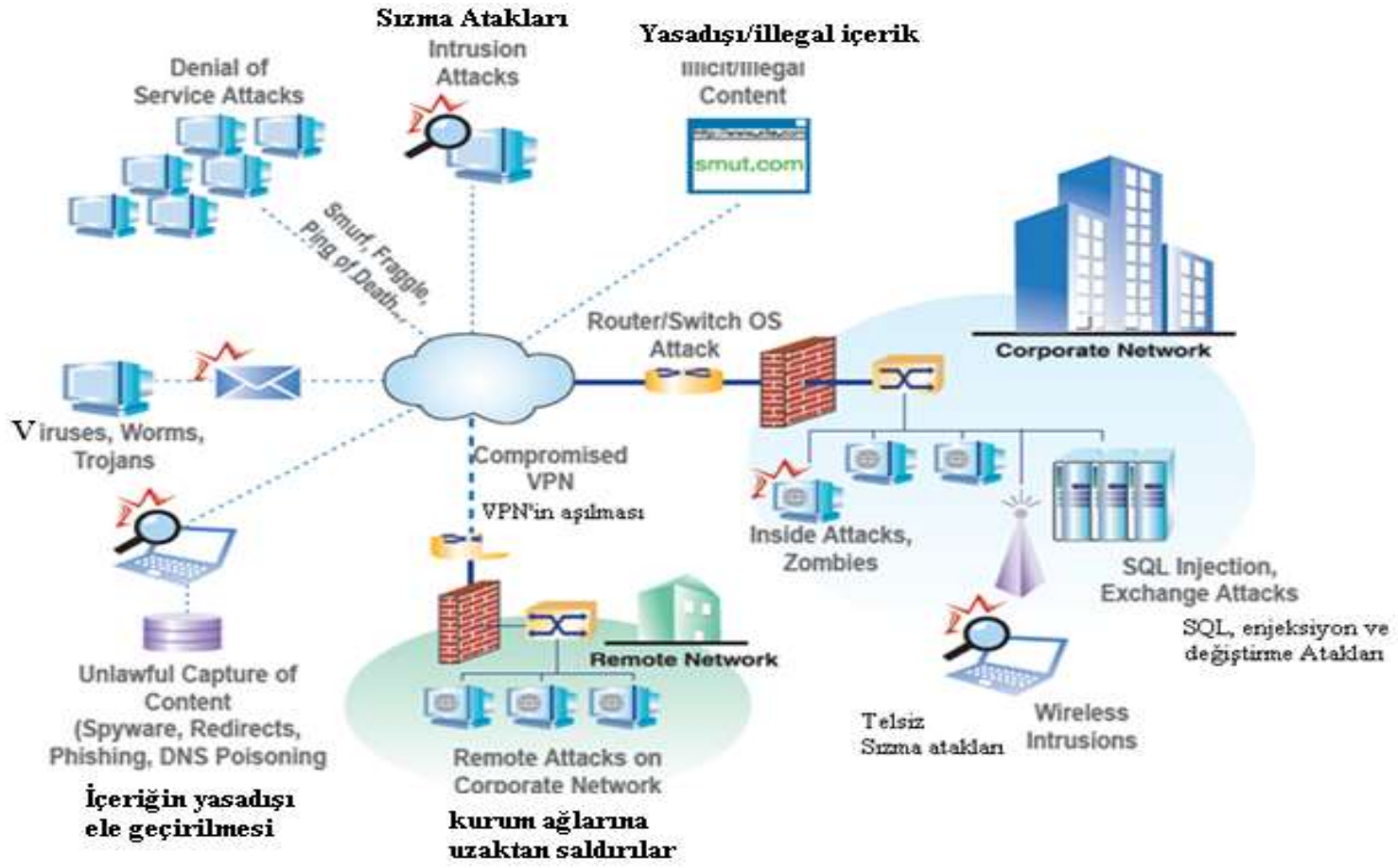
Ağ Güvenliği Dersi (2017-18-Güz)

2.hafta

Günümüz ağ ortamında yaygın tehditler



Virüs: *Belleğe yerleşerek, çalışan programlara kendisini ekleyebilen ve sürekli çoğalabilen zararlı programcıklardır.*

Bilgisayar virüsleri,

*** bilgisayarın çalışmasını engelleyecek,**

***verileri kaybedecek, bozacak veya silecek**

***kendilerini Internet üzerinden diğer bilgisayarlara yayarak yavaşlamalara neden olacak**

şekilde tasarlanmışlardır.

Virüs'ler e-posta, veri taşıma ortamları (disket, cd, dvd vb.) ve web sayfaları ile yayılabilir (Melisa, CIH, Gauss). yazılım programlarıdır.

Günümüz ağ ortamında yaygın tehditler

Worm (Solucan):

*IP adreslerini rastgele tarayarak, internete bağlı kullanıcıların yerel ağ için paylaşıma açık dosyalarının olup olmadığına bakarlar. Yazmaya açık dosya bulduğunda kendisini oraya yazar.

*Worm bir sızma ve çoğalma mekanizmasıdır.

Worm'lar, Virüs'lerin kullandıkları yöntemlere ek olarak, uygulama / işletim sistemi zayıflıkları ile saldırılar düzenleyebilir ve bu şekilde de yayılabilir (Code Red, Nimda, Sasser, Blaster).

Solucanlar yayılmak için bir "taşıyıcı" programa veya dosyaya gereksinim duymadıklarından, sisteminizde bir tünel de açabilir ve başka birinin uzaktan bilgisayarınızın denetimini eline geçirmesini sağlayabilir.

Trojan (Truva atları):

Bulaştıkları bilgisayarlardaki şifreleri, dosyaları veya herhangibir veriyi ele geçirmek üzere tasarlanmışlardır. Virüslerden ayrıldıkları temel nokta, verilere zarar vermekten çok casusluk yapmalarıdır.

Trojanlar sonradan bilgisayarımıza girerek, yazarı tarafından belirtilen portu açan veya yazarın belirlediği bir mail adresine veya v.b yazarın istediği bilgileri aktaran programlardır (Kredi kartı no, key log'ları, dosya bilgilerimiz v.b v.b).

Trojan'lar ancak ilgili uygulama çalıştırıldığında etkili olmaktadır (Netbus, Subseven).

Denial of Service Atakları

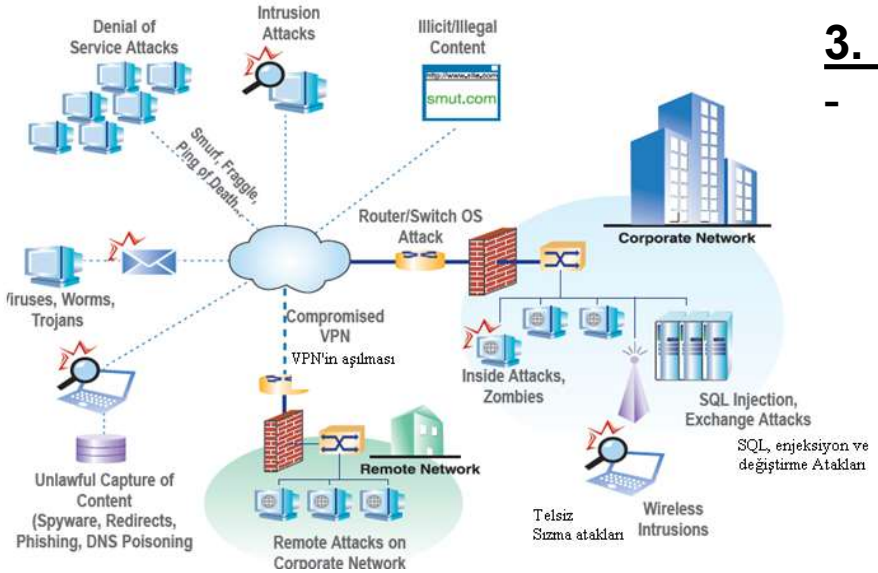
DoS (Denial of Services - Servis Dışı Bırakma) atakları temel olarak sistem kaynaklarını veya bant genişliği tüketerek servislerin hizmet dışı bırakılmasıdır. Bu atakların amacı bilgiyi çalmak değildir. Bu atakları 3 başlıkta toplamak mümkündür.

1. DoS - Denial Of Service :

-Paket direk olarak hedef sistem gönderilir.
-Tek bir kaynaktan tek bir hedefe yöneliktir.

2. DDoS - Distributed Denial of Service :

-Zombi kaynaklardan tek bir hedefe çoklu ataklardır.
-Anlık gönderilen paket sayısı zombilerin sayısı ile doğru orantılıdır.
-Çoğunlukla saldırıyı yapan kaynak tespit edilemez.



3. DRDoS - Distributed Reflective DoS:

- DDoS'tan farklı olarak daha sık ataklar için ek ağlar kullanır

4 çeşit temel DoS atağı vardır:

1. TCP/IP uygulamasındaki kusurları istismar eden ataklar: Örneğin Ping of Death ve Teardrop.

Ping-of-Death :Çok büyük boyuttaki (genelde 65,536 dan daha büyük) ICMP paketleri direk olarak hedefe gönderilir. Paketin büyüklüğüne göre sistemin donmasına, çökmesine yada reset atmasına sebep olabilir.

TearDrop :Parçalanmış UDP paketleri bozuk ofsetler ile hedefe gönderilir. Hedef paketleri tekrar birleştirmeye çalıştığında bozuk veya hatalı bir paket üretmiş olur ve sistem çöker.

2. TCP/IP'deki zayıflıkları kullanan ataklar. Örneğin SYN Flood ve LAND atakları.

SYN Flood :TCP'nin 3 yollu handshake açığını kullanır. Kaynak (Saldıran) SYN paketlerini hedefe gönderir.(1. el sıkışma) . Hedef SYN paketine SYN ACK olarak cevap verir (2. el sıkışma). Saldıran (Kaynak) gelen pakete cevap vermeden yeni bir SYN paketi yollar ve hedef sürekli cevap bekler konumda kalır.

Land Attack :Kaynak ve Hedef adresi değiştirilmiş paketlerdir. Paket içerisindeki kaynak ve hedef gönderilecek hedef adresidir. Paket hedefe ulaştığında hedef kendi paketini sürekli cevaplayarak çöker.

3. Brute-force (Kaba kuvvet) atakları: Web yazılımlarının login kısımlarına yapılan deneme yanılma yöntemidir. Bu işlem yazılmış olan programları kullanılarak otomotik bir şekilde yapılır. Sürekli login sayfasına atak yapılarak deneme yanılma yöntemiyle bir kullanıcı adına ait şifreyi bulmak ve yönetimi ele geçirmektir. Bu tip ataklar networkü gereksiz data ile istila ederler. Örneğin Smurf atağı.

