Ağ ve Bilgi Güvenliği Yönetimi
Güvenlik Duvarı (Firewall)
Saldırı Tespit Sistemleri (Intrusion Detection System-IDS)
E-Posta Güvenliği
WWW Güvenliği

Prof. Dr. Resul Daş

Ağ ve Bilgi Güvenliği Yönetimi

Ağ ve Bilgi Güvenliği Yönetimi

- Bilgi güvenliği çerçevesinde kurulacak güvenlik sistemi altyapısının ve politikasının doğru bir şekilde belirlenebilmesi için, korunmak istenen bilginin değerlendirilmesi ve güvenlik yönetiminin doğru ve eksiksiz bir şekilde yapılması gerekir.
- Güvenlik yönetimi, bilgi ve bilgisayar güvenliğini olumsuz yönde etkileyecek faktörlerinin belirlenmesi, ölçülmesi ve en alt düzeye indirilmesi sürecidir.

Güvenlik Risklerini Değerlendirilmek

- Risk, bir olayın ve bu olayın sonucunun olasılıklarının birleşimi olarak tanımlanmaktadır.
- Risk yönetiminin bir adımı olan risk değerlendirmesi, risklerin tanımlandığı ve tanımlanan bu risklerin etkilerinin ve önceliklerinin belirlendiği bir süreçtir.
- Risk yönetimi, kabul edilebilir düzeyde bir riskin belirlenmesi, hali hazırdaki riskin değerlendirilmesi, bu riskin kabul edilebilir düzeye indirilebilmesi için gerekli görülen adımların atılması ve bu risk düzeyinin sürdürülmesidir.

Güvenlik Risklerini Değerlendirilmek

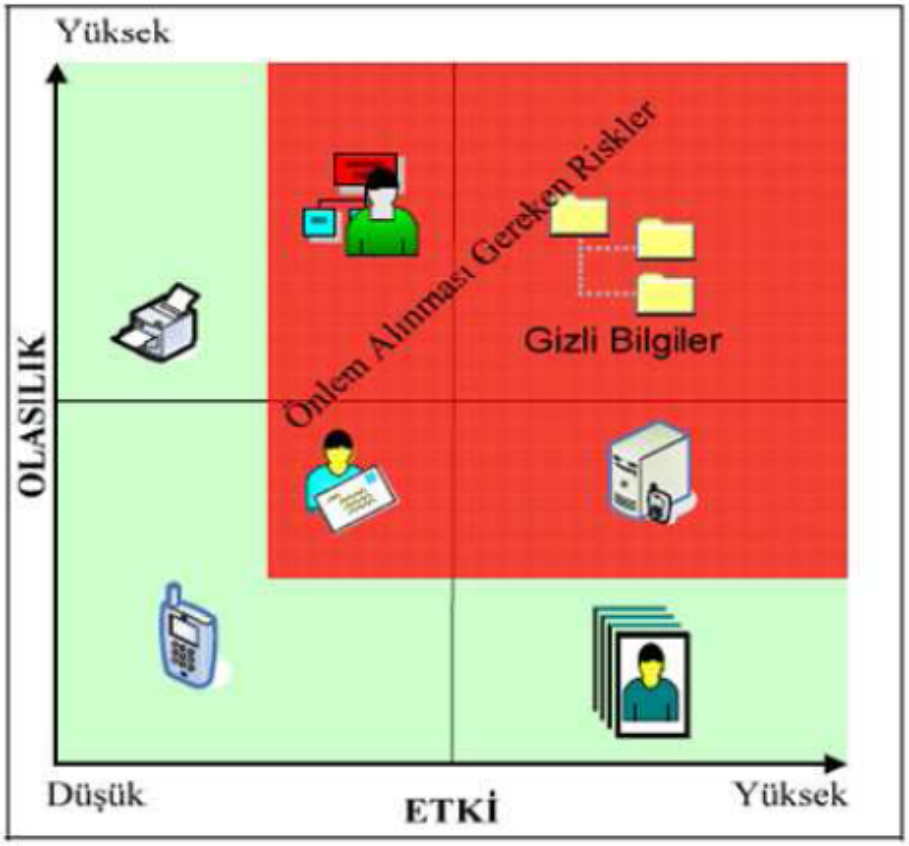
- Korunması gereken bilgi ya da varlıkların belirlenmesi;
- Bu varlıkların kuruluşlar açısından ne kadar değerli olduğunun saptanması;
- Bu varlıkların basına gelebilecek bilinen ve muhtemel tehditlerden hangilerinin önlenmeye çalışılacağının ortaya konulması;
- Muhtemel kayıpların nasıl cereyan edebileceğinin araştırılması;
- Her bir varlığın maruz kalabileceği muhtemel tehditlerin boyutlarının tanımlanması;
- Bu varlıklarda gerçekleşebilecek zararların boyutlarını ve ihtimallerini düşürmek için ilk planda yapılabileceklerin incelenmesi ve ileriye yönelik tehditleri asgari seviyede tutmak için atılması gereken adımların planlanması

risk değerlendirmesinin belli başlı safhalarındandır.

Güvenlik Risklerini Değerlendirilmek

- Bilgi ve diğer varlıklar, bu varlıklara yönelik tehditler, var olan sistemde bulunan korunmasızlıklar ve güvenlik sistem denetimleri, mevcut riski tayin eden bileşenlerdir.
- Hangi bilgi varlıklarının korunacağı belirlendikten sonra kuruluşa uygun risk değerlendirme yönteminin seçilerek risklerin tanımlanması yapılır.
- Seçilen risk değerlendirme yöntemine göre bilgi varlıkları şekilde örneği gösterilen risk haritasında konumlandırılır.
- Değerlendirilme yapıldıktan sonra risk değerlendirme haritasında, etkisi ve olasılığı yüksek olan tehditler için risklerin iyileştirilerek kontrol altına alınması işlemlerini kapsar.
- Risk haritasında bilgi varlıklarının yeri değişebileceğinden risk değerlendirme haritası düzenli olarak güncellenmeli ve gerekli önlemler alınmalıdır.

