# BİLGİSAYAR AĞ GÜVENLİĞİ

## 1.MODERN AĞ GÜVENLİĞİ TEHDİTLERİ

Ağ güvenliği, bilgisayar ağlarının vazgeçilmez bir parçasıdır. Ağ güvenliği veriyi güvenli hale getirme ve saldırıları azaltmak için protokoller, teknolojiler, cihazlar, araçlar ve teknikler kullanır. Ağ güvenlik çözümleri 1960'lı yıllarda ortaya çıkmasına başlamasına rağmen 2000'li yılların başına kadar derli toplu çözümler piyasaya çıkmamıştır.

Ağ güvenliği bilgisayar korsanları yüzünden gelişmek zorunda kalmıştır. Nasıl ki doktorlar mevcut hastalıkları tedavi ederken yeni bir hastalık ortaya çıkmasın diye yöntemler ve ilaçlar geliştirmek zorunda kalırlarsa, ağ güvenliği uzmanları da muhtemel atakları minimize etmek için çalışırlar. İş sürekliliği de bir başka gelişme sebebidir.

Ağ güvenliği konusunda çalışan profesyonelleri bir araya getirmek için Ağ Güvenlik Organizasyonları kurulmuştur. Bu kuruluşlar standartlar oluştururlar, birlikteliği sağlarlar ve ağ güvenlik uzmanlarını birlikte çalışmaya zorlarlar. Böylece yeni uzmanların güvenlik tehditlerinden haberdar olmaları sağlanır.

Ağ güvenliğinin karmaşık yapısı tüm alt alanları kapsamayı oldukça zorlaştırır. Farklı güvenlik kuruluşları kurularak alt alanların parçalanarak kolay yönetilmesini sağlanmıştır. Ayrıca bu bölümler daha özellikli konulara ağ güvenliği uzmanlarının odaklanmasını sağlamıştır.

Devletler ve şirketler tarafından ağ güvenlik politikaları oluşturularak çalışanların günlük takip etmeleri için çerçeve oluşturulması sağlanmıştır. Ağ güvenlik uzmanları yönetim seviyesinde politika oluşturmak ve takip etmekten sorumludurlar. Bu politikalar ağ güvenlikçilerine rehberlik ederler.

Ağ güvenliği, çeşitli alanlardan oluşur. Ağ atakları sınıflandırılarak kolay öğrenilmeleri ve adreslenmeleri sağlanır. Virüsler, solucanlar ve Truva atları network ataklarının özel tipleridir. Daha genel olarak network atakları keşif (reconnaissance), erişim (Access) ve hizmet dışı bırakma (denial of service) olarak sınıflandırılır.

Atakları azaltma ağ güvenliği uzmanları için bir iş bir meslek dalıdır. Bu bölümde ağ güvenliğinin teorisi üzerinde durulacaktır. Teorinin öğrenilmesi derinlemesine bilgi alma ve uygulama yapabilmek için şarttır. Devam eden bölümlerde ağ güvenliği saldırılarını azaltma konularına giriş yapılmaktadır.

### 1.1.GÜVENLİ BİR AĞIN TEMEL PRENSİPLERİ

#### 1.1.1.Ağ Güvenliğinin Tarihçesi

**1.1.1.1**

Temmuz 2001'de web serverlara yapılan Code Red solucanı atağından 350 binden fazla host virüslendi. Solucan sadece enfekte sunuculara erişimi engellemekle kalmadı onları çok yavaş ve kullanılamaz hale getirdi. Code Red solucanı milyonlarca kullanıcıyı hizmet dışı (Dos) bıraktı.

Ağ güvenliği uzmanları olaydan sorumlu olarak bu Code Red bulaşmış sunucularla ilgili politika geliştirmiş ve uygulamış olsalardı, güvenlik yamaları çok kısa sürede uygulanmış olurdu. Code Red yayılmadan durdurulmuş ve ağ güvenliği tarihinde dip not olarak kalırdı.

**1.1.1.2**

"Zorunluluk buluşun anasıdır." Bu deyiş, ağ güvenliği için tam olarak geçerlidir. İnternetin ilk günlerinde, ticari işler ihmal edilebilir derecede azdı. Kullanıcıların büyük çoğunluğu araştırma ve geliştirme uzmanlarıydı. İlk kullanıcıların nadiren de olsa diğer kullanıcılara zarar verecek faaliyetlerde bulunabilirdi, çünkü İnternet güvenli bir ortam değildi.

İlk virüsler yayınlanmaya başladığı ve ilk DoS atakları olmaya başladığı zaman, ağ profesyonellerinin dünyası değişmeye başladı. Kullanıcıların ihtiyaçlarını karşılamak için, ağ uzmanları ağlarını güvenli hale getirmek için teknikler öğrendi. Birçok ağ uzmanı için birincil odak, tasarım, kurulum ve genişlemeden ziyade mevcut ağların güvenliği olmaya başladı.
Bugün, İnternet 1960'lı yıllardaki başlangıcına kıyasla çok farklı bir ağdır. Bir ağ güvenliği uzmanı ağ güvenlik araçları, süreçleri, teknikleri, protokolleri ve teknolojiler konusunda çok bilgili olması gerekir.
Ağ güvenliği tehdit önleme araçlarının sayısı arttıkça, bu konuda bilinmesi gereken bilgi miktarı azalmıştır. Bazı tehditlerin ortaya çıkış tarihleri şöyledir:

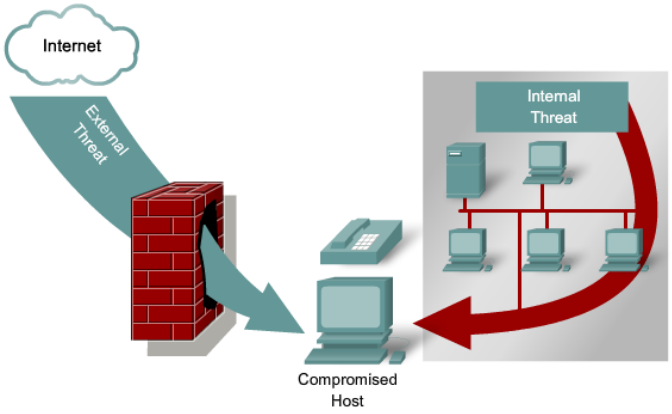
- 1978'de ilk Spam ArpaNet üzerinden gönderildi.
- 1988'de Morris İnternet solucanı yayınlandı
- 1999'da Melissa e-mail virüsü
- 2000'de Mafiaboy DoS atağı, Love Bug solucanı, L0phtCrack şifre kırıcı yayınlandı
- 2001'de Code Red DoS atağı
- 2004'de botnet saldırısı (Amerikan Askeri Sistemlerine)
- 2007'de Storm botnet ve kredi kartı bilgilerinin dağıtımı
- 2008'de veri çalma
- 2011'de Sony Play Station ağı haklendi.

