmektedir. SLA'lar içerisinde sistemlerde gerçekleşen kesintilerin ne kadar sürede çözüleceğine ilişkin hedefler (Recovery Time Objective – RTO) veya veriye ilişkin kayıpların ne kadar olabileceğine ilişkin hedefler (Recovery Point Objective RPO) bilgileri de yer alabilmektedir.

Diğer

Üçüncü tarafların hukuki durumu değerlendirme kapsamına alınmalı, üçüncü tarafın kendi paydaşları ve üçüncü taraflarıyla olan ilişkileri değerlendirilmelidir. Ayrıca, şirket itibarı ve personel riski gibi konulara ilişkin değerlendirmeler yapılmalıdır.

7.2. Sürdürme

Üçüncü taraflarla düzenli olarak sözleşmeler kapsamında kararlaştırılan gereklerin yerine getirildiğine ilişkin kontroller tesis edilmeli ve buna yönelik gözlem ve denetimler gerçekleştirilmelidir.

Değişiklik Yönetimi

Üçüncü taraflar tarafınca gerçekleştirilen değişikliklerin izlenmesi gerekmektedir. Bu kapsamda, üçüncü taraflarda gerçekleşen personel değişikliklerin bildirimine ilişkin kontroller tesis edilmelidir. Özellikle Şirket ile doğrudan ilişki içerisinde bulunan personele ilişkin değişikler ivedilikle bildirilmeli, sonlandırma sürecinde yer alan işlemler ilgili personel için gerçekleştirilmelidir.

Üçüncü tarafların tüzel kişiliğine ilişkin, sözleşmeye etkileme ihtimali bulunan değişiklikler de kontrol edilmeli, yönetici ve sahiplik değişiklikleri takip edilmelidir.

Üçüncü tarafların altyapılarında ve sistemlerinde değişiklik gerçekleştiğinde, bu değişikliğin sözleşme kapsamında alınan hizmet ve ürünleri nasıl etkileyeceği de değerlendirilmelidir.

Erişim Yönetimi

Üçüncü taraflarca, şirketin hangi kaynaklarına ve verilerine erişim olduğu düzenli takip edilmeli ve erişimlere ilişkin iz kayıtları ve uygun kontroller gerçekleştirilmelidir. Bu kapsamda, bilmesi gereken ilkesi işletilmeli, gerektiğinden fazla erişim yetkisi verilmemelidir.

Varlık Yönetimi

Üçüncü taraflar ile olan ilişkiler, varlık yönetimi süreçlerine dahil edilmeli, varlıkların sınıflandırılması ve sahiplik bilgilerine ilişkin uygun kontroller gerçekleştirilmelidir.

Açıklık ve iyileştirme yönetimi

Üçüncü taraflar bünyesinde gerçekleşen açıklıkların ivedilikle bildirilmesi temin edilmeli, iyileştirme ve yama yönetiminin uygun şekilde yapıldığına ilişkin kontroller gerçekleştirilmelidir.

Düzenli Raporlar ve Testler

Üçüncü tarafların güncel durumuna ilişkin düzenli olarak raporlar talep edilebilir. Bu kapsamda, sözleşme kapsamında tanımlanan gerekler test edilebileceği gibi tarafsız bir denetim raporu veya sızma testi raporu ile değerlendirmeler gerçekleştirilebilir.

Hizmet Seviyesi Takibi

Üçüncü taraflar ile gerçekleştirilen sözleşme kapsamındaki hizmet seviyelerinin sağlanıp sağlanmadığına ilişkin kontroller yapılmalıdır.

7.3. Sonlandırma

Üçüncü taraflarla gerçekleştirilen sözleşmelerin ve ilişkinin sonlandırılması durumunda, sözleşme ve bilgi güvenliği kapsamında kontroller tesis edilmeli ve buna yönelik gözlem ve denetimler gerçekleştirilmelidir. Bu kapsamda, fiziksel ve sistem erişim yetkilerinin kaldırılması ile verilerin güvenliğinin sağlanması gerekmektedir.

Erişim Yetkilerinin Kaldırılması

Üçüncü taraflara verilen erişim yetkilerinin, sözleşme sonlandıktan sonra kaldırılması gerekmektedir. Bu kapsamda, kullanıcıların askıya alınması, uzak erişim yetkilerinin kısıtlanması, eğer sağlanan başka erişim yöntemleri varsa (sertifikalar, ssh anahtarları, vd.) kısıtlamaya gidilmesi gerekmektedir. Fiziksel erişim araçlarının (kart, kimlik, token, anahtar vd.) da teslim alınması gerekmektedir. İlgili taraflara sözleşmenin sonlandığına ilişkin bilgilendirmeler (Örneğin; güvenlik görevlileri) de yapılmalıdır.