Güvenlik Risklerini Değerlendirilmek



Güvenlik Risklerini Değerlendirilmek

- Risk yönetimi sonucunda kurulacak ve yürütülecek güvenlik sisteminin maliyeti, dikkate alınması gereken bir başka önemli husustur.
- Güvenlik sisteminin maliyeti, korunan bilginin değeri ve olası tehditlerin incelenmesiyle belirlenen risk ile sınırlı olmalıdır.
- %100 güvenliğin olmayacağı ilkesi ile beraber, bilgi güvenliğinin ideal yapılandırılması üç süreç ile gerçekleştirilir.
- Bu süreçler,
  - önleme (prevention),
  - saptama (detection) ve
  - karşılık vermedir (response ya da reaction).

Güvenlik Süreçleri - Önleme

- Güvenlik sistemlerinin en çok üzerinde durduğu ve çalıştığı süreçtir.
- Bir evin bahçesine çit çekmek, çelik kapı kullanmak gibi güncel hayatta kullanılan emniyet önlemleri gibi, bilgisayar sistemlerine yönelik tehdit ve saldırılara karsı, sistemin yalıtılmış olması için çeşitli önlemler geliştirilmektedir.

Güvenlik Süreçleri - Önleme

- Kişisel bilgisayar güvenliği ile ilgili önlemler;
  - virüs tarama programlarının kurulu olması, ve bu programların ve işletim sistemi hizmet paketlerinin ve hata düzeltme ve güncellemelerinin düzenli aralıklarla yapılması,
  - bilgisayarda şifre korumalı ekran koruyucu kullanılması,
  - bilgisayar başından uzun süreliğine ayrı kalındığında sistemden çıkılması,
  - kullanılan şifrelerin tahmininin zor olacak şekilde belirlenmesi, bu şifrelerin gizli tutulması ve belirli aralıklarla değiştirilmesi,

Güvenlik Süreçleri - Önleme

- Kişisel bilgisayar güvenliği ile ilgili önlemler;
  - disk paylaşımlarında dikkatli olunması,
  - Internet üzerinden indirilen veya e-posta ile gelen dosyalara dikkat edilmesi,
  - önemli belgelerin parola ile korunması veya şifreli olarak saklanması,
  - gizli veya önemli bilgilerin e-posta, güvenlik sertifikasız siteler gibi güvenli olmayan yollarla gönderilmemesi,
  - kullanılmadığı zaman İnternet erişiminin kapatılması,
  - önemli bilgi ve belgelerin düzenli aralıklarla yedeklerinin alınması

Güvenlik Süreçleri - Önleme

- Kurumsal ortamlarda bilgisayar güvenliğinde uygulanması gereken önleme adımları daha geniş ve karmaşıktır.
- Güvenlik ile ilgili uzmanlaşmış kişilerin çalıştığı bu tür sistemlerde, önleme ile ilgili yapılanlardan bazıları:
  - İşletim sistemi ve yazılımların servis paketlerinin ve güncellemelerin düzenli aralıklarla incelenmesi,
  - Kullanıcı haklarının asgari seviyede tutulması, kullanılmayan protokol, servis, bileşen ve proseslerin çalıştırılmaması,
  - Veri iletişiminde şifreleme tekniklerinin, korunmasızlık tarayıcıları, Sanal Özel Ağ (Virtual Private Network) kullanılması,
  - Açık Anahtar Altyapısı (Public Key Infrastructure) ve e-imza kullanımı
  - Biometrik tabanlı sistemlerin kullanımı olarak sıralanabilirler.

Güvenlik Süreçleri - Saptama

- Güvenlik, sadece önleme ile sağlanabilecek bir mesele değildir.
- Örneğin bir müzede iyi bir korunmanın sağlanmış olması, müzenin çevresinin çitlerle çevrili olması, kapıların kapalı ve kilitli olması, o müzede geceleri bekçi kullanılmamasını gerektirmez.
- Aynı şekilde bilgisayar sistemlerinde de saldırı girişimlerini saptayacak yöntemlerin de kullanılması şarttır.

Güvenlik Süreçleri - Saptama

- Önleme, saldırıları güçleştiren (ama imkânsız kılmayan) veya saldırganların cesaretini kıran (ama yok etmeyen) bir engel inşa etmeyi sağlar.
- Saptama ve karşılık verme olmadan önlemenin ancak sınırlı bir faydası olabilir.
- Sadece önleme ile yetinilseydi, yapılan çoğu saldırıdan haberdar bile olunamazdı.
- Saptama ile daha önce bilinen veya yeni ortaya çıkmış saldırılar, rapor edilip, uygun cevaplar verebilir.
- Saptamada ilk ve en temel basamak, sistemin bütün durumunun ve hareketinin izlenmesi ve bu bilgilerin kayıtlarının tutulmasıdır.
- Bu şekilde ayrıca, saldırı sonrası analiz için veri ve delil toplanmış olur.

Güvenlik Süreçleri - Saptama

- Saptama sürecinde kullanılan yöntemlerden bazıları şunlardır:
  - Güvenlik duvarları
  - Saldırı tespit sistemleri (intrusion detection system)
  - Ağ trafiği izleyiciler
  - Kapı (port) tarayıcılar
  - Gerçek zamanlı koruma sağlayan karsı virüs ve casus yazılım araçları
  - Dosya sağlama toplamı (checksum) kontrol programları
  - Ağ yoklayıcı (sniffer) algılayıcıları

Güvenlik Süreçleri- Karşılık Verme

- Bekçiler, köpekler, güvenlik kameraları, algılayıcılarla donatılmış bir yerin, hırsızların dikkatini çekmesi gibi, gerçek zamanlı saptama sistemlerine sahip bilgisayar sistemleri de bilişim korsanları ve saldırganlara cazip gelir.
- Hızlı karşılık verme, bu saldırıları püskürtmek için güvenlik sistemini tamamlayan esaslı bir öğe olarak ortaya çıkmaktadır.

Güvenlik Süreçleri- Karşılık Verme

- Karşılık verme, önleme süreci ile baş edilemeyen ve saptama süreçleri ile belirlenmiş saldırı girişimlerini, mümkünse anında veya en kısa zamanda cevap verecek eylemlerin ifa edilmesi olarak tanımlanabilir.
- Saldırı tespit sistemleri, bu tespite cevap verecek birilerinin veya bir sistemin olması ile anlam kazanabilir.
- Aksi takdirde bu durum, hiç kimsenin duyup da önemsemediği bir araba alarmının getireceği faydadan öteye gitmez.
- Bu açıdan karşılık verme güvenlik sürecini tamamlayan önemli bir halkadır.