**1.1.1.3**

Ağ güvenliği günlük işlerin bir parçası olmaya başladığından beri, güvenlik için özel fonksiyonlara sahip cihazların üretimi başlamıştır.
İlk güvenlik araçlarından biri saldırı tespit sistemleridir (intrusion detection system-IDS). SRI, 1984'de ilk IDS'i piyasaya sürdü. IDS gerçek zamanlı olarak saldırı tespit etmeye yarar. Bu araç ağ güvenlik uzmanının çok daha hızlı biçimde atakları azaltma işini yapmasına imkan sağlar. 1990'ların sonunda IDS'ler yerini saldırı önleme sistemlerine (intrusion prevention system-IPS ) bırakmaya başladı. IPS cihazları kötü niyetli faaliyeti algılanmasını sağlar ve otomatik olarak gerçek zamanlı saldırıyı engelleme yeteneğine sahiptir.
IDS ve IPS cihazlarına ek olarak, ağa önceden belirlenmiş kurallar çerçevesinde istenmeyen trafik girişini engellemek için firewall cihazları geliştirildi. 1988'de DEC (Digital Equipment Corporation) paket filtreleme modunda çalışan ilk firewall'u üretti. İlk firewall cihazları belirli kurallara göre paketleri geçiren ya da durduran cihazlardı. 1989'da AT&T firması ilk stateful firewall'u üretti. Paket filtre modunda çalışan firewall'a benzer biçimde stateful olanı da trafiğe izin verir veya yasaklar. Buna ek olarak kurulmuş olan bağlantıyı izleyerek ters yön trafiğine de izin verir ve diğer güvenlik ilkelerinin uygulanmasını da hızlı biçimde sağlar.
İlk firewalllar router gibi mevcut cihazların üzerine yazılımla özellik eklenerek oluşturulurdu. Zamanla birkaç firma tek başına çalışan firewall cihazları ürettiler. Cisco Adaptive Security Appliance (ASA) ismini verdiği paket filtre modunda cihazı üretti. Sonraları firmalar birkaç işi bir arada yapan cihazlar üretti. Örneğin Cisco Integrated Services Router (ISR) adlı stateful cihazı üretti.
Teknolojik gelişmelere bağlı olarak bulut üzerinde çalışan güvenlik cihazları da üretildi. Cisco Security Intelligence Operations (SIO) ürünü ile bulut tabanlı servis veren, küresel tehdit bilgilerini toplayabilen, reputation (itibar) bilgileri tutabilen ve analiz yapabilen bir ürün geliştirdi.

**1.1.1.4**

Ağa dışarıdan gelen saldırılara ek olarak, ağ güvenlik uzmanları iç ağdan gelen saldırılarla da ilgilenmek zorunda kalırlar. İç tehditler kasten veya kazaen olsalar bile dış tehditlerden daha çok zarar verirler. Çünkü iç ağ kullanıcıları kaynaklara doğrudan erişebilirler.
İç ağdan başlatılan tehdit için yaygın bir senaryo mutsuz çalışan senaryosudur. Bazı teknik becerilere sahip bir çalışan zararlı olabilir. İç tehditlerin sebebi LAN teknolojileri ve protokolleridir. Bu tehditler iki kategoriye ayrılır: Spoofing (kandırmaca) ve denial of service DoS.
Spoofing atakları ağdaki bir cihazın başka bir cihaz gibi davranarak verilere zarar vermesi şeklinde uygulanır. Spoofing ataklarının çok türü vardır. Örneğin MAC adres spoofing ile bir bilgisayar başka bilgisayarların MAC adresine sahip gibi davranır.
DoS atakları bir bilgisayarın kaynaklarını tüketerek elverişsiz hale getirmedir. Atak sahipleri çeşitli DoS yöntemleri kullanırlar.
Ağ güvenlik uzmanının bu yöntemleri bilip tedbirlerini alması LAN güvenliği açısından çok önemlidir.




| Year | 1998 | 2000 | 2003 | 2006 |
|---|---|---|---|---|
| Security Technology | Mitigating MAC Address Spoofing Attacks<br><br>Mitigating MAC Address Table Overflow Attacks<br><br>Mitigating LAN Storm | Mitigating Root Bridge Spoofing<br><br>Mitigating VLAN Attacks | Mitigating ARP Spoofing Attacks | Mitigating attacks on Layer 2 protocols with IEEE 802.1AE (MACsec) |

**1.1.1.5**

Network güvenliği istenmeyen trafiği engellemeye ilavaten veriyi de korunaklı halde tutmalıdır. Veriyi gizleme yani kriptografi modern ağlarda kullanılan bir yöntemdir. Günümüzde tüm network haberleşme türleri veriyi istenmeyen kullanıcılardan gizleyecek teknolojilerle ilişkili protokollere sahiptir. Kablosuz ağ verisi çeşitli kriptoloji uygulamaları ile gizlenir. IP telefon konuşması iki kullanıcı arasında kriptolanabilir.
Kriptografi veri gizliliğini sağlayabilmek için üç bileşen kullanır: confidentiality (mahremiyet), integrity (doğruluk-bütünlük), availability (geçerlilik). Bilgi güvenliği, bilgiyi ve bilgi sistemlerinin yetkisiz erişimi, kullanımı, ifşa etme, bozma, değiştirme veya yok etme konularıyla ilgilenir. Kriptolama açık veriyi (plaintext data) gizleyerek mahremiyeti korur. Veri bütünlüğü-doğruluğu hashing mekanizmasıyla verinin korunmasını sağlar. Geçerlilik veriye erişimi koruma ve yedekleme sistemleriyle muhafaza eder.