Verilerin Gizliliği

Üçüncü taraflar ile ilişki sonlandırıldığında, sürecin başlama ve sürdürme aşamalarında tanımlanan ve işlenen verilerin güvenliği sağlanmalıdır. Bu kapsamda, uygun silme işlemleri yapılmalı, gerekmesi durumunda veri temizliği için, hemen silme, belirli bir süre sonra, arşivleme, anonimleştirme vb. işlemlerin uygun olanları gerçekleştirilmelidir. Fiziksel dokümanların da bu sürece dahil edilmesi gereklidir. Erişimlere ilişkin iz kayıtları takip edilmeli, iz kayıtlarının ne kadar süre takip edileceği ve saklanacağına ilişkin belirlenen politika kapsamında işlemler gerçekleştirilmelidir.

Örnek Sorular

Soru 1: Aşağıdakilerden hangisi, üçüncü taraflara verilen erişim yetkilerinin sonlandırılması durumunda, üçüncü taraflarca yapılması gereken bir işlem değildir?

A) Kimlik kartlarının teslim edilmesi

B) SSH anahtarlarının teslim edilmesi

C) Erişim Kartlarının teslim edilmesi

D) Fiziksel anahtarların teslim edilmesi

E) Token cihazlarının teslim edilmesi

Cevap: B

Soru 2: Aşağıdakilerden hangisi, Üçüncü taraflarla ilişki yaşam döngüsünde, Başlama aşamasına ait bir süreç değildir?

A) Hizmet Seviyesi Anlaşmaları

B) Veri Gizliliği

C) Fiziksel Güvenlik

D) Erişim Güvenliği

E) Düzenli Testler

Cevap: E

KAYNAKÇA

Albayrak, O. (2021, April 14). Surface, Deep ve Dark Web Nedir? BGA Cyber Security - Siber Güvenlik Çözümleri. Retrieved December 17, 2022, from https://www.bgasecurity.com/2019/08/surface-deep-ve-dark-web-nedir/

Anadolu Üniversitesi. (2018). *Ağ yönetimi ve bilgi güvenliği.* Anadolu Üniversitesi. https://www.aof.tc/ag-yonetimi-ve-bilgi-guvenligi-ybs302u-ders-kitabi.html

Aydın, Ç. T. (2020, 6 Haziran). *Siber Tehdit Aktörleri.* Cahit Cengizhan. 27 Ocak 2022 tarihinde https://cahitcengizhan.com/siber-tehdit-aktorleri-2/ adresinden erişildi.

Beasley, J. S., & Nilkaew, P. (2021). *Networking Essentials: A CompTIA Network+ N10-008 Textbook* (6th ed.). Pearson IT Certification. https://learning.oreilly.com

Canadian Centre for Cyber Security. (2021, Şubat). *Baseline Security Requirements for Network Security Zones (version 2.0) - ITSP.80.022*. https://cyber.gc.ca/en/guidance/baseline-security-requirements-network-security-zones-version-20-itsp80022

Cascarino, R. E. (2012). *Auditor's Guide to IT Auditing (2nd ed.)*. Wiley. https://learning.oreilly.com

Cisco Networking Academy. (2022). *Networking Essentials Companion Guide* (1st ed.). Cisco Press. https://learning.oreilly.com

Computer Network. (2022). In *Wikipedia*. Retrieved December 16, 2022, from https://en.wikipedia.org/wiki/Computer_network

Davies, G. (2019). *Networking Fundamentals: Develop the networking skills required to pass the Microsoft MTA Networking Fundamentals Exam 98-366*. Packt Publishing. https://learning.oreilly.com

DDO. (2020). *Bilgi ve İletişim Güvenliği Rehberi (1st ed.).* Cumhurbaşkanlığı Dijital Dönüşüm Ofisi.

Demchenko, A. (2022, 20 Kasım). Surface Web vs Deep Web vs Dark Web - Key Differences. DataOx. Retrieved December 17, 2022, from https://data-ox.com/web-dark-web-and-deep-web/

Diogenes, Y., & Ozkaya, E. (2019). *Cybersecurity – Attack and Defense Strategies (2nd ed.).* Packt Publishing. https://learning.oreilly.com

Doshi, H. (2020). *CISA – Certified Information Systems Auditor Study Guide.* Packt Publishing. https://learning.oreilly.com

Doshi, H. (2021). *Certified information security manager exam prep guide.* Packt Publishing. https://learning.oreilly.com

Drozhzhin, A. (2020, 25 Eylül). *Kimlik tanımlama, kimlik doğrulama ve yetkilendirmenin farkı nedir?* Kaspersky Daily. https://www.kaspersky.com.tr/blog/identification-authentication-authorization-difference/8851/

EKC Grup. (t.y). *Hassas Klima.* Hassas Klima. 20 Ocak 2022 tarihinde https://hassasklima.com/bilgi-bankasi/tag/sistem%20odas%C4%B1%20nem%20oran%C4%B1%20ne%20olmal%C4%B1.html adresinden erişildi.

Gazi Üniversitesi Bilişim Enstitüsü. (2016). IPv4 ile IPv6 Protokollerinin Karşılaştırılması. DocPlayer. Retrieved January 4, 2023, from https://docplayer.biz.tr/1628904-Ipv4-ile-ipv6-protokollerinin-karsilastirilmasi-ve-kurumsal-veri-guvenliginin-ipv6-ile-saglanmasi.html

Georgescu, E. (2021, 12 Aralık). *IT Asset Management – Everything You Need to Know About ITAM.* 7 Şubat 2022 tarihinde https://heimdalsecurity.com/blog/it-asset-management-itam/ adresinden erişildi.