Güvenlik Süreçleri- Karşılık Verme

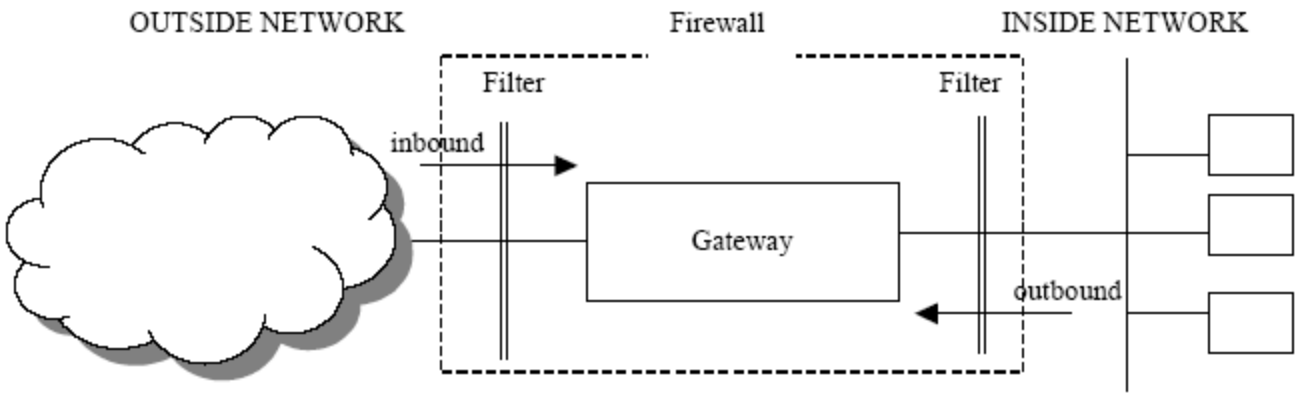
- Saldırı tam olarak önlenmese bile; sistemin normal durumuna dönmesine, saldırıya sebep olan nedenlerin belirlenmesine, gerektiği durumlarda saldırganın yakalanmasına, güvenlik sistemi açıklarının belirlenmesine ve önleme, saptama ve karşılık verme süreçlerinin yeniden düzenlenmesine olanak verir.
- Saldırı tespit edilince yapılması gereken işlerin, daha önceden iyi bir şekilde planlanması, bu sürecin etkin bir şekilde işlemesini ve zaman ve para kaybetmemeyi sağlayacaktır.
- Yıkım onarımı (disaster recovery), bu aşama için gerçekleştirilen ve en kötü durumu ele alan esaslı planların başında gelir.

Güvenlik Duvarları (Firewall)

Güvenlik Duvarı

- Bir güvenlik duvarı, bilgisayara ve ağa veri geçişini denetleyen, belirli kriterlere uymayan paketleri geçirmeyen bir yazılım programı veya donanım parçasıdır.
- Kullanılan güvenlik duvarının tipine göre bu işlem, verinin kaynağıyla istemci bilgisayar arasında olabilir veya bilgisayarda bir uygulama olabilir.

Güvenlik Duvarları



Güvenlik Duvarları

- 3'e ayrılırlar:
  - Paket Filtreleyici Güvenlik Duvarları (Packet Filtering Firewalls)
  - Devre Düzeyinde Güvenlik Duvarları (Circuit-Level Firewalls)
  - Uygulama Düzeyinde Güvenlik Duvarları veya Vekil Sunucular (Application-Level Firewalls or Proxy Servers)

Paket Filtreleyici Güvenlik Duvarları

- Gelen IP paketlerinin iletilip iletilmeyeceğine daha önceden belirlenmiş bir takım kurallara göre karar veren çok portlu bir araçtır.
- Bu güvenlik duvarları, üzerlerinden geçen paketleri incelerler ve bunları verinin kaynağına, hedefine, kaynak ve hedef portuna bağlı olarak çeşitli kurallarla karşılaştırırlar.
- Bu güvenlik duvarları ile bilgilerin belirli türlerini engellemek, iyi bilinen portları kapatmakla kolayca yapılabilir.

Paket Filtreleyici Güvenlik Duvarları

- Bu güvenlik duvarları verinin içeriğine bakmazlar.
- Sadece şu bilgilere göre filtreleme yaparlar:
  - Kaynak ve hedef IP adresleri
  - Kaynak ve hedef port numaraları
  - TCP bağlantı bayrakları

Paket Filtreleyici Güvenlik Duvarları

- Paket filtreleme yapan yönlendiricilere perdeleyici yönlendiriciler (screening routers) denir
  - Örneğin,

    Standart izin listesi

    Interface Ethernet0

    Ip address 172.16.1.1 255.255.255.0

    Ip access-group 1

    Access-list 1 deny host 172.16.3.10

    Access-list 1 permit any
- Paket filtreleyiciler yönlendirme yapmak zorunda değildirler

Paket Filtreleyici Güvenlik Duvarları

- İkiye ayrılırlar:
  - Durumsuz (Stateless)
  - Durumlu (Stateful)
- Durumsuz olanlarda pratikte problemler yaşanmaktadır.
- Bu problemleri engellemek için “stateful inspection” yöntemi kullanılır.

Paket Filtreleyici Güvenlik Duvarları

- Stateful inspection
  - Checkpoint Software Technologies tarafından bulunmuştur.
  - Eski IP paketlerine ait bilgiler saklanır.
  - Arkadan gelen paketler daha hızlı geçerler

Paket Filtreleyici Güvenlik Duvarları

- Dezavantajları
  - Sistem yöneticisinin saldırıları anlamasına yardımcı olabilecek kayıt tutma (logging) kabiliyeti çok azdır.
  - Paket filtreleme kuralları doğrudan test edilmek için zordurlar. Dolayısıyla, test edilemeyen açık noktalar kalabilmektedir.
  - Eğer karışık filtreleme kuralları gerekirse bunlar yönetilemez bir hale gelebilirler.
- Çoğu kablo/DSL cihazları bu güvenlik duvarlarını korumalarının bir parçası olarak kullanırlar.

Devre Düzeyinde Güvenlik Duvarları

- Bu tip güvenlik duvarları, dışarıdan bilgi akışına sadece içerideki bilgisayarlardan istek geldiğinde izin verir.
- Dışarıya giden isteklerin kaydı tutulur ve sadece isteğe karşılık gelen cevaba izin verilir.
- Bu tip bir güvenlik duvarının en önemli avantajlarından biri, dışarıdakilerin bütün bir ağı sadece güvenlik duvarının adresi olarak görmesidir. Böylelikle, ağın gerisi korunmuş olur.