### 1.1.2.Ağ Güvenliğinin Aktörleri

**1.1.2.1**

Hacker kelimesi çeşitli anlamlara sahiptir. Çoğu kişiye göre hacker internet üzerindeki cihazlara yetkisiz erişim yapmaya çalışan internet programcısıdır. Kullanıcıların erişimlerini yavaşlatırlar veya engellerler veya sunucular üzerindeki verileri bozarlar. Bazılarına göre hacker çok yönlü kabiliyetleri olan ve atak düzenlemeyen programcılardır. İyi veya kötü hacking ağ güvenliğinin itici bir gücüdür.
İş dünyası açısından bakıldığında, kötü niyetli hackerların etkilerini en aza indirmek önemlidir. Ağ yavaş veya tepkisiz olduğunda işletmelerin verimliliği düşer. İşletme karı veri kaybı ve veri bozulmasından etkilenir.
Bir ağ güvenliği uzmanı eğitim ve çalıştaylara katılarak, güvenlik organizasyonlarına dahil olarak, tehditlere ilişkin güvenlik web sitelerini takip ederek hackerlardan bir adım önde olur. Ağ güvenliği uzmanları aynı zamanda güvenlik araçlarına, protokollere, tekniklere ve teknolojilere erişebilmelidir. Ağ güvenliği uzmanları kolluk kuvvetlerine benzer özelliklere sahip olmalıdır. Her zaman kötü niyetli faaliyetlerin farkında olması en aza indirmek veya bu faaliyetlerle ilişkili tehditleri ortadan kaldırmak için beceri ve araçlara sahip olmalıdır.

**1.1.2.2**

Hacking ilk olarak 1960'larda çeşitli ses frekanslarını kullanarak telefon sistemlerini bedava kullanmayla başladı. Beleşçilik AT&T telefon sistemleri için otomatik anahtarlarını tanıttığında başladı. AT&T telefon anahtarları çağrı sonlandırma ve çağrı arama gibi farklı işlevleri göstermek için çeşitli ses tonları veya tonlu arama kullanır. Birkaç AT&T müşterisi ıslık gibi sesleri kullanarak santral ses tonlarını taklit edip, bedava uzun mesafe arama yaptılar.
Haberleşme sistemlerinin gelişmesine paralel olarak hacking yöntemleri de gelişti. 1980'lerde modemlerin kullanılmaya başlamasıyla wardialing tekniği ortaya çıktı. Wardialing, PBX telefon santrallerine modem tarama yöntemiyle saldırıdır. Wardialing programları yerel ağdaki faks makineleri, santraller, bilgisayar modemlerine bağlı telefon numaralarını otomatik olarak tarar. Bir numara bulunursa şifre kırma programları kullanılıp erişim kurmaya çalışılır.
Wardriving 1990'larda başlayan ve bugün hala popüler olan bir yöntem. Wardriving ile kullanıcılar, kablosuz erişim noktaları aracılığıyla ağlara yetkisiz erişim elde eder. Bu işlem kablosuz özellikli taşınabilir bilgisayar ya da PDA kullanılarak gerçekleştirilir. Gerek kimlik doğrulaması için gerekse erişim noktası şifreleme düzenini kırmak için parola-kırma yazılımları vardır.
Diğer saldırı yöntmeleri 1960'lardan itibaren ortaya çıkmaya başlamıştır. Nmap veya SATAN gibi network tarama araçları, Back Orifice gibi uzak erişim yönetim kırma araçları kullanıldı. Ağ güvenlik uzmanları bu araçları bilmek zorundadır.

**1.1.2.3**

Her gün trilyonlarca dolar işlem internet üzerinden yapılıyor ve milyonlarca insan geçimini internet ticareti üzerinden sağlıyor. Bu nedenle ceza yasaları bireysel ve kurumsal varlıkları koruması gerekir. Bu yasalarla yüz yüze kalan sayısız birey vardır.
İlk e-posta virüsü olan Melissa virüsü, Aberdeen David Smith tarafından New Jersey'de yazılmıştır. Bu virüs Internet posta sunucularının belleklerinin dolarak taşmasına yol açar. David Smith bu virüs yüzünden 20 ay hapis ve 5,000 ABD Doları para cezasına mahkum edildi.
Robert Morris 99 satır kod ile ilk internet solucanını yazdı. Morris Worm yayıldığında, internet sistemlerini % 10 durma noktasına getirdi. Robert Morris üç yıl toplum hizmeti cezası ve 10 bin ABD Doları para cezası aldı.
En azılı İnternet korsanlarından biri olan Kevin Mitnick, 1990'ların başında kredi kartı hesaplarını elde ettiği için hapsedildi.
Atak ister spam ile ister virüsle ister DoS ile olsun hesap ele geçirme amacıyla yapılıyorsa cezası büyük olmaktadır.

**1.1.2.4**

1990'larda hackerların artması ve hacker araçlarının artması üzerine 1990'ların sonunda ağ güvenlik çözümleri hızla gelişmeye başladı. Pek çok kurum ağında güvenlik tedbirleri aldı. Bunlarla birlikte yeni iş fırsatları oluştu.

Network güvenlik uzmanları kurumların veri bütünlüğünü, mahremiyetini ve emniyetini sağlamaktan sorumludurlar. Firewall kurma, IPS konfigüre etme onların sorumluluğundadır. Kimliklendirme politikası hazırlama da bir başka görevdir.

### 1.1.3.Ağ Güvenliği Kuruluşları

**1.1.3.1**

Network güvenlik uzmanları diğer meslektaşlarına göre daha fazla iletişim halinde olmaları gerekir. İletişim yerel, ulusal veya uluslararası teknoloji kuruluşlarınca düzenlenecek çalıştaylar ve konferanslarla sağlanabilir.

Üç tane iyi organize olmuş ağ güvenliği kuruluşu şunlardır:

- SysAdmin, Audit, Network, Security (SANS) Institute
- Computer Emergency Response Team (CERT)
- International Information Systems Security Certification Consortium $(ISC)^2$

Bunun dışında çok sayıda kuruluş vardır. InfoSysSec güvenlik haber portalı sunar. Mitre, FIRST, CIS gibi önemli kuruluşlar vardır.

**1.1.3.2**

SANS 1989'da kurulan bir araştırma ve eğitim organizasyonudur. SANS'ın asıl amacı bilgi güvenliği eğitimi ve sertifikasyonudur. Bilgi güvenliği ile ilgili farklı alanlarla araştırma makaleleri yayınlar. Global Information Assurance Certification (GIAC) adlı sertifika SANS tarafından verilir.