Smurf :ICMP paketlerindeki kaynak adresi değiştirir. ICMP paketlerini zombilere gönderir. Zombiler paketleri hedefe yollar. Hedef kendisinin göndermediği bir sürü cevap mesajları alarak şişer.

4. IP Spoofing (IP Sahtekarlığı) : Sistemlere girmek için, saldırganın kimliğini gizleyebilmesi için veya DoS atağının etkisini büyütmek için kullanılır. Saldırganın kendisini gizleyebilmesine sebep olan şey, HTTP, DNS gibi Internet servislerinde, IP numaralarını doğrulayacak bir denetim (authentication) bulunmamasıdır. IP spoofing'de, saldırgan, IP paketlerine kendi gerçek IP numarası yerine, var olmayan bir IP numarasını veya kurban sitenin numarasını koymaktır. Zombiler veya kurban siteler bu paketlerdeki gönderen IP numarasını doğrulayamadıkları için saldırgan kendisini gizleyerek istediği siteye saldırabilmektedir. Bu saldırının temel alındığı DDoS saldırıları **SYN-flood , smurf** v.b

İntrusion Attacks (Sızma Atakları)

Bir ağ ortamında, ağ kaynaklarına izinsiz erişim yapan veya yapmaya çalışan, sistemi kötüye kullanan kişiler saldırgan kapsamındadır. **Bunlara cracer veya hacker denir.**

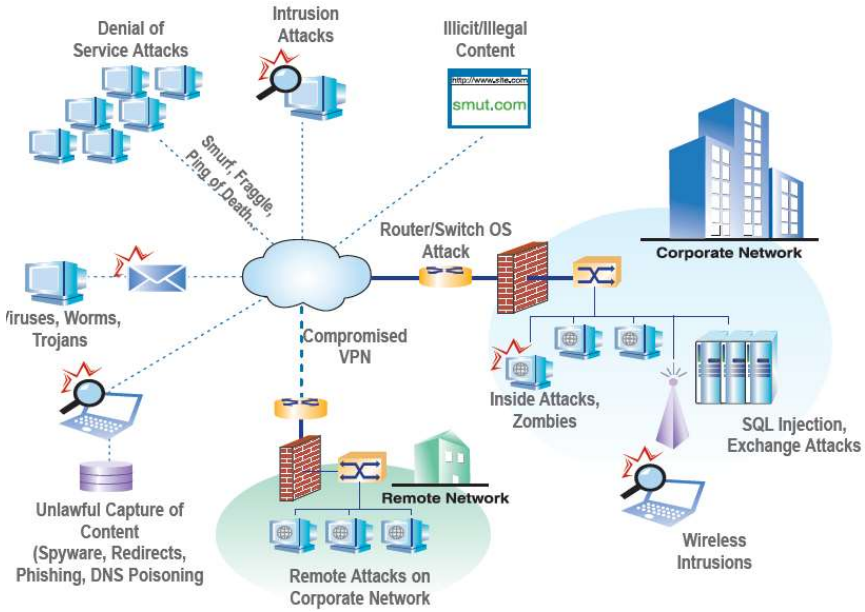
Saldırısını sonuçlandırarak sisteme girmeyi başaran saldırgana ise sızan-nüfüz eden (intruder) olarak tanımlanır. Sızma işleminin sonucunda; sistemde yetkisiz kullanım, kaynaklara izinsiz erişim, bilgi çalınması, sadece sistemi meşgul ederek servis dışı kalması gibi kötü olaylar oluşur.

Sisteme sızma için gerçekleştirilen ataklara ise intrusion attacks (Sızma Atakları) denir.

İLLEGAL CONTENT (yasadışı içerik)

Yasadışı içerik tanımı ülkeden ülkeye değişir. Özellikle internet üzerinden yapılan illegal içerikli en yaygın yayınlardan bazıları ;

- Pornografi görüntüleri ve web siteleri
- Yasadışı faaliyet sohbet odaları
- Online nefret ve yabancı düşmanlığı web siteleri



ZOMBİ'ler (İç atak)

Zombi'ler hacker tarafından sistem açığı bulunarak hacklenilen ve aynı zamanda pc'deki tüm kişisel bilgiler, iletişim ve veri ağının takip edilmesine açık bilgisayarlardır. Trojanın bulaştığı PC'ler Zombi adayıdır.

Zombiler genellikle güvenliği zayıf olan sistemlere yerleştirilirler. Hack'lenen sisteme yerleştirilen zombiler, belirli bir porttan (1524 tcp, 27665 tcp, 2744 udp, 31335 udp, 33270 tcp) gelecek olan DDoS isteklerini gerçekleştirirler.

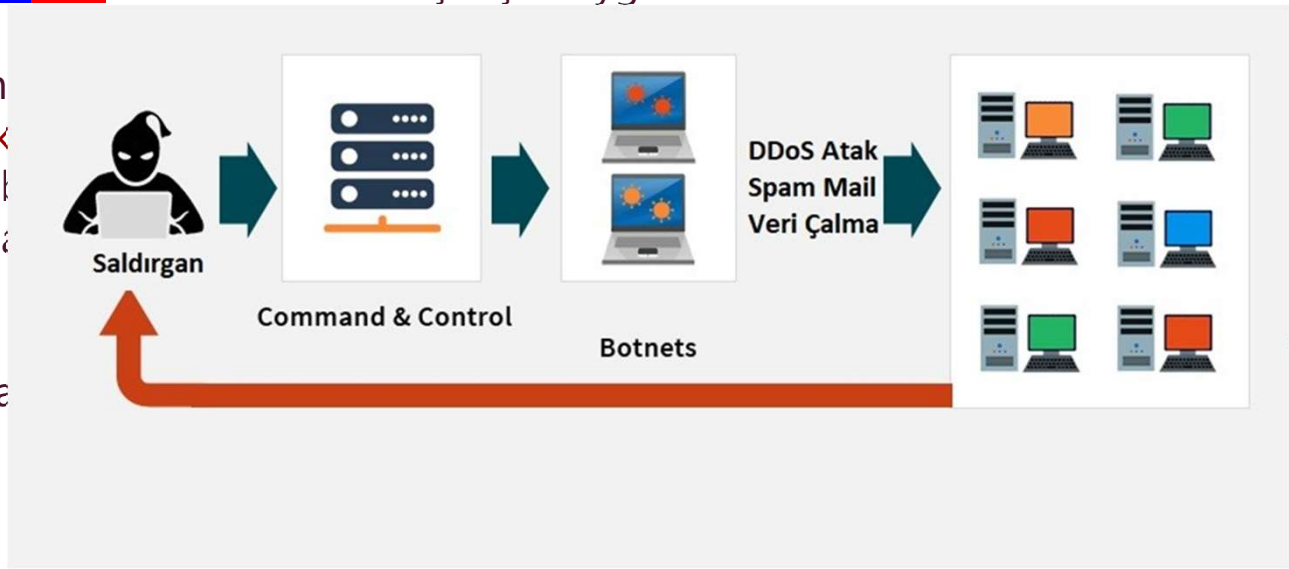
Unix , Linux, Windows tabanlı sistemlerdeki zombiler, DDoS ataklarını gerçekleştirirken yakalanmamak için kullanılır.

BOTNET (roBOTNETwork)

Botnet, hacker tarafından, trojanlar'ın çeşitli ve çok sayıda bilgisayar sistemlerine bulaştırılarak bu bilgisayardaki yetkilere sahip olması olarak tarif edilebilr. Bir botnet trojanı sisteme bulaştıktan sonra artık o bilgisayar bir zombiye dönüşerek botnet ağının bir üyesi olmuştur ve botnet ağ yöneticisinin her istediğini yapmaya hazır hale gelmektedir. DDOS için kullanılan Botnet virüslerin CPU kullanımları fazla olmadığı için kullanıcı tarafından fark edilmez. Botnetteki her bilgisayar bir BOT veya Zombi'dir. Botnet ağındaki tüm zombiler, sadece bir bilgisayardan (hacker) komut verilerek yönlendirilir.

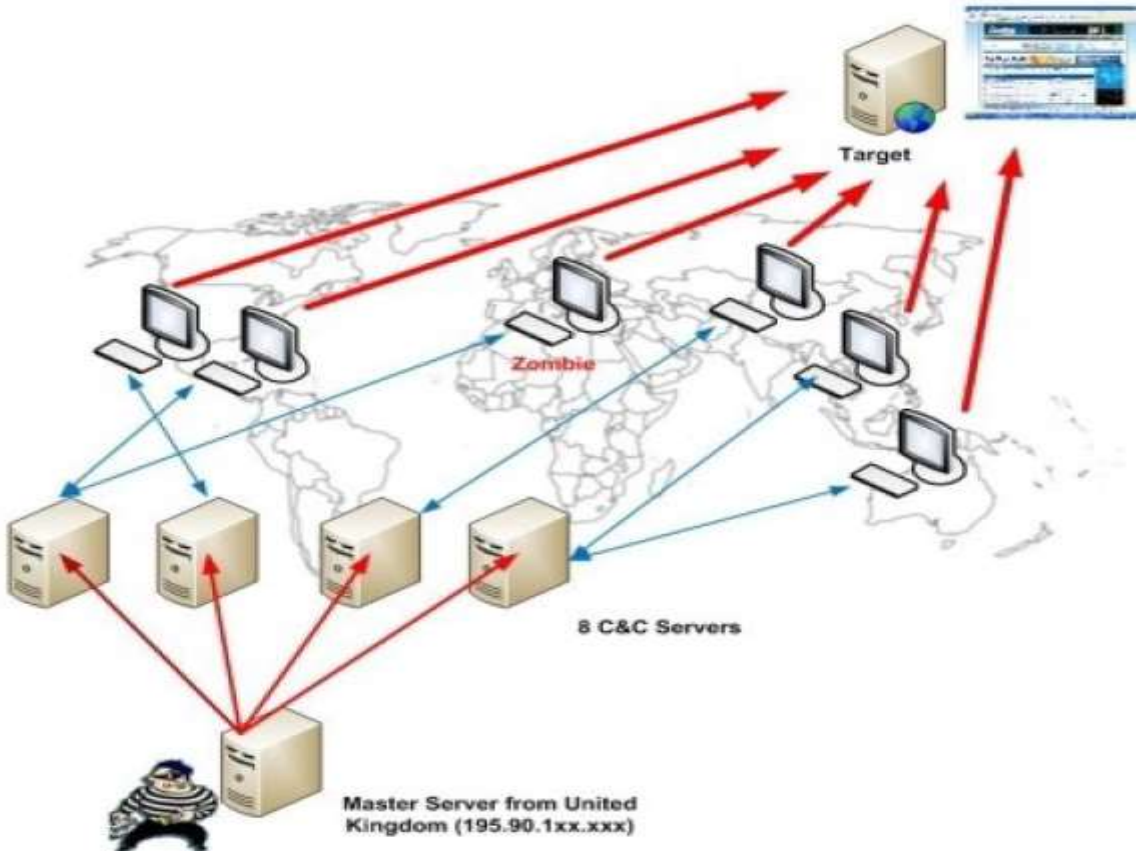
Botnet'ler, DDOS Saldırıları için çok uygundur.

