VERİ GÜVENLİĞİ

Ağ Güvenliği

Ağ Saldırı Riskleri

- İnternet üzerindeki bu tür güvenlik açıklıkları kullanıcıları İnternete karşı güvensizleştirebilir.

- Saldırıyı gerçekleştirenler, yazılımın zayıflıkları, kullanıcı adına ve bu kullanıcıya ait parolayı tahmin etme ve donanım saldırıları gibi daha düşük düzeyli teknik yöntemlerle kolayca ağa erişim kazanabilir.

Bilgi Hırsızlığı

- Bilgi hırsızlığı izinsiz ağa erişimin, korumalı ağ bilgilerini elde etmek amacıyla kullanıldığı bir saldırıdır.

- Saldırgan, bir sunucuda veya bilgisayarda, daha önce kimlik doğrulaması için çaldığı bilgileri kullanabilir ve dosyalarda saklanan verileri okuyabilir.

Kimlik Hırsızlığı

- Kimlik hırsızlığı, kişinin izni olmadan kişisel bilgilerinin elde edilmesidir.

- Kimlik hırsızlığı ile kişinin kredi kart numarası, ehliyet numarası, vatandaşlık numarası, İnternet bankacılığı bilgileri, eposta şifre parolası ve önemli diğer kişisel bilgileri bir başkası tarafından çıkar sağlamak amacı ile kullanılabilir.

Ağ İletişim Tehditleri

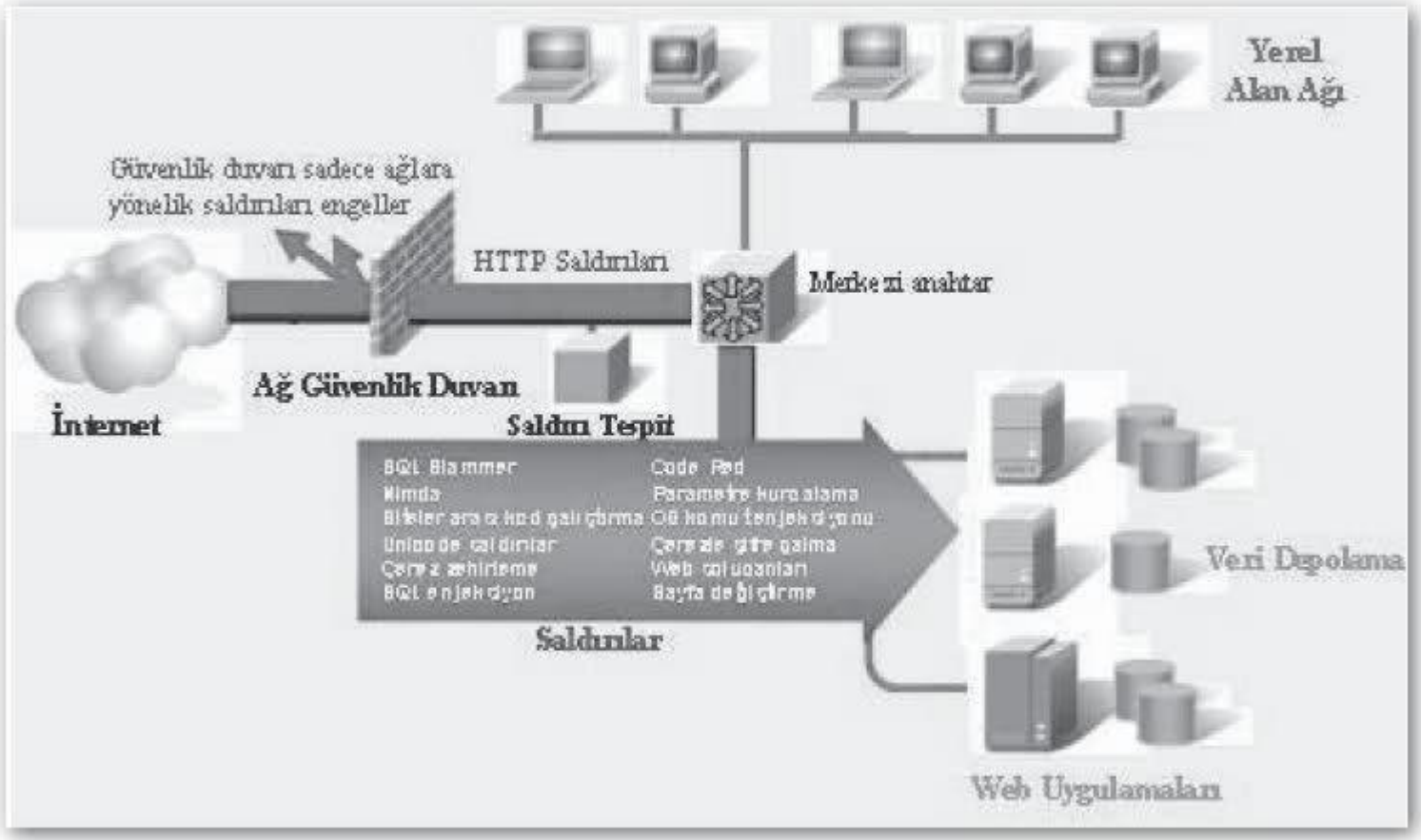
İnternetin genişlemesi ile beraber ağ uygulaması da beklenmedik şekilde genişlemiştir.