**1.1.3.3**

CERT Carnegie Mellon Üniversitesinde kurulan Yazılım Mühendisliği Enstitüsünün bir bölümüdür. Morris solucanı CERT'in motivasyon sebeplerinden biridir. CERT büyük güvenlik olayları ve analiz çözümlerinden sorumludur.

**1.1.3.4**

$(ISC)^2$ 135'den fazla ülkede üretici bazlı eğitim ürünleri ve kariyer servisleri sunan bir organizasyondur. Görevi siber dünyanın daha güvenli olması için dünya çapında uzmanlar yetiştirmektir.

Dört önemli sertifikasyon yapar. Certified Information Systems Security Professional (CISSP), System Security Certified Practioner (SSCP), Certification and Accreditation Professional (CAP) ve Certified Secure Software Lifecycle Professional (CSSLP).

**1.1.3.5**

Güvenlik kuruluşlarının websitelerine ilaveten kullanılabilecek bir başka araç Really Simple Sindication (RSS) aracıdır.

RSS, sık güncellenen bilgilerin yayınlandığı web sitelerinden XML tabanlı bilgi akışı sağlar. Örneğin US-CERT aktif bir RSS kaynağı sunar.

### 1.1.4.Ağ Güvenliği Alanları

Network güvenlik alanları konuyu öğrenmek için bir çerçeve sunarlar. ISO/IEC (International Electrotechnical Commission) tarafından oluşturulmuş 12 güvenlik alanı vardır. Bu 12 alan kurumsal güvenliği sağlamak için imkanlar sağlar.
Risk değerlendirme: Risk yönetiminin ilk adımıdır. Sayısal ve nicelik olarak özel durumlara göre saldırı değerlendirmesi yapar.
Güvenlik politikası: Kurum personelinin davranışlarını, verilere nasıl erişileceğini, kimlerin erişeceğini belirleyen dökümanlardır.
Bilgi güvenliği organizasyonu: Bilgi güvenliği organizasyonunun yönetim modelini ortaya koyar.
Varlık yönetimi: Varlıkların sınıflandırma bilgilerini ortaya koyar.
İnsan kaynağı güvenliği: Çalışanların işe giriş, görev değişikliği ve işten ayrılmayla ilgili güvenlik prosedürlerini tanımlar.
Fiziksel ve çevresel güvenlik: Bir kurumdaki bilgisayar imkanlarını korumayı tanımlar.
Haberleşme ve operasyon yönetimi: Sistem ve ağdaki teknik kontrollerle ilgili prosedürleri tanımlar.
Erişim Kontrolleri: Veriye, sisteme, ağa erişim kısıtlamalarını ve yetkilerini tanımlar.
Bilgi sistemleri oluşturma geliştirme ve bakım: Uygulamalarla güvenliğinin entegrasyonunu sağlar.
Bilgi güvenliği vaka yönetimi: Bilgi güvenliği ihlallerinde yapılacak işlemleri tanımlar.
İş sürekliliği yönetimi: Sistemlerin bakım, yönetim ve geri yükleme prosedürlerini tanımlar.
Uyum: Bilgi güvenliği politikalarının, standartlarının ve kanuni düzenlemelerin uyumunu tanımlar.

**1.1.4.2**

Ağ güvenliği için ortaya konan 12 alan ağ güvenliği elemanları için bir ayrım sağlar. Bu 12 alanı ezberlemek önemli değildir ancak ISO tarafından onların varlığı ve resmi beyanı farkındalık oluşturmak için önemlidir. Onlar bir ağ güvenliği uzmanı için yararlı bir referans olarak hizmet verirler.
En önemli alanlardan biri güvenlik politikasıdır. Bir güvenlik politikası bir kurumun teknoloji ve bilgi varlıklarına ve verilerine erişimle ilgili kişilerin uymak zorunda olduğu kuralların resmi ifadesidir. Bir güvenlik politikası kavramı, geliştirmesi ve uygulaması bir organizasyonu güvende tutmak için kritik öneme sahiptir. Bu işler bir kurum içinde ağ güvenliği uzmanının sorumluluğundadır.

### 1.1.5.Ağ Güvenlik Politikaları

**1.1.5.1**

Ağ güvenliği politikası bir kuruluşun faaliyetleri ile ilgili tasarlanmış geniş, uçtan uca belgedir. Politika, ağ tasarımına yardımcı olur, güvenlik ilkelerini ve ağ uygulamasını kolaylaştırır.
Ağ güvenlik politikası ile ağ erişimi için kurallar, politikaların uygulama ilkeleri ve kurumun ağ güvenlik ortamının temel mimarisi açıklanır. Onun kapsamı ve etkisi, geniş bir komite tarafından oluşturulmasından kaynaklanır. Politika belgesi veri erişimi, web görüntüleme, şifre kullanımı, şifreleme ve e-posta ekleri gibi öğeleri yönetme amaçlı bir kompleks belgedir.
Güvenlik politikası kötü niyetli kullanıcıların ortaya çıkaracağı potansiyel riskleri içermelidir.

**1.1.5.2**

Cisco'nun SecureX mimarisi her hangi bir kullanıcının, herhangi bir cihazı her hangi bir zamanda herhangi bir yerden kullanımı için etkili güvenlik sağlamak için tasarlanmıştır. Bu yeni güvenlik mimarisi tüm durumları (kim, ne, nereye, nasıl, ne zaman) dikkate alan yüksek seviyeli politika dili kullanır. Oldukça dağıtık güvenlik politikası zorlaması ile son kullanıcı nerede çalışıyorsa ona yakın hale getirilir.
Bu mimari şu elemanları içerir:

- Tarama motorları

- Dağıtım mekanizmaları
- Güvenlik istihbarat operasyonları
- Politika yönetim konsolları
- Yeni nesil son nokta

**1.1.5.3**

Kullanıcı hareketliliğinin artması, tüketici cihazlarının çoğalması ve bilginin gelenekselin dışında hareketi BT altyapısının güvenliğini karmaşık hale getirdi. Bölük pörçük güvenlik çözümleri uygulama iki kat insan gücü, maliyet ve uygunsuz erişim politikalarına yol açabilir.

Cisco Securex ürünleri herhangi bir zaman, herhangi bir yerden, herhangi bir aygıtı kullanan herhangi bir kullanıcı için etkin güvenlik sağlamak için komple çözüm sunar. Bu neden Cisco Securex mimarisi kullanmanın gerekçelerinden biridir.