•Zom
•Uzak
•Sahil
•Her a
•Tüm
•Tüm
yapıla



komutla

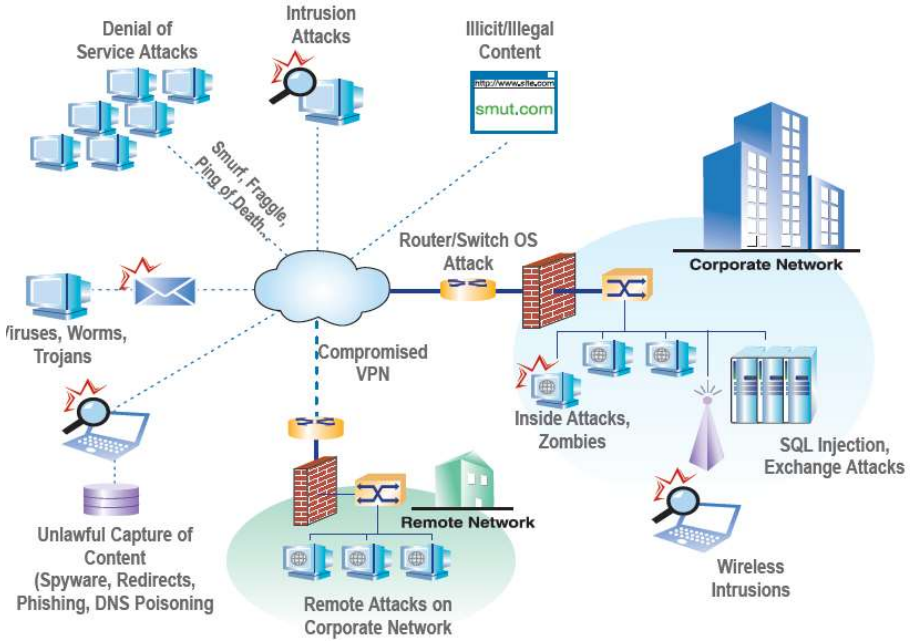
BOTNET DDOS saldırı şematiği



SQL İnjection (SQL Atakları)

Sql Injection atakları, web uygulamalarında yer alan veri girişleri için kullandığımız TextBox form elemanlarının içine yazılan bazı sql komut deyimlerinin yazılması ile olur.

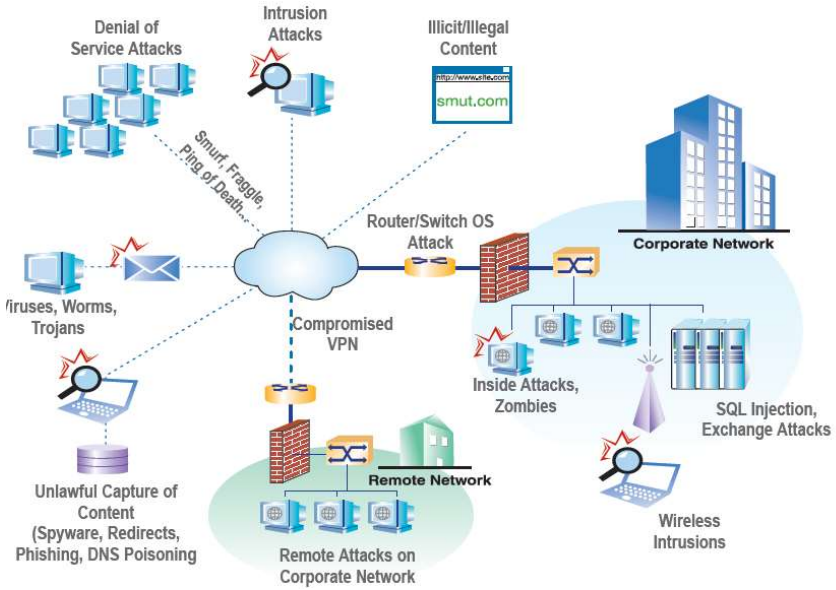
Web uygulamalarının en zayıf bölümü kullanıcı girişlerinin yapıldığı ve sonucunda yetkilendirme yapıldığı bölümlerdir. Buradan yapılan kaçaklar ile veri tabanında istenmeyen işlemlerin yapılması sözkonusudur.



İçeriğin Kanunsuz olarak ele geçirilmesi (Unlawful capture of content)

DNS Önbellek zehirlenmesi, bir DNS sunucusuna yetkisiz bir kaynaktan veri yüklenmesine verilen genel isimdir. Hatalı yazılımla, yapılandırma hatalarıyla ya da DNS protokolünün açıklarıyla başarıyla iletilen özgün olmayan veri, saldırılan sunucunun önbelleğine gelir ve böylece önbellek "zehirlenmiş" olur.

Bu tür saldırılar, sorgu yapıldığında asıl yanıt vermesi beklenen DNS sunucusundan önce saldırganın yanıt vermesi esasına dayanır.



Spyware (Spy software) (Casus) programlar bilgisayarınızda casusluk yapmak için yaratılmış programlardır. Tam anlamı ile virüs olarak adlandırılamayan bu programların temel amaçları kuruldukları bilgisayarda bilgi toplamak ve bu bilgileri bu programları yaratan kişilere göndermektir. Spyware (casus) programların tehlikeli olan türevleri sizin bilgisayar ve/ya internet ayarlarınızı kendi istedikleri gibi değiştirirler ve sizleri kendi istedikleri sitelere yönlendirirler.

Redirect (URL-Redirect): Bir URL'e gelenleri başka bir URL'e iletme işlemi yönlendirmedir. Birçok sebep için yönlendirmeler kullanılmaktadır.

Dns Poisioning (DNS zehirlenmesi): Yanlış DNS bilgileri Birincil DNS sunucuya tanıtılır. Tüm istekler değiştirilmiş DNS sunucusuna yönlendirilir

AĞ güvenliğine katmanlı bakış

Güvenlik seviyesi Security level	Uygulanabilir güvenlik önlemleri Applicable security measures
1. Perimeter (Geniş kapsamlı - Çevresel)	• Firewall (Ateş duvarı) • Network-based anti-virus (Ağ temelli anti-virüs) • VPN encryption VPII şifreleme
2. Network	• Intrusion detection/prevention system (IDS/IPS) (Saldırı tesit/Önleme Sistemi) • Vulnerability management system (Güvenlik açığı yönetim sistemi) • Network access control (Ağ erişim kontrolü) • Access control/user authentication (Erişim kontrol/Kullanıcı kimlik doğrulaması)
3. Host	• Host IDS (Host saldırı tespit sistemi) • Host vulnerability assessment (VA) (Host güvenlik açığı değerlendirmesi) • Network access control (Ağ erişim kontrolü) • Anti-virus Anti-virüs • Access control/user authentication (Erişim kontrol/Kullanıcı kimlik doğrulaması)
4. Application	• Application shield (Uygulama koruması) • Access control/user authentication (Erişim kontrol/Kullanıcı kimlik doğrulaması) • Input validation (Giriş Doğrulama)
5. Data	• Encryption (Kripto) • Access control/user authentication (Erişim kontrol/Kullanıcı kimlik doğrulaması)

Güvenlik Seviyelerine katmanlı bir yaklaşım ve her katmanda uygulanacak teknolojik fonksiyonlar.

Level 1- Çevresel (Bütünsel) Güvenlik seviyesi

- Çevresel güvenlik, güvenli olmayan ağlarda savunmanın ilk basamağıdır.
- Çevresel güvenlik ,bir ağı korumak için ilk (giriş) ve son(çıkış) temas noktası olarak değerlendirilir.
- İç ağın dış ağdan ayrıştığı bir yer olarak değerlendirilir. Ağın dünyaya açıldığı kapısıdır.
- Çevresel (perimeter) güvenlik bir veya birkaç firewall'dan ve bölgelerden oluşur.
- Network'te çevresel güvenlik için, FİREWALL, Ağ Tabanlı anti-virüs yazılımları, VPN şifreleme gibi teknolojiler kullanılır.

Firewall - Güvenlik duvarı

- Firewall - Güvenlik duvarı, genellikle bağlı bir sunucu üzerinde yüklü bir yazılımdır veya donanımsal bir kutudur.
- İç ve dış ağı biribirnden ayıran noktadır. Genellikle iç ağı dış ağdan korur.
- Güvenlik duvarı üç genel işlevleri gerçekleştirir;
  1) Trafik kontrol,
  2) Adresi çevirisi (NAT),
  3) VPN (Virtual Private Network) sonlandırma.

- Güvenlik duvarı, gelen ve giden trafikteki hedef ve kaynakları inceleyerek sadece izin verilen trafiğin akışını sağlar.
- Ayrıca, güvenlik duvarları iç IP adreslerini farklı IP adreslerine çevirerek iç ağı Internetten koruyabilir.
- Güvenlik duvarı, VPN tünelleme işlemini yaparak, genel bir ağ üzerinden şifreli bir yol elde edilmesini sağlayabilir.
- Bu yetenekleri, bir güvenlik duvarını ağ güvenliği için bir vazgeçilmez parça yapar.