Bu gelişmeyle birlikte ağ kurulup işletmeye alındıktan sonra ağ yönetimi ve ağ güvenliği büyük önem kazanmıştır.

Ağ İletişim Tehditleri

- **Harici tehditler**, ağ dışında çalışan kullanıcılardan gelir.
- Bu kişilerin bilgisayar sistemlerine veya ağa yetkili erişimi bulunmamaktadır.
- Harici saldırganlar, ağa saldırılarını genellikle İnternet üzerinden veya kablosuz ağlardan gerçekleştirir.

Ağ İletişim Tehditleri



Ağ İletişim Tehditleri

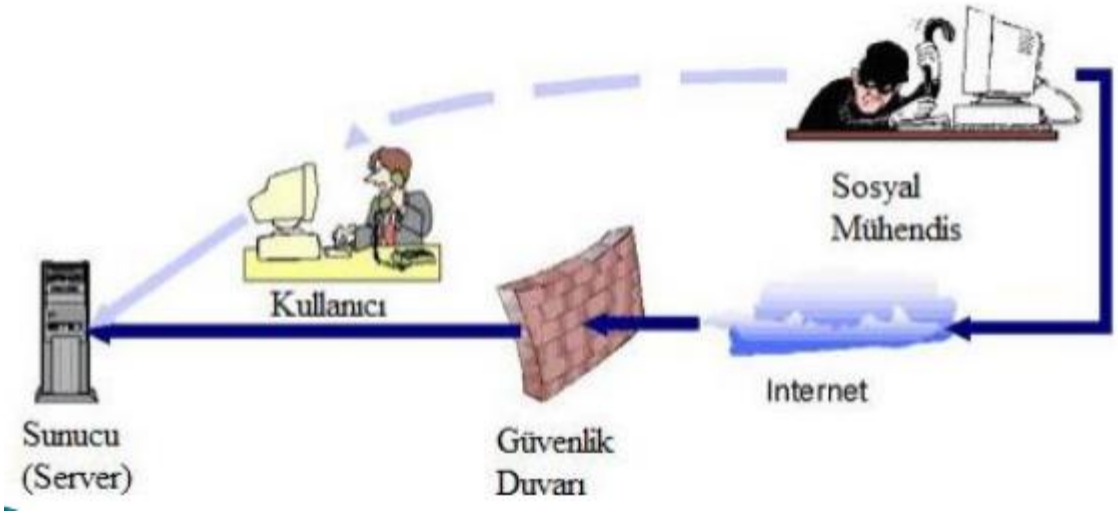
- **Dahili tehditler** ise; bir kullanıcının hesabı üzerinden ağa yetkisiz erişimi olduğunda ya da ağ ekipmanına fiziksel erişimi olduğunda gerçekleşir

Sosyal Mühendislik

- Sosyal mühendislik, insanlar arasındaki iletişimdeki ve insan davranışındaki modelleri açıklıklar olarak tanıyıp bunlardan faydalanarak güvenlik süreçlerini atlatma yöntemine dayanan müdahalelere verilen isimdir.