**1.1.5.4**

Güvenlik politikası şu sorulara cevap verebilmelidir.

Kullanıcıların ihtiyaçları nelerdir?

Hangi işlemler, veri veya bilgi sistemleri sizin için veya kurumunuz için kritik öneme sahiptir?

Hangi durumlarda kurumunuzun işleyişi kesintiye uğrar veya tamamen durur?

## 1.2.VİRÜSLER, SOLUCANLAR (WORMS) VE TRUVA ATLARI (TROJAN HORSES)

### 1.2.1 Virüsler

**1.2.1.1**

Bir kullanıcı bilgisayarı için güvenlik açıkları virüsler, solucanlar ve Truva atlarıdır.

Bir virüs, bilgisayara belirli bir istenmeyen işlevi yürütmek için başka bir programa iliştirilmiş yazılımdır.

Bir solucan bulaştığı bilgisayar üzerinde keyfi kodunu çalıştırır belleğe yerleşir ve daha sonra diğer bilgisayarlara bulaşır.

Bir Truva atı başka bir şey gibi görünen bir uygulamadır. Bir Truva Atı indirilip çalıştırıldığında içinde bulunduğu bilgisayardan atak yapmaya başlar.

**1.2.1.2**

Geleneksel olarak virüs terimi hücrelere bulaşarak yetişen ve kendini değiştiren organizmalar için kullanılır. Southern California Üniversitesinde öğrenci olan Frederick Cohen ilk olarak 1983'de "bilgisayar virüsü" terimini önerdi.

Bir virüs yasal programlara veya exe dosyalarına eklenmiş kötücül kodlardır. Çoğu virüs son kullanıcı aktivasyonu gerektirmez, uzun bir süre boyunca hareketsiz yatar ve daha sonra belirli bir zamanda etkinleşir. Basit bir virüs, bir yürütülebilir dosyanın ilk kod satırına kendini kurabilir. Aktive edildiğinde diski kontrol eder ve henüz bulaşmadığı tüm dosyalara bulaşabilir. Virüsler ekranda bir resim görüntülemek gibi zararsız bir iş yapabileceği gibi sabit diskteki dosyaları değiştirebilecek ya da silecek kadar yıkıcı olabilir. Virüsler de yakalanmamak için mutasyona programlanabilir.

Önceleri virüsler sadece floppy diskler ve modemler üzerinden yayılırken günümüzde USB memory stickler, CDler, DVDler, ağ paylaşımları veya e-mailler üzerinden yayılabilir. Üstelik günümüzde en yaygın olanı email virüsleridir.

### 1.2.2 Solucanlar

Wormlar kötücül kodun tehlikeli bir türüdür. Ağlardaki güvenlik açıklarından faydalanarak kendilerini çoğaltırlar. Solucanlar genellikle ağları yavaşlatabilir.
Bir virüs çalışabilmek için bir konak program gerektirir. Oysa solucanlar kendileri çalışabilirler. Onlar kullanıcıya ihtiyaç duymadan ağ üzerinden çok hızlı bir şekilde yayılabilir.
Wormlar internette en yıkıcı saldırıların bazılarından sorumludur. Örneğin, Ocak 2003'de, SQL Slammer Wormu, Denial of Service yöntemiyle küresel internet trafiğini yavaşlattı. 30 dakika içinde 250,000 'in üzerinde hotsa kendini yaydıktan sonra etkili oldu. Solucan, Microsoft SQL Server'da tampon taşma hatası ortaya çıkardı. Aslında bu güvenlik açığı için bir yama 2002 ortasında piyasaya sürülmüştü. Etkilenen sunucular güvenlik güncelleştirmesi yapılmamış olanlardı. Güvenlik güncelleştirmeleri bir kurumun güvenlik politikasında önemli bir yer tutar.

**1.2.2.2**

Azaltım teknikleri yıllarca önce ortaya çıkmış olmasına rağmen, solucanlar İnternet ile gelişmeye devam etti ve hala bir tehdit olarak duruyor. Solucanlar zamanla daha karmaşık hale gelmiş olsa da, yazılım uygulamalarındaki zafiyeti kullanma eğilimindedirler. Solucan saldırılarının çoğu üç ana bileşene sahiptir vardır:

- Güvenlik açığının etkinleştirilmesi: Bir solucan savunmasız bir sistem üzerinde bir istismar mekanizması (e-posta eki, yürütülebilir dosya, Truva Atı) kullanarak kendisini yükler.
- Yayılma mekanizması: Bir cihaza erişim elde ettikten sonra, solucan kendini çoğaltır ve yeni hedefler bulur.
- Yük: Bazı eylemler sonucu herhangi bir zararlı kod oluşur. Çoğu zaman, virüs bulaşmış bir konakçıdan bir arka kapı oluşturmak için kullanılır.

Solucanlar bilinen bir güvenlik açığından yararlanarak sisteme saldırmak için kendine yeten programlardır. Başarılı bir atak üzerine, yeni bulaşılan sistemde döngüye katılır ve tehlike büyütülür.

**1.2.2.3**

Son 20 yılda gerçekleştirilen büyük solucan ve virüs saldırıları incelendiğinde, hackerlar tarafından kullanılan saldırı yöntemlerinin çeşitli benzer aşamaları olduğu görülmüştür

- Probe faz (Araştırma fazı): Savunmasız hedefler belirlenir. Amaç, yıkılabilir bilgisayarları bulmaktır. ICMP ping taramaları ağların haritasını çıkarmak için kullanılır. Sonra uygulama taranır ve savunmasız yazılımı barındıran işletim sistemi belirlenir. Hackerlar şifreleri sosyal mühendislik, sözlük atakları, kaba kuvvet saldırısı, ya da ağ koklama kullanarak belirleyebilirler.
- Penetrate (Nüfuz) fazı: Exploit kodu savunmasız hedefe aktarılır. Amacı, tampon taşması, ActiveX veya CGI üzerinde kod çalıştırma veya e-posta virüsü gibi bir saldırı yoluyla istismar kodu yürütmek için hedef elde etmektir.
- Persist (Israr) fazı: Saldırı bellekte başarı ile başladıktan sonra, kod hedef sistemde devam etmeye çalışır. Amaç saldırganın kodunun sistem yeniden başladığında bile çalışır ve kullanılabilir olduğundan emin olmaktır. Bu işlem, sistem dosyalarını değiştirerek, kayıt defteri değişiklikleri yaparak ve yeni kod yükleyerek gerçekleştirilir.
- Propagate (Yayma) fazı: Saldırgan savunmasız komşu makinelere bakarak hedef saldırı bölgesini genişletmeye çalışır. Yayılma, diğer sistemlere e-posta göndererek, Internet Relay Chat (IRC) veya FTP üzerinden dosya paylaşımları yaparak, aktif web bağlantıları ile gerçekleştirilir.