Gregory, P. H. (2019). *CISA Certified Information Systems Auditor All-in-One Exam Guide, Fourth Edition (4th ed.).* McGraw-Hill Education. https://learning.oreilly.com

Haber, M. J. (2020). *Privileged Attack Vectors (2nd ed.).* Apress. https://learning.oreilly.com

Haber, M. J., & Hibbert, B. (2018). *Asset Attack Vectors: Building Effective Vulnerability Management Strategies to Protect Organizations (1st ed.).* Apress. https://learning.oreilly.com

IATAM. (t.y.). *What is IT Asset Management (ITAM)?* 7 Şubat 2022 tarihinde https://iaitam.org/what-is-it-asset-management/ adresinden erişildi.

Internet - Glossary | CSRC. (n.d.). In NIST Computer Security Research Center. Retrieved December 17, 2022, from https://csrc.nist.gov/glossary/term/internet

ISACA. (2018). *ISACA terimler sözlüğü*. 24 Kasım 2021 tarihinde https://www.isaca.org/resources/glossary adresinden erişildi.

ISACA. (2019). *CISA Review Manual, 27th Edition.* ISACA.

ISO. (t.y.). *Information technology — IT asset management — Part 1: IT asset management systems — Requirements*. 7 Şubat 2022 tarihinde https://www.iso.org/obp/ui/#iso:std:iso-iec:19770:-1:en adresinden erişildi.

ISO. (t.y.). *Information technology — Security techniques — Information security management systems — Overview and vocabulary*. 8 Şubat 2022 tarihinde https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en adresinden erişildi.

Kim, D., & Solomon, M. G. (2021). *Fundamentals of information systems security (4th ed.)*. Jones & Bartlett Learning. https://learning.oreilly.com/

Kimlik doğrulama. (2022, 8 Ocak). Wikipedia. https://tr.wikipedia.org/wiki/Kimlik_do%C4%9Frulama

Meyers, M., & Jernigan, S. (2022). CompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008). McGraw-Hill. https://learning.oreilly.com

Milli Savunma Bakanlığı. (2010, 4 Haziran*). Savunma Sanayii Güvenliği Yönetmeliği.* Resmi Gazete Sayı:27601. 16 Ocak 2022 tarihinde https://www.resmigazete.gov.tr/eskiler/2010/06/20100604-2.htm adresinden erişildi.

Network Topology. (2022). In Wikipedia. Retrieved December 21, 2022, from https://en.wikipedia.org/wiki/Network_topology

NIST. (1995, Ekim). *Special Publication 800–12: An Introduction To Computer Security: The NIST Handbook.* NIST CSRC. 11 Ocak 2022 tarihinde https://csrc.nist.rip/publications/nistpubs/800-12/800-12-html/index.html adresinden erişildi.

NIST. (2017, Haziran). *NIST Special Publication 800–12 Rev.1 An Introduction to Information Security.* https://doi.org/10.6028/NIST.SP.800-12r1

NIST. (2020a, Ağustos). *NIST Special Publication 800–207 Zero Trust Architecture.* https://doi.org/10.6028/NIST.SP.800-207

NIST. (2020b, Ekim). *SP 800–53B control baselines for information systems and organizations.* https://doi.org/10.6028/NIST.SP.800-53B

NIST. (2020c, Aralık). *SP 800–53 Rev. 5 security and privacy controls for information systems and organizations*. https://doi.org/10.6028/NIST.SP.800-53r5

Şeker, E. (2019, 17 Temmuz). *Siber Ölüm Zinciri'ni Anlamak.* BGA Security. 28 Ocak 2022 tarihinde https://www.bgasecurity.com/2019/06/siber-olum-zincirini-anlamak-bolum-6/ adresinden erişildi.

Solomon, M. G., & Kim, D. (2021). Fundamentals of Communications and Networking (3rd ed.). Jones & Bartlett Learning. https://learning.oreilly.com

SPK. (2018, Ocak). *Bilgi sistemleri yönetimi tebliği (VII-128.9).* https://mevzuat.spk.gov.tr

Stewart, M. J., & Kinsey, D. (2021). *Network Security, Firewalls, and VPNs (3rd ed.)*. Jones & Bartlett Learning. https://learning.oreilly.com

Sosinsky, B. (2009). Networking Bible (1st ed.). Wiley. https://learning.oreilly.com

TSE. (2013, Aralık). *TS ISO/IEC 27001*. Türk Standartları Enstitüsü.

Uzay Yangın Sis. ve Müh. (t.y.). *Gazlı Yangın Söndürme Sistemleri Nelerdir?* Uzay Yangın. 21 Ocak 2022 tarihinde https://www.uzayyangin.com/gazli-yangin-sondurme-sistemleri-nelerdir.html adresinden erişildi.

Wi-Fi Alliance. (2023). In Wikipedia. Retrieved January 8, 2023, from https://en.wikipedia.org/wiki/Wi-Fi_Alliance