Sosyal Mühendislik

- Sosyal mühendis, kendisinin sistem sorumlusu olduğunu söyleyerek kullanıcının şifresini öğrenmeye çalışmak veya teknisyen kılığında kurumun içerisine fiziksel olarak sızmak veya çöp tenekelerini karıştırarak bilgi toplamak gibi değişik yollarla yapılabilir.



Sosyal Mühendislik

- İnsan faktörü içermeyen bir bilgisayar sistemi yoktur.
- Güvenlik zincirindeki en zayıf halka insandır.
- Sosyal mühendislikte en yaygın kullanılan tekniklerden üçü şunlardır: **sahte senaryo uydurma**, **oltalama (phishing)** ve **sesle oltalama (vishing).**

Sahte senaryo uydurma

- Genellikle telefonla iletişim üzerinden gerçekleşen bir yöntemdir.

- Saldırganın amacına ulaşmak için sahte bir senaryo oluşturması ve bu senaryonun satırları arasından saldırılanın erişimindeki hassas bilgiye (bir sonraki adımda kullanmak üzere kişisel bilgiler ya da şifreler, güvenlik politikaları gibi erişim bilgileri) ulaşması şeklinde gelişir.

Oltalama

- Kimlik avcısının geçerli bir dış kuruluşu temsil ediyor gibi davrandığı bir sosyal mühendislik biçimidir.
- Genellikle e-posta üzerinden hedef bireyle (phishee) iletişim kurar.
- Kimlik avcısı, kullanıcıları kandırmak ve güvenilir bir kurumdan aradığını kanıtlamak için parola veya kullanıcı adı gibi bilgilerin doğrulanmasını isteyebilir.

Ses Oltalama

- Kimlik avcılarının, IP üzerinden ses (VoIP) uygulamasını kullandığı yeni bir sosyal mühendislik biçimidir.

- Sesle oltalamada, güvenilir bir kullanıcıya geçerli bir telefon bankacılığı hizmeti gibi görünen bir numarayı aramasını bildiren sesli mesaj gönderilir.

- Daha sonra kullanıcının yaptığı aramaya bir hırsız tarafından müdahale edilir. Doğrulama için telefondan girilen banka hesap numaraları veya parolalar çalınır.

Saldırı Yöntemleri

- Saldırılar ağ üzerinden olacağından ağa bağlı cihazlar her zaman saldırıya açık durumdadır.
- Saldırganlar ağ üzerinden hedef makinaya ulaşarak yazılım veya donanıma zarar vermek isteyebilir.
- Bunun yanı sıra bir işletmenin ağına ulaşarak veritabanındaki verilere erişebilir, değiştirebilir veya silebilir.
- Saldırgan ağın İnternet bağlantısını kesebilir, hedef makinaya truva atı gibi program yükleyerek kullanıcıyı takibe alabilir.

Saldırı Yöntemleri

- **Hizmet Reddi (Denial of Service-DoS),** hizmet aksatma amaçlı bir saldırı çeşididir. Bir sisteme yapılan düzenli saldırılar sonucunda sistem çalışamaz ve hizmet veremez hale gelebilir.