- Paralyze (Felç) fazı: Sisteme gerçek hasar bu aşamada verilir. Dosyalar silinebilir, sistemler çökebilir, bilgiler çalınabilir ve DoS, DDoS atakları başlatılabilir.

### 1.2.3. Truva Atları

Truva atı terimi Yunan mitolojisinden gelir. Yunan savaşçıları at şeklindeki bir yapıya saklandılar ve beklenmedik bir anda şehri kuşattılar.
Bilgisayar dünyasında bir Truva atı istenen bir fonksiyonun kisvesi altında kötü niyetli faaliyetleri yürütmektir. Bir Truva atı gizli, kötü amaçlı kod içerir. Genellikle oyunlar Truva atına sahip olabilirler. Kullanıcı oyunu çalıştırırken, oyun çalışır ama arka planda kullanıcının sisteminde yüklü olan Truva Atı çalışır ve oyun kapatıldıktan sonra da çalışmaya devam eder.
Truva Atı kavramı esnektir. Bu, sisteme uzaktan erişim (arka kapı) sağlamak, ya da uzaktan talimat gibi eylemleri gerçekleştirebilir. Mesela "haftada bir kez bana şifre dosyasını gönder." Gibi.
Belirli bir amaç için yazılmış Truva atlarını sistemden algılamak oldukça güç bir iştir.

**1.2.3.2**

Truva atları sisteme verdikleri zararlara göre şöyle kategorize edilebilir:

- Remote-access Trojan Horse: Yetkisiz uzaktan erişime yol açar.
- Data sending Trojan Horse: Şifre gibi bilgileri gönderir
- Destructive Trojan Horse : Dosyaları bozar veya siler
- Proxy Trojan Horse: Kullanıcı bilgisayarını Proxy server olarak çalıştırır
- FTP Trojan Horse: 21 numaralı portu açar.
- Security software disabler Trojan Horse: Antivirüs yazılımları ve firewalların fonksiyonlarını durdurur.
- Denial of Service Trojan Horse: Ağı yavaşlatır veya durdurur.

### 1.2.4. Virüs, Solucan ve Truva Atlarını Azaltma

Keşfedilen yazılım açıklarının çoğunluğu tampon taşmaları ile ilgilidir. Bir tampon verileri geçici olarak saklamak için işlemler tarafından kullanılan bellek alanıdır. Sabit uzunluktaki tampon maksimum kapasitesine ulaşır ve yeni bir işlem tamponu kullanmak istediğinde bellek taşması oluşur. Bu durum bitişik bellek konumlarına ekstra veri yazılması yanı sıra diğer beklenmedik davranışlar oluşmasına neden olabilir. Tampon taşmaları genellikle virüsler, solucanlar ve Truva Atlarının kullandığı birincil kanaldır. Aslında, CERT tarafından tanımlanan üç yazılım açığından biri tampon taşmalarıdır.

Virüsler ve Truva Atları yerel kök tampon taşmalarından yararlanma eğilimindedir. Bir kök bellek taşması bir sisteme root yetkileri elde etmek için tasarlanmış bir tampon taşmasıdır. Yerel kök tampon taşmaları son kullanıcı veya sistemin bir hareketini gerektirir. Yerel kök bellek taşması, genellikle bir kullanıcı bir e-posta eki açtığında, bir web sitesini ziyaret ettiğinde ya da anlık mesajlaşma yoluyla bir dosya alışverişi yapıldığında başlatılır.
SQL Slammer ve Code Red gibi solucanlar uzak kök tampon taşması oluştururlar. Uzaktan kök tampon taşmaları sistem veya son kullanıcı müdahalesine gerek olmaması dışında yerel kök tampon taşmalarına benzer.

**1.2.4.2**

Virüs, solucan ve Truva atlarına karşı antivirüs yazılımları yaygın olarak kullanılır. Antivirüs yazılımları kullanıcıların kötücül kod almalarını engellerler. Antivirüs yazılımları ile sistemi taramak, yazılımları

güncel tutmaktan daha fazla zaman alır. Güncel tutma sayesinde yeni virüs tanımları alınır ve onlar bilinir hale getirilir. Bu yazılımlar genel olarak PC bazlı uygulanan sistemlerdir.

**1.2.4.3**

Solucanlar virüslere göre daha fazla network bazlı çalışırlar. Solucanları azaltmak için titizlik ve ağ güvenliği uzmanlarıyla koordinasyon gerekir. Solucan bulaşmasına karşı alınacak tedbirler dört aşamalıdır: Çevreleme, aşılama, karantina ve tedavi.

Çevreleme fazı solucandan etkilenmiş ağ alanlarında solucanın yayılmasını sınırlamayı içerir. Bu, solucanı durdurmak veya yavaşlatmak ve diğer sistemlere bulaşmasını engellemek için ağ segmentasyonu gerekir. Çevreleme ağ içinde kontrol noktalarında yönlendirici ve güvenlik duvarları tarafından giden ve gelen paketler için ACL kullanarak yapılabilir.

Aşılama aşaması çevreleme fazına paralel veya daha sonra çalışır. Aşılama safhasında tüm bulaşmamış sistemleri güvenlik açığı için uygun yamalar temin edilir.

Karantina fazı enfekte olmuş makineleri belirleme ve ağdan çıkarma şeklinde uygulanır. Bu da ağdaki enfekte makinelerin izolasyonu ile yapılır.

Tedavi aşamasında, aktif bulaşmış sistemler solucandan dezenfekte edilmektedir. Bu işlem, solucanın işlemini sonlandırma, solucanın değiştirdiği dosyaları veya sistem ayarlarını silme veya değiştirme, yamaları yapma şeklinde gerçekleştirilir. Bir diğer seçenek olarak, daha şiddetli vakalarda, sistem, solucan ve yan ürünler silinir ve sistemin yeniden kurulması gerekebilir.