Devre Düzeyinde Güvenlik Duvarları

- Bunun en büyük avantajı, içeriden istek gelmediği takdirde dışarıdan içeriye girilmesine izin verilmemesidir.
- Güvenlik duvarı açana kadar bütün portlar kapalıdır.
- Ana dezavantajı ise, diğer filtreleme yöntemleriyle birleştirilmediği takdirde içeriden gelen herhangi bir veri isteğine izin vermesidir.

Devre Düzeyinde Güvenlik Duvarları

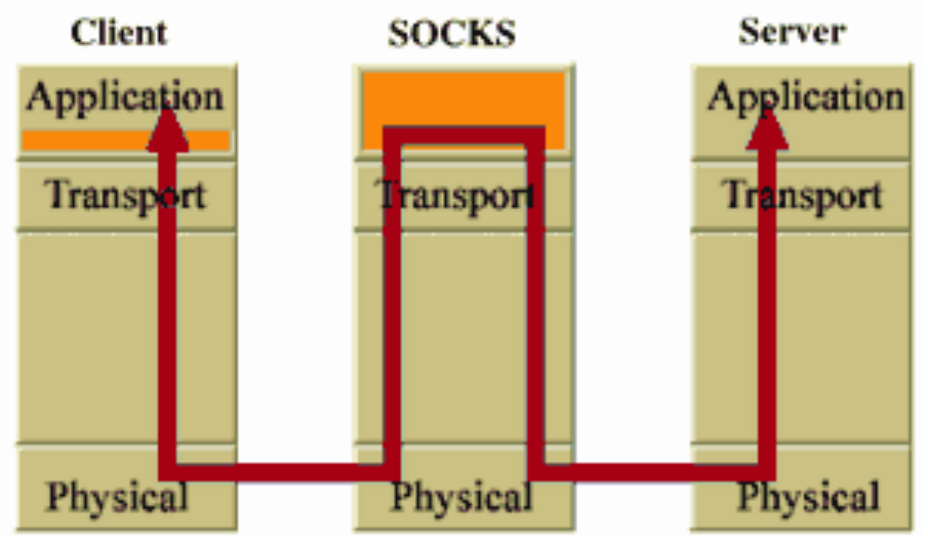
- Kablo/DSL yönlendiricileri bu yöntemi birincil olarak kullanırlar.
- Daha belirgin olarak, bunlar internet paylaşımlı devre düzeyinde ağ geçitlerinin bir kombinasyonu olan NAT (Network Address Translation) kullanırlar.
- Devre düzeyinde ağ geçitleri arasında SOCKS yaygın olarak kullanılmaktadır.

SOCKS

- İstemci yazılımına ve/veya TCP/IP yığınına modifikasyon gerektirir
- İki parçadan oluşur
  - SOCKS sunucusu (daemon)
  - SOCKS istemcisi (kütüphanesi)

SOCKS

- SOCKS sunucusu uygulama katmanında çalışır
- SOCKS istemcisi uygulama ve ulaşım katmanları arasında çalışır



Uygulama Düzeyinde Güvenlik Duvarları

- “Proxy” olarak da anılan bu güvenlik duvarları, devre düzeyindekilere benzer şekilde, ağa giriş ve çıkış için tek geçiş olarak davranırlar.
- En önemli fark ise bilgiyi ele alış şekillerindedir.
- Devre düzeyindeki güvenlik duvarları adres ve port bilgisine bakarken, bu güvenlik duvarları daha detaylı olarak inceler ve içeriğe bakar.
- Bu yöntemi kullanan güvenlik duvarları, yaygın veri türlerinin güvenlik duvarından geçmesine izin vermeden önce proxy uygulamaları çalıştırırlar.

Uygulama Düzeyinde Güvenlik Duvarları

- Bunun iki önemli avantajı vardır.
  - İlki, dış kaynaklar güvenlik duvarı arkasındaki bilgisayarlar arasında doğrudan bağlantıya izin vermemesi,
  - diğeri ise verinin içeriğine bakılarak filtreleme yapılabilmesidir.

Uygulama Düzeyinde Güvenlik Duvarları

- Uygulama düzeyindeki güvenlik duvarları sundukları kontrol düzeyleri nedeniyle çok güvenlidirler fakat önemli konfigürasyon gereksinimleri vardır.
- Ayrıca, paketleri geçirmekte de, çalışan proxy uygulamaları nedeniyle, diğer güvenlik duvarlarına göre yavaştırlar.
- İstemci bilgisayarlara da dışarıdaki kaynaklara erişim için ayrıca proxy konfigürasyonları yapılması gerekir.

Uygulama Düzeyinde Güvenlik Duvarları

- Kullanıcı asıllama ve yetkilendirmesi yapılır
- Kullanıcı asıllama için gerekli bilgiler başka bir güvenlik sunucusunda tutulabilir
- Bunun için en çok kullanılan protokoller
  - Livingston Enterprises firmasına ait olan RADIUS
  - Cisco firmasına ait olan TACACS
- Bir sunucuya bağlanmadan önce uygulama düzeyinde bir ağ geçidine bağlanmak işlemi saydamlaştırılabilir. Buna “saydam vekillik (transparent proxy)” denir

Uygulama Düzeyinde Güvenlik Duvarları

- Bu güvenlik duvarları da devre düzeyindeki güvenlik duvarları gibi internet paylaşımı ile bütünleşmiştir.
- Bu tip güvenlik duvarları genellikle büyük bilgisayar ağlarını korumak için iş amaçlı kullanılmaktadırlar.

Güvenlik Duvarı Konfigürasyonları

- Değişik çeşitleri vardır.
- En yaygın kullanılan ikisi:
  - Çift-Evli Güvenlik Duvarları (Dual-Homed Firewalls)
  - Perdelenmiş Alt Ağ Güvenlik Duvarı (Screened Subnet Firewall)

Güvenlik Duvarı - Özet

- Paket filtreleyici güvenlik duvarları basit bir güvenlik çözümü sağlarlar ve paketlerdeki verinin içeriğine bakmazlar
- Devre düzeyindeki güvenlik duvarları dışarıdan gelen paketler için tek giriş noktasıdır. Dışarıdaki bilgisayarlar sadece bunun adresini bilirler. Böylelikle, arkasındaki ağı güvenli bir şekilde korur. Ayrıca, asıllama ve yetkilendirme de yapılır. Burada da verinin içeriğine bakılmaz
- Uygulama düzeyindeki güvenlik duvarları ise bilginin içeriğine bakarak paketi geçirip geçirmeyeceğine karar verir. Asıllama ve yetkilendirme mekanizmaları kullanır.