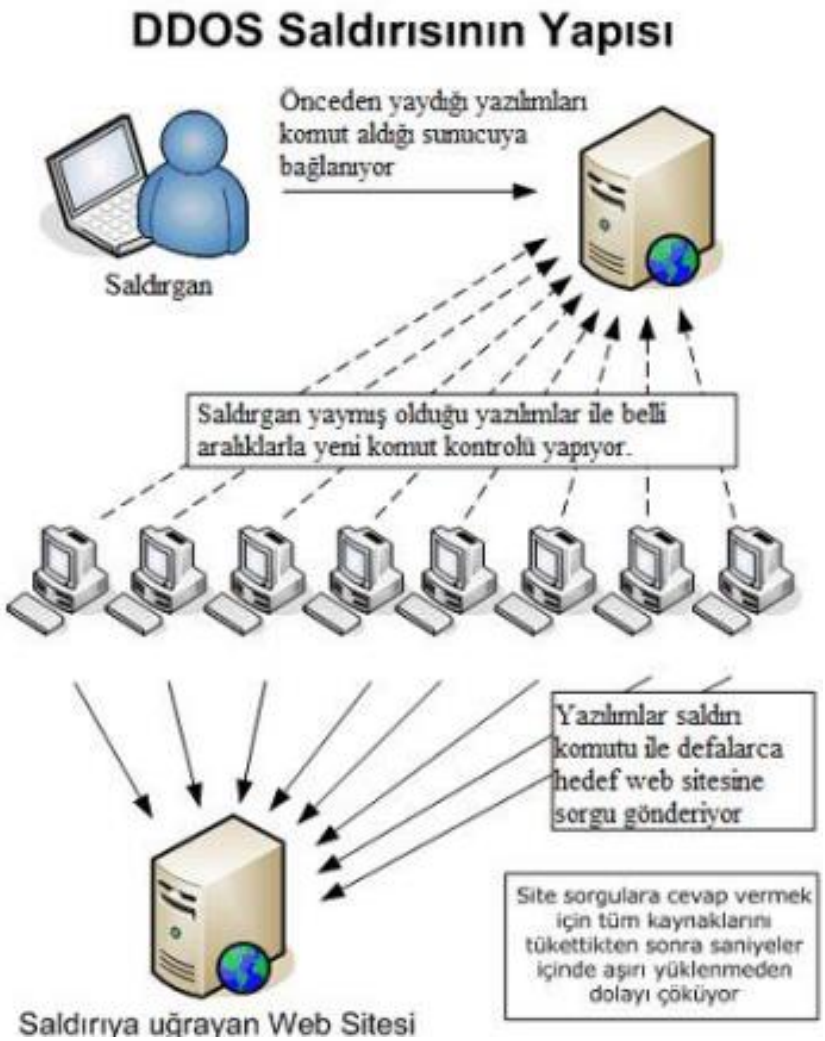
- Ayrıca DoS saldırılarıyla hedef sisteme ait kaynakların tüketilmesi de amaçlanır.

- Dağıtılmış hizmet reddi (DDoS) saldırıları DoS saldırılarının farklı kaynaklardan yapılması ile gerçekleşir.

Saldırı Yöntemleri

Saldırı Yöntemleri

Dağıtılmış hizmet reddi (DDoS) saldırıları



Saldırı Yöntemleri

- **Deneme yanılma** saldırılarında hızlı bir bilgisayar, parolaları tahmin etmeye veya bir şifreleme kodunun şifresini çözmeye çalışmak için kullanılır.

- Saldırgan, koda erişim kazanmak veya kodu çözmek için art arda hızlı şekilde çok sayıda olasılığı dener.

- Deneme yanılma saldırıları, belirli bir kaynakta aşırı trafik oluşması nedeniyle veya kullanıcı hesaplarının kilitlenmesiyle hizmet reddine yol açabilir.

Saldırı Yöntemleri

- **Casus yazılım** (spyware) kişisel bilgi toplama veya kullanıcının onayı alınmadan bilgisayarın yapılandırmasını değiştirme gibi belirli davranışları gerçekleştiren programlardır.

- Casus yazılım genellikle bir dosya indirilirken, başka bir program yüklenirken veya bir açılır pencereye tıklandığında kullanıcının onayı alınmadan bilgisayara kurulur.

Saldırı Yöntemleri

- **Açılır pencereler (pop-up**) bir web sitesi ziyaret edildiğinde görüntülenen ek reklam pencereleridir.

- Açılır pencereler kullanıcı hakkında bilgi toplamak için tasarlanmamış olup genellikle yalnızca ziyaret edilen web sitesiyle ilişkilidir.