**1.2.4.4**

SQL Slammer solucanı bulaşması durumunda, kötü niyetli trafik UDP 1434 portunda tespit edilir. Bu port normalde bir güvenlik duvarı tarafından bloke edilmelidir. Ancak, çoğu enfeksiyonlar güvenlik duvarı üzerinden geçemeyip arka kapılar yoluyla girerler. Bu nedenle solucanın yayılmasını önlemek için tüm iç ağdaki cihazlarda bu port engellenmelidir.

Bazı durumlarda 1434 portu işletmenin çalışması için gerekli olduğundan açık tutulur. İşletmede yasal işlemler için portun açık olması gerekebilir ve SQL Slammer'ın yayılmasına yardım edilebilir.

1434 portu sınırlı sayıda cihaz üzerinde açık tutularak seçici erişim verilmeli ve solucan bulaşma ihtimali azaltılmalıdır.

Virüsler, solucanlar ve Truva Atları ağı yavaşlatmayı veya tamamen durdurmayı amaçlarlar. İyi güvenlik politikaları ve antivirüs yazılımı seçenekleri ile tehditler azaltılabilir. Ağ güvenliği uzmanları uyanık durarak ağını korumalıdır. İyi bir ağ güvenliği profesyoneli güvenlik açıklarını bulmak için tüm ağı inceler ve bir saldırı meydana gelmeden önce onları giderir.

## 1.3.Atak Metodolojileri

### 1.3.1. Keşif (Reconnaissance) Atakları

Virüsler, solucanlar ve Truva atları dışında çok farklı tür network atakları vardır. Saldırıları azaltmak için, ilk olarak saldırı tipleri kategorize edilir. Ağ saldırıları kategorize edilirken bireysel saldırılardan ziyade saldırı türleri ele alınır. Ağ saldırılarını kategorize edecek bir standardizasyon yoktur. Bu derste üç ana kategoride saldırılar sınıflandırılmıştır.

**Keşif Saldırıları**

Keşif saldırıları sistemleri, hizmetleri veya güvenlik açıklarının izinsiz keşif ve haritalamasını içerir. Keşif saldırıları sıklıkla internette ücretsiz indirilebilen paket izleyiciler ve port tarayıcılar kullanılarak yapılır. Keşif, hırsızların boş bir konut veya kolay bir açık kapı veya penceresi olan evi tespit etmelerine benzer.

**Erişim Saldırıları**

Erişim saldırıları web hesapları, gizli veri tabanları ve diğer hassas bilgilere giriş kazanmak için kimlik doğrulama hizmetleri, FTP hizmetleri ve web hizmetlerinin kullanılmasıdır. Bir erişim saldırısı, birçok farklı şekilde gerçekleştirilebilir. Bir erişim saldırısı genellikle sistem şifrelerini tahmin etmek için bir sözlük saldırısı kullanır.

**Servis Dışı Bırakma Saldırıları**

Denial of service saldırıları bir ağ veya internet üzerinden istekleri son derece çok sayıda göndererek hedef cihazı gerçek işini yapamaz hale getirir. Sonuç olarak, saldırıya maruz kalan cihaz meşru erişim ve kullanım için kullanılamaz hale gelir.

**1.3.1.2**

Keşif bir erişim veya DoS saldırısı öncesinde, bilgi toplama olarak bilinir. Bir keşif saldırısında, kötü niyetli bir saldırgan IP adreslerini belirlemek için hedef ağa bir ping demeti gönderir. Saldırgan daha sonra servisleri veya portları canlı IP adreslerinin kullanılabilir olduğunu belirler. Nmap port taramalarını gerçekleştirmek için en popüler uygulamadır. Elde edilen bilgiye göre, saldırgan işletim sistemi türünü ve uygulamaları belirlemek için portları sorgular.

Keşif saldırıları bir ağa erişim sağlamak için şu araçları kullanabilir

- Paket koklayıcıları (packet sniffer)
- Ping demetleri (ping sweeps)
- Port taramaları (port scans)
- İnternet bilgi sorguları (Internet information queries)

**1.3.1.3**

Bir paket dinleyicisi bir LAN üzerinden gönderilen tüm ağ paketlerini karışık modda ağ kartı ile yakalamak için kullanılan bir yazılım uygulamasıdır. Karışık mod ağ bağdaştırıcısının uygulamaya alınan tüm paketleri elde ettiği moddur. Bazı ağ uygulamaları şifresiz düz metin olarak ağ paketlerini gönderir. Paketler şifreli olmadığından herhangi bir uygulama ile yakalanıp içlerine bakılabilir

Paket koklayıcılar aynı collision domain içindeki cihazlardan paket yakalayabilirler.

Wireshark gibi çok sayıda ücretsiz paket koklama ve analiz yazılımı vardır.

**1.3.1.4**

Yasal araçlar kullanılarak ping demeti gönderme, port tarama veya diğer yöntemlerle hostlardaki güvenlik açıkları belirlenir. Bilgi, IP adresleme veya port üzerinden elde edilir. Saldırgan sistemin güvenliğini aşmak için bu bilgileri kullanır.

**1.3.2.Erişim Atakları**

**1.3.2.1**

Hackerlar üç sebepten dolayı erişim ataklarını kullanır: Veri elde etme, erişim kazanma, erişim haklarını artırma.

Erişim saldırıları genellikle sistem parolalarını tahmin etmek için şifre saldırılarını kullanır. Şifre saldırıları brute-force saldırıları, Truva Atı programları, IP sızdırma ve paket izleyiciler de dahil olmak üzere çeşitli yöntemler kullanılarak uygulanabilir.

Bir brut-force saldırısı genellikle ağda çalışır ve sunucu gibi paylaşılan bir kaynağa oturum açmaya yarayan bir program kullanılır.

Örnek olarak, bir L0phtCrack veya LC5 çalıştırılarak bir Windows sunucunun şifresi elde edilebilir. Parola elde edildiğinde, saldırganın istenilen hedefe tüm tuş vuruşlarının bir kopyasını gönderen bir keylogger yüklenebilir. Ya da, bir Truva Atı ile benzer işlem yapılabilir.