Ağ tabanlı anti-virüs (Network-based anti-virus)

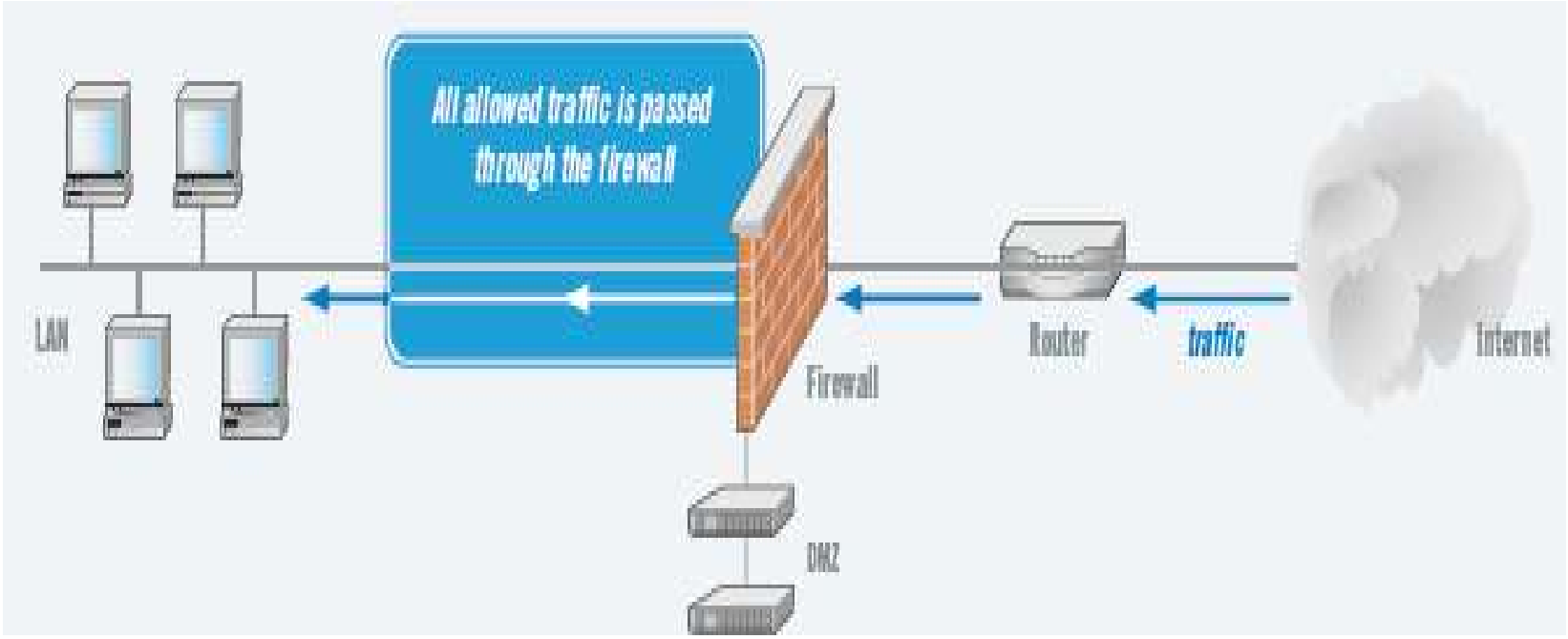
- DMZ'de Yüklü, ağ tabanlı anti-virüs yazılımı gelen ve giden e-posta mesajını, içeriği bilinen bir virüs profilleri veritabanı ile karşılaştırır.
- Ağ tabanlı antivirüs ürünleri, şüpheli ve virüslü e-posta mesajları karantinaya alır ve virüslü e-posta trafiğini engeller. Bu durumu alıcılara ve yöneticilere bildirir.
- e-posta sunucusu üzerinde yapılan bir Ağ tabanlı anti-virüs koruması, bireysel masaüstü bilgisayarlar için bir tamamlayıcı etkendir.
- Bu işlem e-posta ile giren bir virüs ile enfekteyi ve virüslü e-maili'in ağ üzerinden yayılmasını önler.
- Etkin çalışması için, veritabanının güncel virüsleri tanıması gerekir.

Özel Sanal Ağ (Virtual private network (VPN))

- VPN - Sanal özel ağ (VPN), dizüstü bilgisayarlar, ve hedef ağ gibi uzak cihazlar arasında güvenli bir bağlantı oluşturmak için yüksek düzey bir şifreleme tekniği kullanır.
- Aslında özel ağın güvenliğine ve gizliliğine yaklaşılan bir uygulamadır. Internet(Genel bir ağ) üzerinden şifreli bir haberleşme şekli olarakta düşünülebilir.
- VPN tüneli, DMZ içinde bir VPN-etkin yönlendirici, güvenlik duvarı, ya da sunucu üzerinden sona erdirilir.

Çevresel güvenlikle ilgili

- Kullanılan ağın karmaşıklığı, çevresel güvenlik teknolojilerinin etkinliğini etkiler. Yani Birden fazla dış bağlantı durumu, büyük olasılıkla birden fazla güvenlik duvarını ve anti-virüs yazılımlarını gerektirebilir.
- Karmaşık mimarinin tek bir noktadan korunabilmesi için kullanılan teknolojilerde mevcuttur.



Çevresel güvenliğin pozitifleri

- İyi kurulmuş ve konfigüre edilmiş çevre düzey teknolojileri, uzun yıllar kullanılabilir ve iyi IT profesyonellerinin yetenekleri ve işletme bilgilerine gereksinim duyar. Aynı zamanda onların tecrübesinide arttırır.

- Bunun için , üreticiler makul fiyatlı, etkin uygulamalı yazılım ve donanım seviyesinde çözümler geliştirip sunuyorlar.

Çevresel güvenlikle ilgili olarak Dikkat edilecek konular

- Bir anti-virüs yazılımı, veritabanında olmadığı sürece bir virüsü tespit edemez.

- VPN etkili şifreleme, sağlamasına karşın , şifreleme gibi, BT personelinin idari bir yük bindirip tuşları ve kullanıcı gruplarının sürekli olarak yönetilmesi gerekir.

- Ayrıca VPN'ler sizi enfekte olmuş cihazlardan koruyamaz, veya VPN bağlantısı kullanarak, kötü niyetli trafiği önleyemezsiniz.

- DMZ’de bulunan cihaz türleri de önemli bir faktördür. Ayrıca ağda yaptığınız işin önemide bu cihazlarla ilgilidir. Işiniz önemi ve kritikliği ne kadar yüksek ise , çevresel güvenlikten daha sıkı güvenlik önlemleri ve politikaları ve cihazları uygulanmalıdır.

Level2- Ağ güvenlik seviyesi

- Katmanlı yapıdaki ağ güvenliği seviyesi; biribiriyle iletişim içindeki LAN ve WAN sistemlerini kasdeder. Uzak LAN'ların FrameRelay v.b servislerle biribirine bağlantısı buna dahildir.
- Çoğu ağlar bugün oldukça saldırıya açık bir yapıdadır. Ağ içine sızıp hiçbir engele takılmadan istediğiniz işlemi yapabilirsiniz.
- Bu durum internete bağlı orta ölçekli ağları saldırganların kolay ve cazip bir hedefi haline getiriyor.
- Ağ seviyesinde güvenlik için,

  a-) ***IDS (Saldırı tespit sistemleri),***

  b-Güvenlik açığı yönetimi,

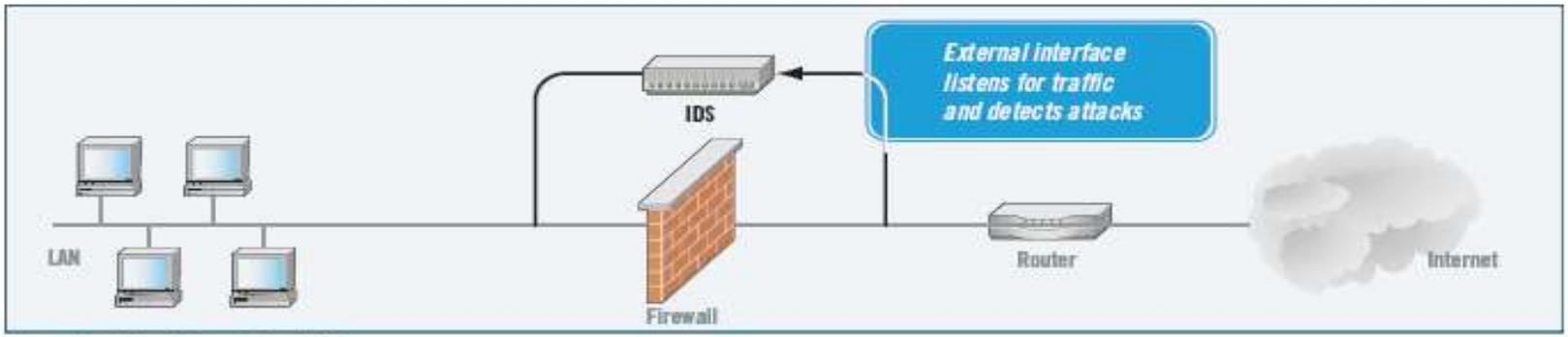
  c-) ***ağa erişim teknolojileri,***

  d-) ***Erişim kontrol ve kimlik doğrulama*** teknolojileri kullanılabilir.

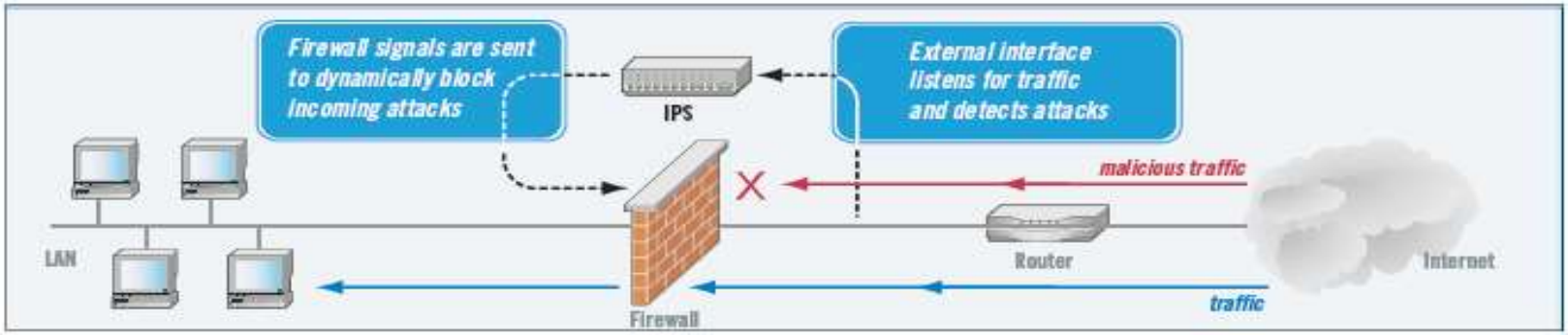
Level 2: IDS-IPS'ler

- Saldırı Tespit Sistemleri (Intrusion detect sysytems – IDS -STS) ve Saldırı Önleme Sistemleri (Intrusion Prevention systems- IPS-SÖS) , ağınızdaki hareketli trafik analizi açısından ***güvenlik duvarı*** 'na oranla çok daha fazla ayrıntı verir.
- IDS'ler saldırıları uyarır.
- IPS'ler saldırıları belirler ve engeller.
- IDS ve IPS cihazları, çalışma prensibi olarak anti-virüs sistemine benzerdir. Yani trafik analizi ve paketler bilinen saldırı profillerinin tutulduğu veritabanı ile karşılaştırılır.