Güvenlik Duvarı - Özet

- Çift-evli güvenlik duvarları daha güvenli bir yapı sunarken performans ve esneklik bakımından perdelenmiş alt ağ güvenlik duvarlarından daha düşük seviyededirler.

Saldırı Tespit Sistemleri

Saldırı Tespiti Nedir?

- Saldırı tespit sistemleri bir bilgisayar sisteminde veya ağında meydana gelen olayları görüntüleme ve bu olayların bilgisayar veya ağın mahremiyetine, bütünlüğüne, kullanılırlığına uyuşma teşebbüsleri veya güvenlik sistemini atlatma olarak tanımlanan izinsiz olarak erişim işareti olup olmadığını analiz eden süreçtir.

Saldırı Tespiti Nedir?

- İzinsiz olarak erişim;
  - Sisteme internetten erişen saldırganlar,
  - Yetkisi kapsamında olmayıp ilave ayrıcalık kazanma teşebbüsünde bulunan sistem yetkili kullanıcıları,
  - Kendilerine verilen ayrıcalıkları yanlış kullanan sistem yetkili kullanıcılar tarafından kaynaklanmaktadır.
- Saldırı tespit sistemleri bu görüntüleme ve analiz sürecini otomasyona çeviren yazılım ve donanım ürünleridir.

Saldırı Tespit Sistemleri Neden Kullanılmalıdır?

- Saldırı tespit sistemleri her şirketin güvenlik altyapısına ilave gerekli tedbir olarak geçerliliğini kazanmıştır.
- Saldırganların cezalandırılması ve keşfedilme riskinin artmasıyla problemli davranışları engellemek,
- Saldırıları ve diğer güvenlik ölçütleri tarafından önlenemeyen diğer güvenlik ihlallerini bulmak,
- Saldırı başlangıçlarını bulmak ve çözmek,

Saldırı Tespit Sistemleri Neden Kullanılmalıdır?

- Özellikle geniş ve karmaşık şirketlerin güvenlik dizaynı ve yönetimi için kalite kontrolcüsü olarak rol almak,
- İzinsiz olarak erişimler hakkında faydalı bilgi sağlamak.
- Var olan tehdidi belgelendirmek,

Başlıca Saldırı Tespit Sistemleri

- Farklı görüntüleme ve analiz yaklaşımlarıyla karakterize olan birkaç çeşit saldırı tespit sistemi mevcuttur.
- Her yaklaşımın avantaj ve dezavantajları vardır.
- Bütün yaklaşımlar saldırı tespit sistemleri için soysal süreç modeli terimi ile tanımlanabilir.
  - Süreç,
  - Zamanlama,
  - Bilgi kaynakları.

Ağ Tabanlı Saldırı Tespit Sistemleri

- Temel amacı ağ üzerinden yapılan saldırıları ağ trafiğini gözetleyerek tespit etmektir.
- Ağ paketlerini yakalayıp bunları analiz ederek saldırı tespiti yaparlar.
- Bir bilgisayar ağının tamamını ya da belli bir kısmını izlerler.

Ağ Tabanlı Sistemlerin Avantajları

- İyi yerleştirilmiş birkaç ağ tabanlı nüfuz tespit sistemi geniş bir ağı görüntüleyebilir.
- Genellikle ağı dinleyen pasif cihazlar oldukları için mevcut ağa etkileri yok denecek kadar azdır.
- Saldırılara karşı büyük güvenlik sağlayabilirler ve çoğu saldırgan tarafından fark edilmeleri zordur.

Ağ Tabanlı Sistemlerin Dezavantajları

- Geniş veya yoğun ağlarda tüm paketleri işlemede zorluklar yaşanmakta ve dolayısıyla yoğun trafik zamanlarında saldırıları sezmede hataya düşebilmektedir.
- Şifrelenmiş bilgi incelenememektedir. Bu daha çok sanal özel ağ (Virtual Private Network-VPN) kullanılarak yapılan saldırılarda baş gösteren bir sorundur.
- Bir çok ağ tabanlı saldırı tespit sistemi sadece ağa saldırının olduğunu tespit etmekte saldırının başarılı olup olmadığını sezememektedir.
- Anahtarlama cihazları bulunan ağlarda çalışmamaktadır.

Host Tabanlı Saldırı Tespit Sistemleri

- Belli bir bilgisayarı izlerler.
- İki tür bilgi kaynağı kullanırlar:
  - işletim sistemi izleme seçenekleri ve
  - sistem günlük dosyaları.

Host Tabanlı Sistemlerin Avantajları

- Host tabanlı saldırı tespit sistemleri yerelden hosta kadara olan olayları görüntüleme yetenekleriyle ağ tabanlı saldırı tespit sistemleriyle tespit edilemeyen saldırıları sezebilmektedirler.
- Host tabanlı saldırı tespit sistemleri genellikle host tabanlı bilginin veri şifrelenmeden önce ve/veya varış hostunda veri şifresi çözüldükten sonra analiz yaptığından trafiği şifrelenmiş koşularda çalışabilmektedirler.

Host Tabanlı Sistemlerin Avantajları

- Anahtarlama cihazlı ağlardan etkilenmemektedirler.
- Host tabanlı saldırı tespit sistemleri işletim sistemleri denetleme denemeleri üzerine çalıştığı zaman trojenleri ve yazılımla bütünleşik açıkları içeren saldırıları sezmeye yardımcı olabilmektedir.

Host Tabanlı Sistemlerin Dezavantajları

- Host tabanlı saldırı tespit sistemleri görüntülenen her host için yapılandırılması ve yönetilmesi gerektiğinden yönetimi daha zordur.
- Saldırıya uğrayabilir ve saldırının bir parçası olarak hizmet dışı bırakılabilirler.
- Host tabanlı saldırı tespit sistemleri ağ taramalarını sezmek veya tüm ağı hedef alan gözetleme için uyumlu değildir; çünkü ait olduğu hostun aldığı ağ paketlerini görebilmektedirler.