Saldırı Yöntemleri

- Bir e-postanın talepte bulunmamış, birçok kişiye birden, zorla gönderilmesi durumunda, bu e-postaya istenmeyen e-posta yani **spam** denir.
- Spamlar genellikle kitlesel veya ticari amaçlı olabilir.
- İnternetteki her kullanıcının yılda 3.000'den fazla spam e -postası aldığı tahmin edilmektedir

Zararlı Yazılımlar

- **Virüs**
  - Bir programın içine, kendi program kodlarını ekleyen ve çalıştırıldığı yerdeki uygun programlara da bulaşarak çoğalan, girdiği sistem ve dosyalara zarar veren program veya kod parçacıklarına **virüs** denir.

  - **Elk Cloner** adlı bir program ilk bilgisayar virüsü olarak tanımlanmıştır. Bir lise öğrencisi tarafından hazırlanıp şaka olarak oyun dosyaları içerisine gizlenmişti. Oyunu 50. çalıştırmada virüs gönderiliyor ve sonrasında boş bir ekranda Elk Cloner adlı virüs hakkında bir şiir gösterilerek görevini tamamlıyordu.

Zararlı Yazılımlar

- **Trojan**
  - Bilgisayar çok iyi korunuyor olsa bile sisteminde bulunan programın içerisine gizlenmiş trojanlar, program çalıştığında ortaya çıkarak değişik programlar kurabilir veya sistem içindeki gizli bilgileri dışarıya iletebilir.
  - Bilgisayarda çalışır hale gelen trojan sayesinde IP taraması yapılarak bilgisayardaki açık portlar bulunur.
  - Trojan'ı hazırlayan kullanıcı da bu giriş ortamını kullanarak bilgisayarın içine girebilir.

Zararlı Yazılımlar

- **Spy (Casus)**
  - İstenmeyen ve tanıtımını yapmak istediği internet sayfalarını açan yazılımlardır.
  - Sizi istediği internet sitelerini açmaya zorlayan ve reklam yapma amacındaki yazılımlardır.
  - Bazen web tarayıcısının başlangıç sayfasına, kendi sayfasını ekleyerek değiştirilmez duruma getirir.

Zararlı Yazılımlar

- **Worm (Solucan)**
  - Solucanları virüsten ayıran özellik, kendi başlarına bağımsız şekilde çalışabilir ve bir taşıyıcı dosyaya ihtiyaç duymadan ağ bağlantıları üzerinde yayılabilir olmalarıdır.

  - Solucanlar sistemdeki önemli dosyaları tahrip etmek, bilgisayarı büyük ölçüde yavaşlatmak ve bazı gerekli programların çökmesine neden olmak gibi bütün olası zararları yaratabilmeyi amaçlar.

Güvenlik Önlemleri

- **Tanımlama ve Kimlik Doğrulama İlkeleri**
  - Kimlik doğrulama, sunucu bilgisayar tarafından belirli kullanıcıları tanımlamak ve kendi verilerine erişim izinlerini doğrulamak için kullanılan işlemdir.
  - İletişimde bulunan bilgisayarların birbirlerinin kimliklerini doğrulamaları için aynı kimlik doğrulama metodunu kullanması gerekir.
  - Tanımlama ve kimlik doğrulama işlemleri yerel ve geniş ağlarda kullanılabilir.