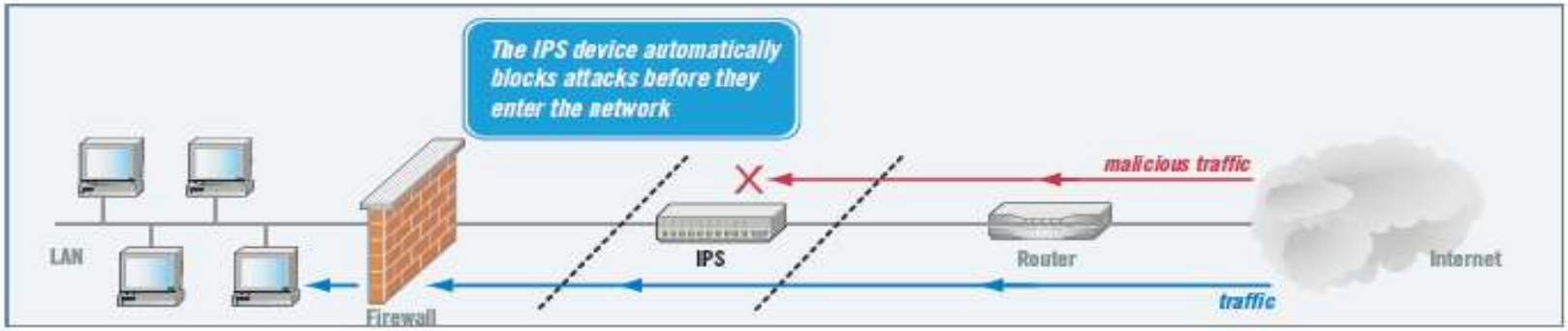
- Ati-virüsler dosyaları, IDS'ler paketleri inceler.



Intrusion detection system (IDS)



Intrusion prevention system (out-of-band configuration)



Intrusion prevention system (in-line configuration)

Figure 3. Typical IDS/IPS installations

Level 2: Güvenlik açığı yönetimi

İki farklı fonksiyonu gerçekleştirir.

1- Ağı güvenlik açıkları için sürekli tarar.

2- Güvenlik açıklarının giderilmesi sürecini yönetirler.

- Güvenlik açıklarını giderici gelişmiş cihazlar piyasada mevcuttur.
- Güvenlik açığı yönetici cihazları korsanlardan önce güvenlik açıklarını bulup giderebilmelidir.
- Daha çok bilinen açıkların var olup olmadığı konusunda etkendirler.

Level 2: Network access control (Ağ erişim kontrol)

- Ağ erişim kontrol çözümleri, önceden tanımlanmış ve müsaade edilmiş ağ uç noktalarına (Sunucular, network cihazları v.b) girişleri kontrol etmek üzerinedir.
- Bu da ağ üzerinden ***'içerden'*** saldırıya uğrayabilecek, tehlikeye açık masaüstü ve dizüstü bilgisayarlar, yüklenici makineleri, VPN ve RAS aygıtlarını korumak içindir.

Level 2: Access control/authentication

- ***Erişim kontrol / kimlik doğrulama*** , Ağa Erişmek isteyen kullanıcılar için kimlik doğrulama kontrolu gerektirir.

  Erişim kontrolu üç aşamalı olarak gerçekleştirilebilir. Bu kontrol hostlar için de kullanılır.

  1.Tanımlama (Identification)

  2.Kimlik Sınama (Authentication)

  3.Yetkilendirme (Authorization)

- Kimlik Doğrulama genellikle RADIUS, LDAP, ya da Windows Active Directory'deki kullanıcı bilgilerine karşı gerçekleştirilen erişimler için yapılır.

Ağ güvenlik seviyesinin pozitifleri

- IDS, IPS, ve güvenlik açığı yönetim teknolojileri, gerçekleştirmek ağ tehditleri ve güvenlik açıklarının analizleri için önemli ve yeni analizlerin başarılmasına yol açar.
- Güvenlik duvarı sonuçta, hedefe ait trafiğe izin veren veya vermeyen kaba bir analiz yöntemi olmakla beraber, IPS ve IDS araçları çok daha derin bir analiz yapar ve dolayısıyla daha iyi koruma sağlar.
- Bu ileri teknolojiler sayesinde, bir legal network trafiğindeki gömülü ataklar, ki onlar bir güvenlik duvarı üzerinden - tespit edilebilir ve hasar meydana getirmeden önce potansiyel olarak - iptal edilebilir.

Ağ güvenlik seviyesinin pozitifleri

- Güvenlik Açığı yöneticileri, bir ağdaki güvenlik açıklarını kontrol sürecini otomatikleştirmek için kullanılırlar.
- Bu tür kontroller manuel olarak yapılsaydı – güvenliği sağlamak için gerekli olan çalışma- pratik olmazdı. Ayrıca, ağlar dinamiktir. Yeni cihazlar, uygulama yükseltmeleri ve yamalar, ve kullanıcı ekleme ve çıkarma, yeni güvenlik açıkları tanıtmak v.b.
- VA (Vulneratibilty assestment – Güvenlik açığı değerlendirme) araçları, yeni tanıtılan ağ için sık sık ve iyice güvenlik açıkları taraması sağlar.
- Ağ erişim kontrolü çözümleri, ağ içine tehlikeli bir *arka kapıları* kapatmak açısından da çok önemlidir.

DİKKAT EDİLECEK HUSUSLAR

- Ağ düzeyi güvenlik önlemlerinin başarısı biraz dahili ağ bağlantı hızına bağlıdır. Çünkü, IDS / IPS, güvenlik açığı yönetimi ve ağ erişimi/ kimlik kontrol araçları korunacak ağların kaynaklarını tüketir.

- Artan bağlantı hızları , genel ağ performansı üzerinde bu koruma performansını düşürür.

- Bu teknolojilerin uygulanmasında geliştirilmiş güvenlik ve fiyatlandırma ilişkisini düşünmek gerekir.
- Bu ürünlerin çoğu sürekli olarak yönetilmesi gereken, kullanım kolaylığı , etkin bir şekilde gerçekleştirme, ağ üzerinde rahat hareket, ölçeklenebilme gibi özellikleri gözetilmelidir.

Level3- Host Güvenliği

- Katmanlı güvenlik modelinde, Host seviyesi ile bireysel cihazlar, sunucular, masaüstü bilgisayarlar, switchler, routerlar gibi cihazların güvenliği kasdedilir.

- Host seviyesi güvenliği; **Host tabanli saldırı tespit sistemleri (IDS)**, ***Host-tabanlı güvenlik açığı değerlendirmesi (VA)***, ***Network erişim kontrolu***, ***anti-virüs yazılımları***, ***Erişim kontrolü / kimlik doğrulama*** gibi teknolojilerle sağlanır.

Host-based intrusion detection systems (IDS)
(Host temelli saldırı tespit sistemleri (IDS))

- Ana bilgisayar tabanlı(host) IDS'ler, ağ IDS'lerine benzer şekilde çalışırlar. Tek farkı biri ağ trafiğini biri host trafiğini izler.

- Ana bilgisayar tabanlı IDS'ler belirli operasyonel özellikleri , ince ayarlanma özelliği ile doğru uygulandığında yüksek dereceli güvenik sağlar.

Host-based vulnerability assessment (VA)
(Host-tabanlı güvenlik açığı değerlendirme (VA))

- Host-tabanlı VA araçları, güvenlik açıkları için tek bir ağ aygıtını tarar.
- Host-tabanlı VA araçları ince ayarlı ve son derece doğru monitör cihazlarıdır.
- Bunlar son derece doğru olarak ve en az performansla host kaynaklarını tararlar.
- Sadece Host cihazları için üretildiklerinden, düzgün bir şekilde yönetildiklerinde mükemmel bir kapsama alanı sunarlar.

Ağ erişim kontrolu – (Network access control)

- Ağ erişim kontrol çözümleri çifte görev üstlenirler. Hem ağ korunması olarak (önceki bölümde) hemde bireysel host cihazları için.

- Bu çözümler, ana makinayı, zararlı uygulamalar ve enfeksiyonlar için sürekli kontrol eder.

- Bir çeşit anti-virüs, bireysel firewall gibi güvenlik tedbirlerini ve güncelliğini'de denetler.

Anti-virus

- Ağ tabanlı anti-virüs araçlarının yanısıra; Cihaza özel bir anti-virüs uygulamaları, host’lar için önemli bir defans uygulamasıdır..

Access control/authentication
(Erişim Kontrol/Kimlik Doğrulama)

- Kontrol / kimlik doğrulama, erişim kontrolü tedbirleri , cihaz düzeyinde, cihaza yetkili erişimi hakkı sağlayan en iyi uygulamadır.

- Sadece yetkili kullanıcılar için, yüksek düzeyde bir güvenlik sağlanır.

Level3- Host Güvenliği seviyesinin pozitifleri

- Host tabanlı güvenlik teknolojileri; tek bir cihazın fonksiyonel karekteristiğini karşılamak için konfigüre edilebidiklerinden mükemmel koruma sağlarlar.

- Host ortamı, yöneticilere ,Onların hassasiyeti ve yanıt hızlı, güvenli çalışmasını sağlamak için cihaz ayarlarını güncelleştirme için izin verir.

DİKKAT EDİLECEK HUSUSLAR

- Kendi giderleri ve işletme masrafları söz konusu olduğundan; host tabanlı güvenlik cihazları mantıklı dağıtılabilir olmalıdır.

- Genel bir kural olarak, önemli kuruluşlar bu önlemleri almadan önce, sadece 'taç mücevherlerinin‘ bulunduğu kendi özel ağ yapılarını kurarlar.

- Bu kuralın istisnası, bir ağ erişim kontrolü çözümü, genellikle her masaüstü ve çıkış arasında görev yapacak bir dizüstü ağa erişim sağlamak için çalıştırılır..

LEVEL 4: APPLICATION SECURITY (Uygulama seviyesi güvenlik)

- Uygulama düzeyinde güvenlik, şu anda büyük bir ilgi alanıdır. Çünkü Kötü korunan uygulamalar gizli verilere ve kayıtlara kolay erişim sağlar.
- Acı bir gerçektir ki; birçok programcı programını yazarken güvenlik kodlamasını aklına bile getirmemektedir.
- Çoğu kimsede yazdığı programın saldırılara karşı güçsüz olduğunu bildiği halde tedbir düşünmez.
- Uygulamalar, Web 'e müşteriler tarafından erişim için konuyor. Satış gücü, müşteri ilişkileri gibi kolaylıklar sağlayabilen bu uygulamalar, saldırganlar için hazır bir hedef sağlayabilir.
- Bu nedenle, özellikle her biri için kapsamlı bir güvenlik stratejisi empoze etmek, önemli bir güvenlik uygulamasıdır.
- ***Uygulama zırhı (Application shield), Erişim kontrol/Kimlik denetlemesi***, ***Giriş Doğrulama (Input validation)*** gibi teknolojiler bu katmanda koruma sağlamak içindir.