Uygulama Tabanlı Saldırı Tespit Sistemleri

- Avantajları:
  - Bireysel kullanıcıların yetkisiz işlemlerini takip edilmesine yarayan, kullanıcılar ve uygulamalar arasındaki etkileşimleri görüntüleyebilirler.
  - Genellikle uygulama hareketlerinin son noktasını ara yüzledikleri için şifreli koşullarda çalışabilmektedirler.
- Dezavantajları:
  - Saldırıya daha açıktır.
  - Genellikle kullanıcı seviyesindeki olayları görüntülemekte olup, trojen veya diğer yazılım saldırılarını sezememektedir.
  - Bundan dolayı uygulama tabanlı saldırı tespit sistemlerinin host tabanlı ve/veya ağ tabanlı sistemlerle birlikte kullanılması uygundur.

E-Posta Güvenliği

E-Posta Güvenliği

- E-posta sistemleri geleneksel posta sistemi ile büyük benzerlik göstermektedir:
  - İletilmesi istenen mesaj hazırlanarak sonra alıcı tarafın e-posta adresi de eklenerek uygun bir program veya ücretsiz internet siteleri aracılığıyla mesaj gönderilir.
  - E-posta öncelikle bir sunucuya iletilir.
  - Sunucu ise alıcı alanındaki e-posta adresine mesajın gönderilmesini sağlar.

E-Posta Güvenliğine Yönelik Tehditler

- Gizlilik Adımındaki Eksiklik
- Brute Force
- Fake Mail
- Phishing
- Keylogger-Trojan
- Uygulama Zaafları
- Sosyal Mühendislik
- XSRF-CSRF-XSS
- Clickjacking

Tehditler- Gizlilik Adımındaki Eksiklik

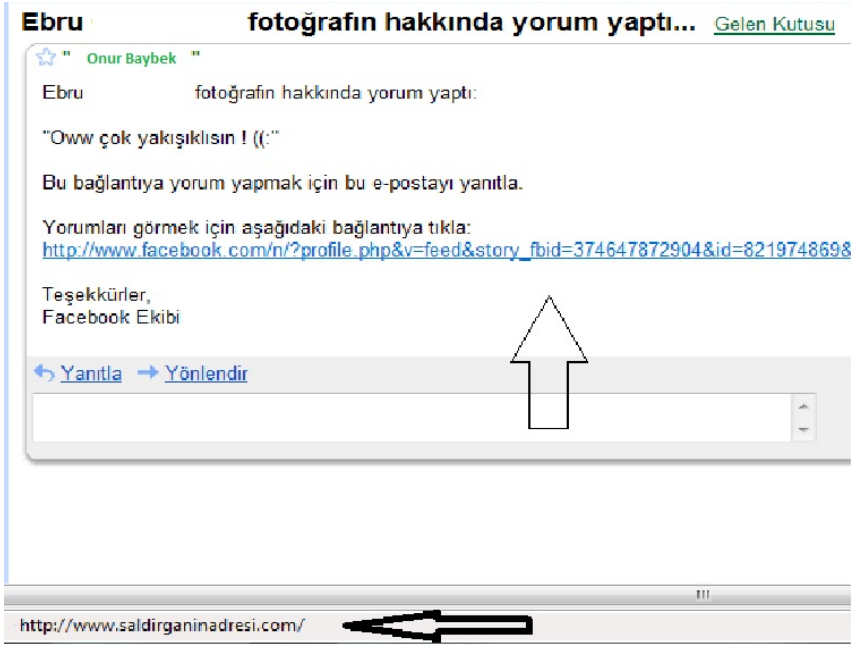
- Herhangi bir web sayfasına üye olduğunuz anda o sayfanın arama motorlarının robotları tarafından indexlenmesi sonucunda mail adresiniz "bulunabilir" olacaktır.
- Diğer bir ihtimal ise üyelik profilinizden e-posta adresinizin okunabilmesidir.
- Arama motoru kayıtlarına mail adresiniz girdiği anda spam listelerine de girmiş olursunuz, bu durumda da brute force (kaba kuvvet) ile saldırı yapanlarında "tesadüfen" saldırı listesine dahil olabilirsiniz.
- Üye olduğunuz web uygulamasının veritabanı kırıldığı (hacklendiği) zaman eğer şifreniz kriptolanmamış ya da bir hash fonksiyonu içinden geçirilip kaydedilmemiş ise üyelik için kullandığınız şifre de ele geçirilecektir. Genel olarak kullanıcıların birçok yerde aynı şifreyi kullandığını düşünürsek bu ciddi bir durumdur.
- **Bu nedenlerden dolayı başkaları tarafından ele geçirildiğinde sizin için sorun olacak mail adreslerinizi sitelere üye olmak için kullanmamalısınız.**

Tehditler- Brute Force (Kaba Kuvvet) Atak

- Deneme yanılma yada bazı kelime listeleri kullanarak şifreyi tahmin etmeye çalışan saldırı türüdür.
- Günümüzde teknoloji saldırganlar lehinde çalışarak tanıdığınız kişilerin bazı bilgilerini girip onlardan şifre üreten ve deneyen programlar geliştirilmiştir.
- **Bu saldırıdan korunmak için e-posta şifrelerimizi küçük-büyük harfleri, rakamları ve özel karakterleri birlikte kullanarak oluşturmamız gerekir.**

Tehditler- Fake Mail (Sahte Mail) Atak

- Posta kutunuza giriş yaptığınız sayfanın veya herhangi bir web sayfasının fake'inin (sahte) basit html kodları ve formmail ile hazırlanmış halidir.
- Kullanıcıyı bu adrese bir mail yardımı ile çekmeye çalışmak ve bu sahte giriş panelinden giriş yapmasını sağlatmaya çalışma işlemidir.
- **Saldırıdan korunmak için dikkatli davranılarak tıklanacak bağlantının nereye götüreceğini gösteren adres çubuğu incelenmelidir.**