**1.3.2.2**

Erişim saldırılarının beş türü vardır:

- Şifre saldırısı: Saldırgan sistem parolaları tahmin etmeye çalışır. Yaygın kullanılan bir yöntem sözlük saldırısıdır.
- Güven Sömürüsü: Saldırgan yetki verilmiş sistem ayrıcalıklarını kullanır
- Port yönlendirme: Bir saldırı aracı oturumları yeniden yönlendirmek için zayıf sistem üzerine yüklenir.
- Man-in-the-middle saldırısı: Saldırgan iki taraf arasına girer ve kendisini hedef sistem olarak gösterip tüm veri trafiğini üzerinden geçirir.
- Tampon taşması: Bir program ayrılan tampon belleğin ötesine veri yazar. Tampon taşmaları genellikle C veya C ++ programında bir hata sonucu olarak ortaya çıkar. Taşmanın bir sonucu olarak geçerli veri üzerinde kötü amaçlı kod yürütülmesi sağlanır.

**1.3.2.3**

Erişim saldırıları genellikle loglara göz atarak, band genişliği kullanımına bakarak ve işlem yüklerinden tespit edilebilir.

Ağ güvenlik politikası ile loglar tüm ağ cihazları ve sunucular için tutulmalıdır. Loglara bakılarak başarısız oturum açma girişimi olağan dışı bir sayıya ulaştığı fark edilebilir. ManageEngine EventLog Analyzer veya Cisco Secure Access Control Server (CSACS) gibi yazılımlar başarısız erişim girişimlerini raporlar. UNIX ve Windows sunucuları da başarısız oturum açma denemelerinin bir günlüğünü tutar. Cisco yönlendiricileri ve güvenlik duvarları da başarısız erişim denemeleri konusunda yapılandırılabilir. Man-in-the-middle saldırıları sıklıkla verileri çoğaltır. Böyle bir saldırının bir göstergesi ağ izleme yazılımı tarafından ağ etkinliğinin ve bant genişliği kullanımının alışılmadık miktarda artmasıdır.

**1.3.3.Denial of Service Atakları**

Bir DoS saldırısı kullanıcılar, cihazlar veya uygulamaların hizmet kesintisi ile sonuçlanan bir ağ saldırısıdır. Çeşitli mekanizmalar bir DoS saldırısı oluşturabilir. En basit yöntem geçerli bir ağ trafiği gibi görünen büyük miktarda veri üretmektir. Bu geçerli gibi görünen trafik ağı veya cihazı doldurur.

Bir DoS saldırısı meydana gelmesinin başlıca iki nedeni vardır:

- Bir host veya uygulama gibi kötü niyetli formatlı veri girişine maruz kalır.
- Bir ağ, host veya uygulama büyük miktarlı veriyi iletemez bu yüzden çökebilir veya aşırı yavaş hale gelebilir.

**1.3.3.2**

DoS saldırısına bir örnek zehirli paket göndermektir. Bir zehirli paket uygunsuz bir şekilde paket alıcısını işlemek için tasarlanmıştır. Zehirli paket alıcı cihazın çökmesine ya da çok yavaş çalışmasına neden olur. Bu atak cihaza gelen veya cihazdan çıkan bütün iletişimin bozulmasına yol açar.

Bir başka örnek, bir saldırgan ağ bağlantılarını ve bant bant genişliğini dolduran sürekli bir akış gönderir. Çoğu durumda, bu saldırganın oluşturduğu trafikle meşru trafiği ayırdetmek imkansızdır.

DDoS saldırısı çok sayıda koordineli kaynaktan çıkma dışında DoS'a benzer. Bir DDoS saldırısı trafikte bir artış oluştururken dağıtılan kaynaklardan saldırıları tanımlamak ve durdurmak için ağ güvenlik uzmanına ihtiyaç duyulur.

DDoS saldırıları aşağıdaki gibi yürütülür:

- Bir hacker erişilebilir sistemleri tarar.
- Korsan birkaç "eylemci" sisteme eriştikten sonra, onlara zombi yazılım yükler.
- Zombiler ajan sistemleri tarar ve onlara bulaşır.
- Korsan ajan sistemlere erişerek onlara uzaktan saldırı yazılımı yükleyerek DDoS saldırısını gerçekleştirir.

**1.3.3.3**

DoS saldırılarını anlamak için üç tür saldırı örneği incelenecektir.

Ping of Death (ölüm pingi)

Ölüm pinginde, bir hacker 65.535 bayt maksimum paket boyutundan çok daha büyük boyutlu IP ping paketlerini sürekli olarak gönderir. Bu boyuttaki ping hedef bilgisayarı bozabilir. Bu saldırının bir varyantı hedefin tamponları dolduracak ICMP fragmentleri göndererek sistem çökmesine yol açabilir.

Smurf (Şirin) Saldırısı

Bir smurf saldırıda, bir fail çok sayıda ICMP paketlerini broadcast adreslerine gönderir. Bunlar router üzerinden geçemeyecekleri için router tüm paketler için hata mesajı oluşturarak servis dışı kalır

TCP SYN Flood

TCP SYN saldırısı, üç yollu oturum kurma esnasında servera ilk syn gönderildikten sonra ack paketi gönderilmeyerek meşgul edilir.

**1.3.4.Ağ Ataklarını Azaltma**

**1.3.4.2**

Keşif atakları birkaç yolla azaltılabilir.

Güçlü hesap bilgileri kullanmak paket snifferlara karşı alınabilecek ilk önlem seçeneğidir. Güçlü kimlik doğrulama kolay ele geçirilebilecek kullanıcıların kimliğini doğrulamak için bir yöntemdir. Tek Kullanımlık Şifre (One-Time-Password-OTP) bir güçlü kimlik doğrulama şeklidir. OTP iki faktörlü kimlik doğrulama kullanmaktadır. İki faktörlü kimlik doğrulama PIN numarası gibi kimsenin bilmediği bir belirteçle kimlik bilgisini birleştirir. Otomatik vezne makineleri (ATM) iki faktörlü kimlik doğrulaması kullanır.

Şifreleme ayrıca paket dinleyicisi saldırılarını azaltmak için etkilidir. Trafik şifreli ise, az kullanılan bir paket algılayıcı kullanarak yakalanan verileri okumak mümkün değildir.

Ayrıca, port taramalar tam ping demeti olmadan çalıştırılabilir. Inaktif IP adresleri de taranır.

Bir keşif saldırısı olması durumunda ağ tabanlı IPS ve bilgisayar tabanlı IPS genellikle bir yöneticiyi haberdar edebilir.