Application shield (Uygulama Zırhı)

- Uygulama seviyesi güvenlik duvarı olarak görülebilir.
- Bu gelen ve giden legal istekler için uygulama izininin verilmesini sağlar.
- Genellikle Web sunucuları, e-posta sunucuları, veritabanı yüklü sunucular, ve benzeri makinelerde uygulama koruması için en uç cihazlar ile bütünleşik kullanıcılar için yapılır.

- Bir uygulama kalkanı, ana cihazdan beklenen işlevselliğin ince bir şekilde ayarlanmasıdır.
- Örneğin, bir e-posta sunucusundaki uygulama kalkanı muhtemelen gelen bir e-posta iletisi yasaklamak için yapılandırılabilir değildir. Çünkü otomatik olarak, herhangi bir yürütülebilir başlatıyor tipik veya Email işlevini gerekli .

Access control / authentication

- Erişim kontrol / kimlik doğrulama teknolojisi - ağ ve host seviyesinde olduğu gibidir.

- Kimlik doğrulama, yalnızca yetkili kullanıcıların erişebildiği uygulamadır.

Input Validation (Giriş Doğrulama)

- Giriş doğrulama tedbirleri , ağın üzerinde seyahat eden uygulama girişlerini denetlemek , doğrulamak içindir.
- Bu Web tabanlı giriş için hayati önem taşır.
- Genel olarak, Web sunucusu ile herhangi bir etkileşim için güvenli olmalıdır.
- Bir örnek olarak, bir posta kodu alanı olan bir Web formu düşünün. Sadece bu alanda kabul edilebilir bir giriş, beş karakter olmalıdır. Yalnızca rakam. Diğer tüm giriş engellenmeli ve bir hata mesajı üretilmelidir. Giriş doğrulama birden fazla seviyelerde sağlanabilir.

Uygulama güvenlik düzeyinin pozitifleri.

- Uygulama düzeyinde güvenlik önlemleri, genel güvenliğini artırmak ve uygulamaları daha iyi kontrol etmek için izin verirler.

- Ayrıca birçok eylemleri izlemek, kaydedebilmek için daha yüksek düzeyde bir hesap sağlanır

Uygulama güvenlik düzeyinde dikkat edilecekler.

- Kritik noktalar için uygulamaları öncelik ve uzun vadeli planlama.

- Uzun vadeli planlama kontrollü bir şekilde güvenlik önlemleri sağlar.

- Ağınız büyüdükçe ve ek masrafları ortadan kaldırır güçlendirme muhtemelen gerekecektir.

LEVEL 5: DATA SECURITY (Veri Güvenliği)

- Veri düzeyi güvenlik, bir şifreleme politikası gerektirir.
- Network'te seyahat eden Şifrelenmiş veri diğer güvenlik önlemleri aşılmış olsa bile güvenlik sağlayan bir yöntem olarak görülebilir.
- Güçlü şifreleme programı, özel verileri korur.
- Veri güvenliği, organizasyon çapındaki güvenlik politikalarına son derece bağımlıdır.
- Verilere erişimi kimin idare edeceği, kullanıcılar hangi yetkilere sahip olacağı, kendi bütünlüğü v.b
- Şifreleme , erişim kontrol / Kimlik doğrulama teknolojileri bu sevide koruma işlemi yapan teknoloji…

Encryption (Şifreleme)

- Veri şifreleme programları yaygın olarak , veri, uygulama ve işletim sistemi seviyelerinde uygulanmaktadır.

- Tüm şemalarda, veriye erişebilmek için şifreleme / şifre çözme anahtarlarını gerekir.
- Ortak şifreleme stratejileri PKI, PGP, RSA

Kriptografi (Şifreleme)

- Kriptografi, veriyi yalnızca okuması istenen şahısların okuyabileceği bir şekilde saklamak ve göndermek amacıyla kullanılan bir teknolojidir.
- Şifreleme, iletişim sırasında verinin güvenliğini sağladığı gibi, değiştirilmesini önleyici bir tedbirdir (İçerik tabanlı koruma). Şifreleme de veriler şifrelenerek anlamsız hale getirilip hedefe gönderilir. Hedefte ise tam tersi işlem yapılarak (Deşifreleme) orijinal haline çevrilir.
- TCP/IP protokolu verinin doğru adresi bulup ulaşmasını ön plana aldığından ağ güvenliği konusu pek düşünülmez. Bu protokol, paket verilerini açık metin olarak gönderir. Dolayısıyla, ağda dinleme yapan bir nokta bu verilerin içeriğini görebilir veya değiştirme işlemi yapabilir.
- Aşağıda bazı açık metin(Clear text) kullanan protokollar görülmektedir.

• FTP	Doğrulama açık metindir.
• Telnet	Doğrulama açık metindir
• SMTP	posta mesajlarının içeriği açık metin olarak dağıtılır.
• http	Sayfa içeriği ve formlardaki bilgilerin içeriği açık metin olarak gönderilir.
• IMAP	Doğrulama açık metindir
• SNMPv1	Doğrulama açık metindir

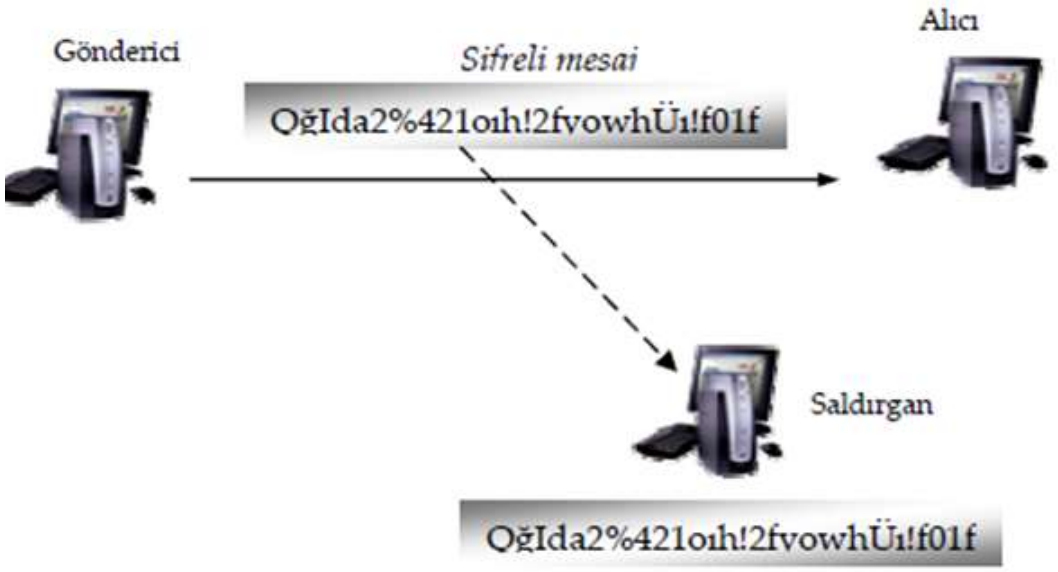
•Şifreleme, bu açıkları büyük ölçüde giderebilir.

- **Kriptografi'de veri, matematiksel yöntemler kullanılarak kodlanır ve başkalarının okuyamayacağı hale getirilir. Bu matematiksel kodlamaya "*kripto algoritması*" adı verilir.**
- **Bir şifreli haberleşme için mekanizma aşağıdakilerden oluşur.**
- **1-Şifreleme Algoritması**
- **2-Deşifreleme Algoritması**
- **3-Anahtar**

Temel Kriptografi Mekanizması

Ödev: Simetrik ve Asimetrik algoritma kullanılan şifreleme tekniklerinin incelenmesi (Rapor ve en az 25 slayt'lık sunu)

- Kripto sistemleri,Gizlilik, Veri Bütünlüğü, Kimlik Sınaması ve İnkâr Edememe hizmetlerinde kullanılır.



Hattı Dinleyen Bir Saldırgana Karşı Şifrelemenin Kullanılışı

Sayısal İmza ve PKI

- Sayısal imza , Kimlik Sınaması ve Veri Bütünlüğü prensiplerinin gerçekleştirilmesinde kullanılırlar (İçerik Tabanlı Güvenlik).

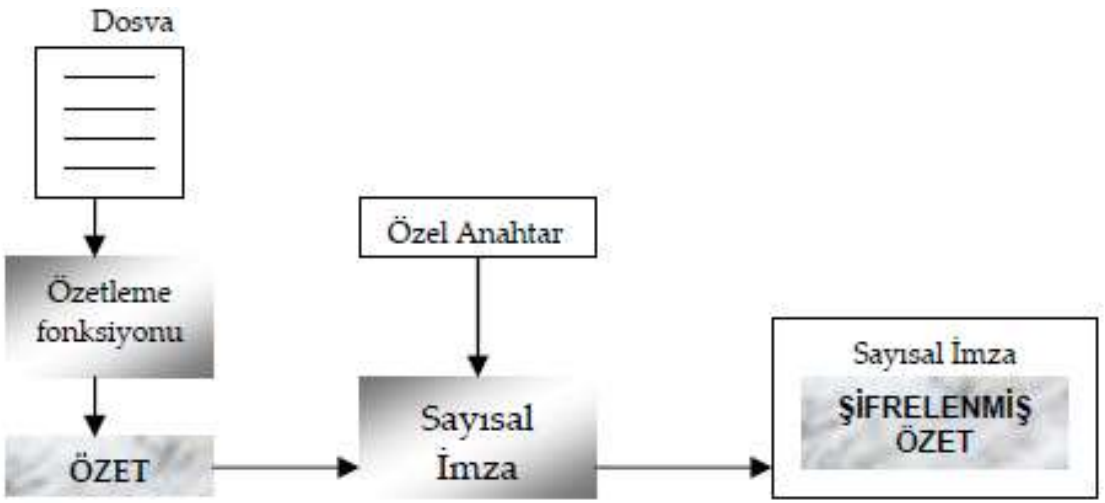
- Bir sayısal imza, şifrelenmiş bir özet (hash) değeridir. Sayısal imzalar yardımıyla, alıcı taraf göndericinin kimliğinin sınamasını yapar ve göndericinin kim olduğundan tam olarak emin olur.

- Bunun yanında, sayısal imza teknolojisi, gönderilen verilerin bütünlük sınamasında da kullanılabilir.