Tehditler- Pnishing

- “Sosyal Mühendislik” teknikleri kullanılarak, kurbanın kredi, Debit/ATM kart numaraları/CVV2, şifreler ve parolalar, hesap numaraları, internet bankacılığına girişte kullanılan kullanıcı kodu ve şifreleri gibi büyük önem arz eden ve çok iyi korunması gereken bilgilerini, kurbanı aldatarak elde etme yöntemi olarak tanımlanabilir.
- Başka bir ifadeyle Phishing; kişileri, yasal bir şirket, ajans veya organizasyon olduğuna inandırarak, kişisel ve finansal bilgilerini ele geçirme yöntemidir.
- Mail'i gönderen kişinin adresine aşina olmanız, bu mailin gerçekten o kişi tarafından yollandığı anlamına gelmez ! Gönderen kısmında yazan adres saldırgan tarafından istediği gibi değiştirilebilir.
- **Tek korunma yöntemi dikkatli ve bilinçli olmaktır.**

Tehditler- Keylogger / Trojan

- Bir malware (Zararlı Yazılım) genellikle temel olarak 2 kısımdan oluşur.
  - Bunlar “server-sunucu” ve “client-istemci”tir.
  - Zararlı dosya hedef kişiye çeşitli yöntemlerle kabul ettirilmeye çalışılır.
  - Server dosyasını hedef kişi çalıştırdığı andan itibaren hedef üzerinden veri gönderilir/alınır, ekran görüntüsü yada klavye vuruşları alınabilir.
  - Bir keylogger veya trojan sayesinde hedef seçilen bilgisayarda yapılan işlemlerin kayıtları da elde edilebilir..
- **Sürekli olarak değişikliğe uğrayan ve yenileri yayılan bilgisayar virüslerine (keylogger – trojan) karşı alınabilecek en belirgin önlem düzenli olarak veritabanları güncellenen bir antivirüs programıdır.**
- **Antivirüs programları doğrudan kullanıcının masaüstü bilgisayarında çalışabileceği gibi e-posta sunucu sistemleri, içerik tarama uygulamaları, firewall gibi merkezi yapılar üzerinde de çalıştırılabilir.**

Tehditler- Uygulama Zaafları

- **E-posta hesabınıza girişlerinizde tarayıcılarınızın “beni hatırla” seçeneğini aktif edilmemelidir.**
  - **Hatırla demeniz durumunda browser'ın (tarayıcı) şifreleri barındırdığı dosyanın çeşitli yollarla saldırganın eline gelmesi ile mail adresiniz hacklenebilir .**
  - **Firefox'un hatırladığı şifreleri görüntüleyebilirsiniz.**
  - **Outlook şifreleriniz “Protected Storage PassView” gibi yazılımlarla çalınabilir.**
- **Outlook gibi yazılımlarda zaman zaman bulunan zaaflar ile mail güvenliğiniz tehlikeye düşebilir.**
- **Bu yüzden otomatik güncelleştirmeleri açık tutmak tavsiye edilir.**

Tehditler- Sosyal Mühendislik

- Sosyal mühendislik kişileri kandırarak değerli bilgi ve parolalarını ellerinden almayı amaçlamaktadır.
- Günümüzde google, bloglar, sosyal ağlar ve daha bir çok yöntem ile hedef kişi hakkında bilgi toplanabilir.
- Günümüzde google, bloglar, sosyal ağlar ve daha bir çok yöntem ile hedef kişi hakkında bilgi toplanabilir.
- Sosyal Mühendislik sanatı kişisel iletişim ve ikna kabiliyeti gerektiren bir iştir.
  - Karşı tarafın şüphesini çekmeden elde edilmek istenilen bilgiyi almak her zaman sanıldığı kadar kolay olmayabilir.
  - Bu yüzden “sabır” çok önemli bir faktördür.

Tehditler- XSRF-CSRF-XSS

- Saldırganın çoğunlukla JavaScript kodunu siteye enjekte etmesiyle ortaya çıkar.
- Saldırganın özel oluşturduğu bir linki kurbana gönderdiğini düşünelim.
  - Kurbanın linke tıklamasıyla JavaScript kodu çalışmaya başlar ve kurbanın cookieleri saldırgana gider, cookieler sayesinde hedef kişinin oturumu yetkisizce çalınabilir.
  - Hedef kişinin oturum bilgileri, saldırganın kurduğu sniffer'da toplanır.
- **Bu tür saldırılarından korunmanın herhangi bir yolu yoktur.**
- **Tek çözüm bilmediğiniz linklere tıklamamanız ve Hex'li url'lere karşı şüpheli yaklaşmanızdır.**

Hex'li url örneği :
http://3513587746@3563250882/d%65f.%61%73p%3F%69d=522

Tehditler- Clickjaking

- Bir browser güvenlik açığıdır.
- Iframe ; Bir web sayfasına zararlı bir web sayfasının (opacity(şeffaflık) değeri=0) olarak gizlenmesidir. Sayfa içinde sayfa mantığıdır.
- Click and Redirect; Normal bir link yerine tıklanış esnasında farklı bir action(yönlendirme) sağlanmış, tuzaklanmış linklerdir.
- Clickjacking ile basit bir web sayfası hazırlayıp, ufak bir sosyal mühendislik senaryosu ile bir formu submit ettirebilir, dolayısı ile XSRF saldırısı gerçekleştirebilir, HTML Downloader, Keylogger gibi yazılımları ile saldırı yapılabilir.
- **Çözümü dikkatli davranmaktır.**

WWW Güvenliği

WWW Güvenliği

- WWW, Web, ya da W3 (World Wide Web), yazı, resim, ses, film, animasyon gibi pek çok farklı yapıdaki verilere kompakt ve etkileşimli bir şekilde ulaşmamızı sağlayan bir çoklu hiper ortam sistemidir.
- Hiper ortam, bir dökümandan başka bir dökümanın çağırılmasına (navigate) olanak sağlar (iç içe dökümanlar). Bu ortamdaki her veri (object), başka bir veriyi çağırabilir .

WWW Güvenliği

- WWW (World Wide Web) kısacası dünyadaki bilgisayarların birbiriyle iletişim kurabildiği, görüntü, ses, veri paylaşımının yapılabildiği global bir ağdır.
- Bu ağa üye olan milyonlarca bilgisayar web sayfalarını düzenleyip belli bir web sunucusu üzerinde yayınlanmaktadır.
- Her bir sitenin kendine ait www ile başlayan bir web adresi vardır.
  - Bu web adreslerini görüntülememize yarayan çeşitli yazılımlar vardır.
  - Bunlara web tarayıcı (Browser) denir. (Internet Explorer, Google Chrome, Mozilla Firefox gibi)

WWW Güvenliği

- Bir Web dokümanına ulaştığımızda her şey 4 ana fazda gerçekleşir:
  1) Bağlantı
  2) Ne istediğimizin web servisine iletilmesi
  3) Cevap
  4) İlgili sayfaya yapılan bağlantının kesilmesi
- Bu ana safhalar, web üzerinde iletişimin kurallarını tanımlayan bir protokolü oluştururlar.
- Bu protokole de, Hyper Text Transfer Protocol (HTTP) denir.