- Sayısal imzalar, gerçek hayatta kullanılan ve elle atılan imzanın (ıslak imzanın) bilişim dünyasındaki karşılığı olarak görülebilir.
- Bir sayısal imza, imzaladığı içeriğin, imzalandığı andan itibaren değişmediğinin kanıtlanmasında kullanılabilir

Ödev: sayısal İmza teknolojisi, yapısı Algoritmaları?

- Sayısal İmza oluşturma Süreci



Bir Mesajın Sayısal İmzası'nın Oluşturulması

Erişim kontrol / kimlik denetimi (Access control/authentication)

- Erişim kontrol /Kimlik denetimi; ağ, host ve uygulama düzeyinde kimlik doğrulaması, yalnızca yetkili kullanıcıların verilere erişimi için kullanılır.

pozitifleri

- Şifreleme, verileri korumak için kanıtlanmış bir yöntem sağlar.

- Davetsiz misafirlerin bilgisayarınızdaki tüm diğer güvenlik önlemlerinden sonra şifrelemeyle koruyan bir son, etkili bir bariyer sağlar.

- Özel bilgi ve fikri mülkiyet.

Dikkat edilmesi gereken hususlar

- Verileri Şifrelemek ve deşifrelemek işlemleri, önemli performans etkilerine (negatif yönde) neden olabilir.

- Ayrıca, anahtar yönetimi, büyük bir idari yük haline gelebilir veya kuruluşlar büyüdükçe bu işlemler dahada karmaşıklaşır.

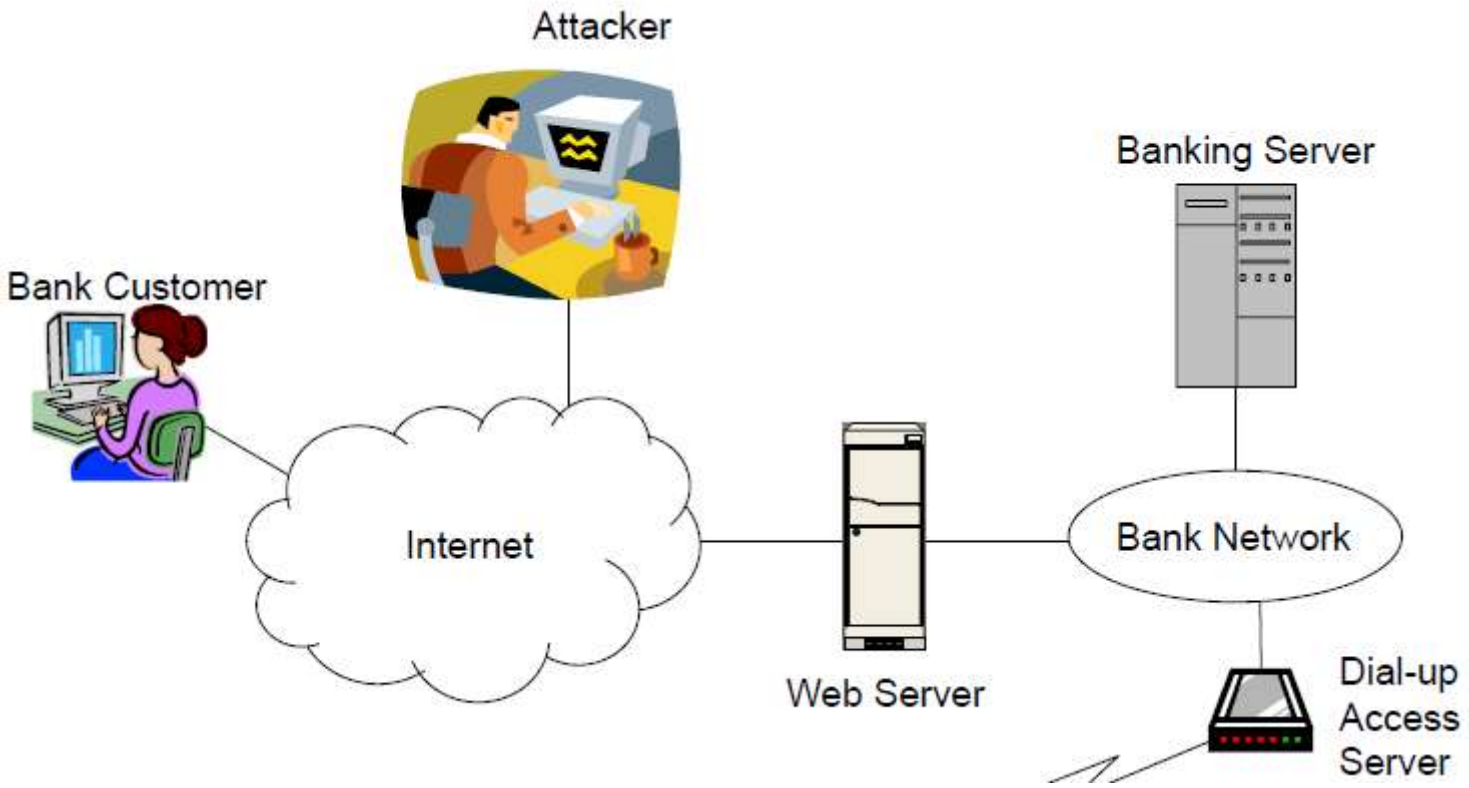
- Derinlemesine veri şifreleme dikkatle yönetilmesi gerekir. Şifreleme anahtarları etkilenen tüm cihazlar için senkronize olmalıdır.

Örnek

- Bir banka, müşterilerine internet bankacılığı hizmeti sağlamak istiyor.
- Bu hizmetler; önceden programlanmış web sayfaları ve uygulamalarıdır.
- Her müşteri, kendi hesabına erişmek için bir ***id*** ve **şifre** bilgisine sahiptir.

- ***Tehditler(Threads) nelerdir?***
- ***Önlemek için güvenlik mekanizmaları nelerdir?***
- ***Güvenlik Servisleri nelerdir?***

Örnek bir seneryo



Güvenliğe yönelik Ataklar

- **Pasif Ataklar – İletişimin dinlenmesi veya izlenmesi**

– Mesaj içeriklerinin elde edilmesi için

– Ağ trafiğini izlemek veya durdurmak

- **Aktif Ataklar: – Veri akışının değiştirilmesi**

– Bir olayın diğerlerinden maskelenmesi.

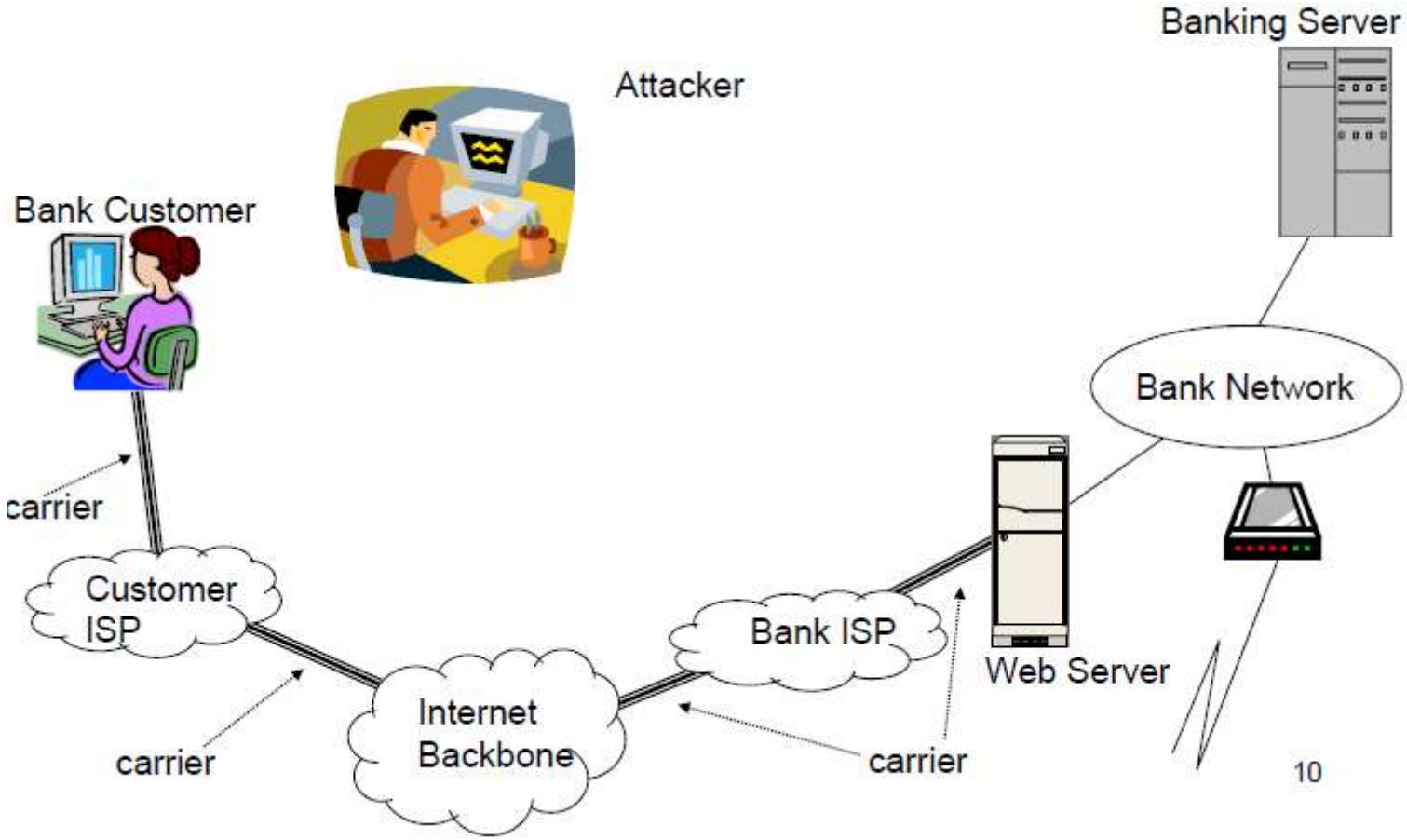
– Bir mesajın uydurulması (fazladan)

– Önceki mesajların tekrarlanması

– Yoldaki mesajların değiştirilmesi

– Servilerin aksatılması.