WWW Güvenliği

- Bağlantı safhasında, web erişiminde kullanılan bir web listeleyici (browser, web client), ilgili bilginin olduğu web servisine bağlanır.
  - Bu servislere HTTP servisleri de denir.
- Bağlantı sağlandıktan sonra web istemci programımız http servisine "ne istediğini" bildirir.
  - Bu istek "http", "ftp", "e-mail" gibi bazı protokol kurallarını içerir ve bu işlemlere genel olarak "navigate" de denir.
- Bu isteği alan http servisi de, istediğimiz işlemi yapar ve cevabı bize gönderir.
  - Biz de gelen cevabı web istemci programımızda görürüz.
  - Eğer istek gerçekleştirilemiyorsa bir hata mesajı ile karşılaşırız.
- Son safhada ise, http servisine yaptığımız bağlantı kesilir.

WWW Güvenliği

- Günümüzde World Wide Web (WWW),güncel ve doğru bilgiyi insanlara ulaştırmak için en kolay ve en etkin yöntem olarak karşımıza çıkmaktadır.
- Kurulan bir web sunucusu ve içine hazırlanan site içeriği üzerinden, kurumunuz hakkında bilgiyi sunabilir ve ticaret yapabilirsiniz.
- Web sitesi saldırıları (web defacement) her geçen gün artmaktadır.
  - Bunun nedeninin web sitesi güvenliğinin yeterince ciddiye alınmaması olduğu düşünülmektedir.
- Yine WWW üzerinde girdiğimiz kişisel bilgiler de saldırganlar tarafından kolaylıkla elde edilebilir durumdadır.

WWW'de Korunma Yöntemleri

- %100 güvenmediğiniz sitelerden program indirmeyin, bu programları kullanmayın.
- Tanımadığınız kişi veya kurumlardan gelen e-postalardaki ekli dosyaları açmayın,chat gibi güvensiz yollarla gelen dosyalar almayın.
- Bilmediğiniz veya güvenliğinden emin olmadığınız sitelere kişisel bilgilerinizi kesinlikle vermeyiniz.
- İnternet üzerindeki güvenlik ile ilgili konu ve bilgileri yakından takip ediniz. İşletim sisteminizi ve programlarınızı korumak için yeni teknolojileri kullanınız.
- Bankaların Internet şubelerinde ya da kimlik doğrulaması yaparak giriş yaptığınız tüm sitelerde işlemlerinizi sona erdirdikten sonra mutlaka "Güvenli Çıkış" butonunu kullanın.

WWW'de Korunma Yöntemleri

- Kredi kartınızı kullandığınız ya da kişisel bilgilerinizi yazdığınız bilgisayarın güvenli olmasına dikkat edin.
  - İnternet cafe gibi yerlerde bu tarz bilgilerinizi kesinlikle girmeyin.
- Kullanmakta olduğunuz işletim sisteminiz ve tarayıcı programınız için üretici firma tarafından yayınlanan güvenlik güncelleştirmeleri ve yamalarını mutlaka kullanın.
  - Microsoft Internet Explorer kullanıyorsanız, Microsoft Security ana sayfasından www.microsoft.com/security/ 'den konu ile ilgili özel güvenlik ayarlarını yükleyin.
- Trojanların, virüsler gibi, tamamen masum programlara iliştirilebileceğini unutmayın. İstediğiniz program bilinen ve saygı duyulan bir şeyse bile, kişisel sayfalardan ziyade, yapımcının sayfasından edinin.

WWW'de Korunma Yöntemleri

- Bilgisayarınızı risklerden korumanın en önemli yollarından birisi de bir Kişisel Firewall yazılımı edinmektir.
  - Firewall (ateş duvarı) ile bilgisayarınız ile art niyetli kullanıcılar arasına bir set çekilmiş olur.
  - Temelde hem şüpheli haberleşmeyi kısmen engellemek, hem de şüphesiz haberleşmelere izin vermek gibi bir fonksiyonu yerine getirir.
  - Bir başka deyişle Firewall, e-posta da dahil olmak üzere pek çok kanaldan size ulaşan bilgi ve belgeleri kontrol eder ve uygun olmayan ya da şüpheli bilgi girişini engeller.

WWW’de Korunma Yöntemleri

- İnternet'te paylaşmanız gerekenden fazlasını paylaşmayın. Gerçekten ihtiyacınız olmadıkça 'File and Printer sharing' gibi şeyleri yüklemeyin.
- Bir network üzerindeyseniz ve dosyalarınızdan bir kısmını paylaşıma açmak zorundaysanız, onları şifre korumalı olarak paylaştırın.
  - 'ky8xdj33bgyt67' gibi uzun ve rasgele bir şifre kullanmalı ve düzenli olarak değiştirmelisiniz.
- Erişmek istediğiniz web sayfasının adresini tarayıcınızın adres satırına kendiniz yazın.

WWW'de Korunma Yöntemleri

- İnternetten indirdiğiniz her dosyayı çalıştırmamalı ve her soruya "Yes" ya da "Evet" butonuna tıklayarak cevap verme alışkanlığına son vermelisiniz.
  - Hatta son zamanlarda "No" ya da "Hayır" tuşuna basmakla da bu programların kendiliğinden yüklenebilmektedir.
  - Pencerenin sağ üst köşesinde yer alan "X" yani pencereyi kapa düğmesine tıklamak en garantili yol gözükmektedir.
- Müzik, resim, film indirmek istediğinizde uzantılara dikkat etmelisiniz.
  - ".exe" uzantısı gördüğünüzde indirmeyip o siteyi kapatmalısınız.
  - Çünkü dialer programları sadece tıklama yapıldığında değil, siz o sayfayı açtığınızda hiçbir yere tıklamasanız da bilgisayarınıza kendiliğinden yüklenebilmektedir.