Tehditler


Banking Server
Attacker
Bank Customer
Bank Network
carrier
Customer ISP
Bank ISP
Web Server
Internet Backbone
carrier
carrier

Saldırı Hedefleri

- ***Müşteri bilgisayarı***
  - DoS
  - Kötü amaçlı kodları: Virüs, Worms
  - Saldıran bilgisayarın kontrolünü alabilir

- ***Müşteri - Web Sunucu iletişim***
  - Dinleme
  - Man-in-the-middle
    - mesajları, değiştirme, ekleme ve silme
  - Session Hijacking (Oturum çalma- hırsızlığı)
  - DoS: SYN saldırı

- ***Internet Altyapısı***
  - Dinleme
  - BGP saldırıları
  - Router OS saldırılar
  - DoS

Saldırı hedefleri

- ***Web Sunucusu***
  - Yığın (Stack) parçalanması
  - Taşınabilir programlar
  - IP spoofing
  - Güvensiz Hizmetler
  - Kötü amaçlı kodları: Virüs ve solucanlar
  - DoS: SYN saldırısı, ping sel.
- ***Banka Network ve Sunucular***
  - Erişmek için arka kapı kullanımı.
  - Dinleme,

  Man-in-the-middle: Bankacılık Server Web Server
  - Session Hijacking
  - DoS
  - DNS saldırısı
  - Diğer sunucuların güvensiz servisleri kullanması
  - Diğer sunuculara kötü niyetli kodların yüklenmesi.
- ***DNS sunucuları***
  - DNS önbellek zehirlenmesi
  - DNS DoS atakları

Müşteri Bilgisayarındaki önlemler

- ***Fiziksel güvenlik***
  - Güçlü Şifreleme
  - OS(İşletim sistemi) güvenlik yamaları
  - Uygulama güvenlik yamaları
  - Güvensiz hizmetlerin yerine göre iptali.

  - Telnet, ftp, nfs
  - Rpc, uzaktan komutları (rlogin, rsh, ...)
  - Dns, web

  - ***Tarayıcı (Browser) konfigürasyonu:***

  - Cep telefonu kodları otomatik olarak kabul etmemek
  - Varsayılan olarak güçlü kripto algoritmaları Seçimi
  - Personel Güvenlik Duvarı

  - İsviçre peyniri değildir!!! dikkatli bir şekilde yapılandırılmış olması gerekir
  - ***Virüs koruma ve tarayıcılar***

Müşteri-Web Sunucu iletişimi için önlemler

- ***Kimlik Doğrulama***

- UserID / Password: "Bildiğiniz"
- İstemci Sertifikası: "Size verilen“

- Çalıntı istemci sertifikalarını önlemek için;

- ***Kısa yaşam süresi, Kullanışlı değil!***
- ***Ön sertifikalı Kullanıcı Kimliği (ID) :*** Aşağıdaki şatlarda kabul edilir.
  - »Yetkisi kontrol edilir
  - »Son kullanma tarihi kontrol edilir
  - »Kara liste kontrol edilir. (sertifika iptal listesi)
  - »Kullanıcının doğruluğu, sertifikayla ilişkili özel anahtardaki kendi bilgisi ile kanıtlanır.

- Kullanıcı, sertifikada saklanan kullanıcı kimliği ile eşleşen bir kullanıcı ID'si ve doğru şifreyi girmişse;

- Sunucu bunu onaylar: Bir oturum zamanlık anahtar üretir. (Gizliliği sağlayan şifre veya özel anahtarın üretilmesinin istenmiyorsa)

Müşteri-Web Sunucu iletişimi için önlemler

- ***Gizlilik ve Bütünlük (Confidentialty ve integrity)***

- Anahtar değişimi;
  - Kimliği doğrulanan, kimlik doğrulama işlemi sürecinin bir parçası olmalıdır.
  - Sadece “Bir oturum yaşam sürelik” olmalıdır.

- Güçlü kripto algoritmaları;
  - Müşteri ve banka tarafında erişim kontrolu için.

Müşteri-Web Sunucu iletişimi

Looks like SSL!

Internet Altyapısı için düzenlemeler

- Router OS düzeltmeleri
- Güvensiz yönlendiriciler servisler
- Saldırı Tespit Sistemleri
- Erişim listeleri
- Omurga güvenlik duvarları
- Güvenli BGP
- Alternatif bağlantılar ve yollar
- Dikkatli sistem yöneticileri için: aksilikler oluşamaz!!!!!!!!!!!!

Şirket Ağının Korunması

- **Router, anahtar ve sunucuların Fiziksel güvenliği.**
- Router, switch, dosya ve uygulama sunucusu
- OS güvenlik düzeltmeleri
- Uygulama güvenlik düzeltmelerini
- **Güvensiz dosya ve uygulama sunucuları servisler**
- Virüs koruma ve istemciler ve sunucular üzerindeki tarayıcılar
- **Arkakapıları yoketmek**
- **DMZ Erişim sunucularının güvenlik duvarları arkasında**
- **VPN / IPSEC, bir kez şifreler ve erişim kontrol Belgesi**
- **Erişim kontrolleri**
- Dahili istemci-Sunucu iletişiminde kimlik doğrulama ve gizliliğin
- IPSEC
- Kerberos
- Ithal uygulaması ile dikkatli olun
- **Bankacılık sunucuları için Firewall koruması**
- Dikkatli sistem ve ağ yöneticileri, aksilikler. Olmaz!!!!!!
- **Güvenli DNS**
- Intrusion Detection System

WEB Server Koruması

•Fiziksel güvenlik
• OS güvenlik düzeltmeleri
• Uygulama güvenlik düzeltmelerini
• Güvensiz hizmetleri tanıma
• Virüs koruma ve tarayıcılar
• Güvenli müşteri erişimi
- SSL
- sunucu sertifikası
- Zayıf olanları silme, varsayılan olarak güçlü bir kripto fonksiyonlarının ayarı
• Yerel depolama yok
- Bankacılık ve finansal veriler
- Güvenlik ile ilgili kritik bilgileri
• Güvenlik duvarı arkasında De militarize Zone (DMZ) bulundurulması
• Güvenli Web sunucusu banka sunucu iletişimi
- IPSEC
- İşlem tabanlı kimlik doğrulama, işlem çift kontrolleri
•Secure DNS

DNS Sunucularda durum

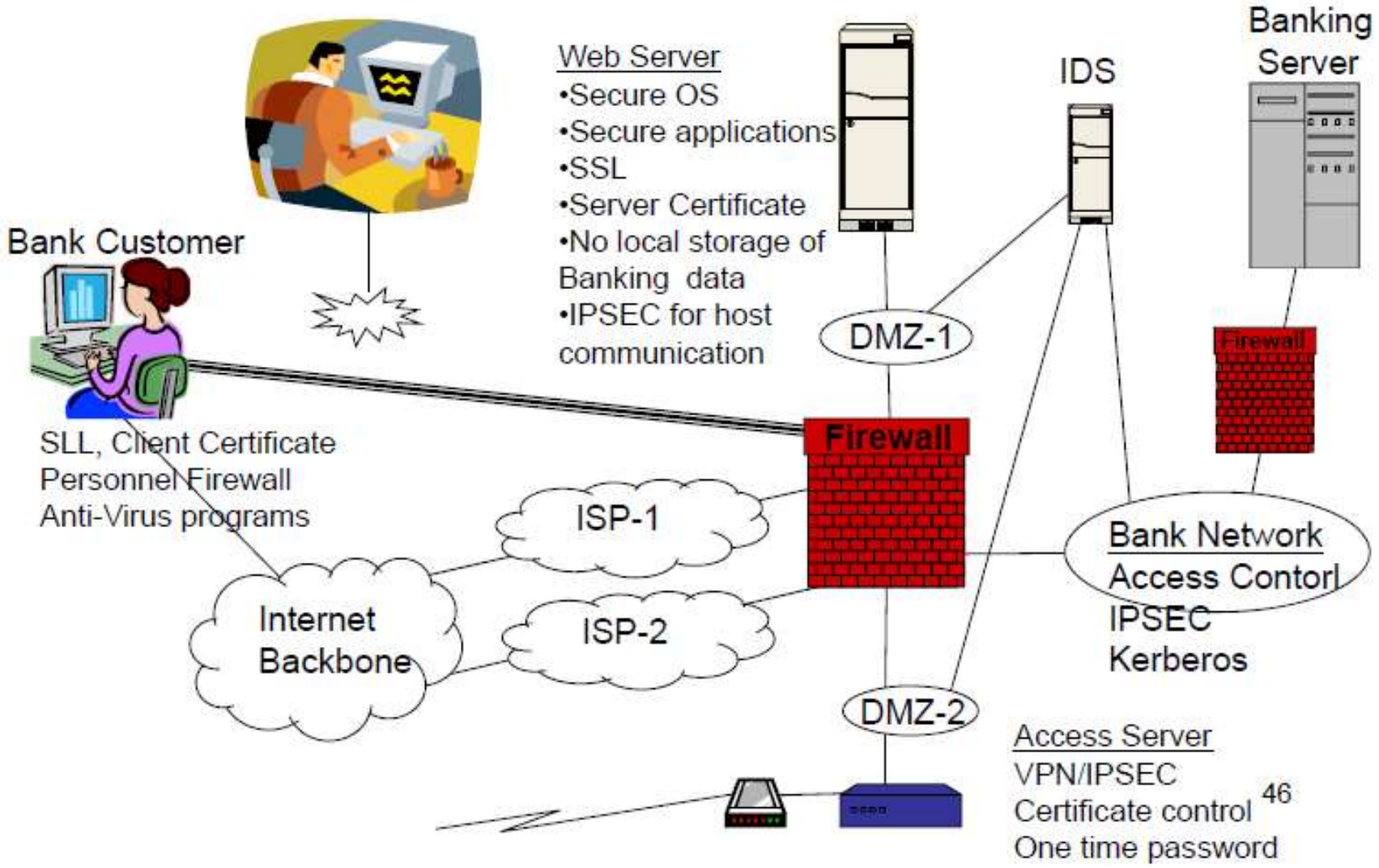
- En son BIND sürümleri, güvenlik yamaları
- DNS yapılandırması

- Zone aktarımı yapmayınız.

- DNS sunucularında OS, Uygulama, güvensiz hizmetlerini takip ediniz.

- DNS DMZ güvenlik duvarı arkasında olmalı
- Secure DNS
- Dikkatli sistem yöneticileri hiçbir aksilikle karşılaşmazlar!

Sonuç Resim


Bank Customer
Web Server
•Secure OS
•Secure applications
•SSL
•Server Certificate
•No local storage of Banking data
•IPSEC for host communication
IDS
Banking Server
DMZ-1
Firewall
Firewall
SLL, Client Certificate
Personnel Firewall
Anti-Virus programs
ISP-1
ISP-2
Internet Backbone
Bank Network
Access Contorl
IPSEC
Kerberos
DMZ-2
Access Server
VPN/IPSEC
Certificate control
One time password