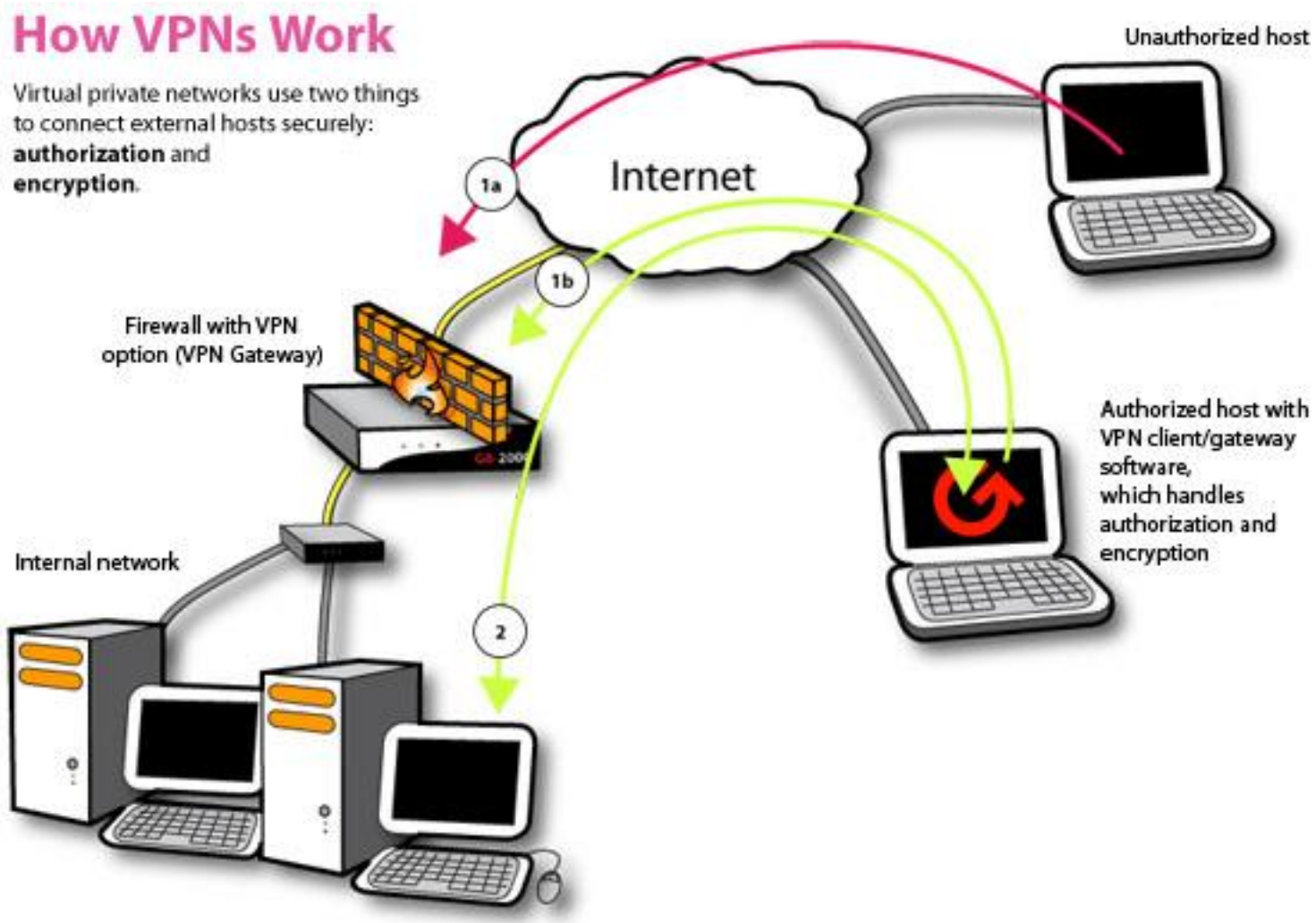
Güvenlik Önlemleri

- **Parola İlkeleri**
  - Bilgisayar ağlarında güvenlik önlemlerinden biri de ağa erişim için parola korumasıdır.
  - İnternet erişimi için veya dosya sunucusuna erişim için güvenlik uzmanları parolalı koruma yöntemini geliştirmiştir.
  - Parola ilkeleri, etki alanı hesapları veya yerel kullanıcı hesapları için de kullanılabilir

Güvenlik Önlemleri

- **VPN Bağlantısı**
  - Ağ güvenlik önlemlerinden biri de VPN (Virtual Private Network-Sanal Paylaşımlı Ağ) kullanılmasıdır.
  - VPN kullanarak yapılan her bağlantıda, veri paketlerinin her biri ayrı ayrı şifrelenerek gönderilir.
  - Güvenliği sağlayan sadece verinin şifrelenmiş olması değil, ayrıca verinin geçtiği yol boyunca içeriğinin bozulmamış olması da önemlidir.

Güvenlik Önlemleri



Güvenlik Araçları ve Uygulamaları

- **Güvenlik Duvarı**
  - Ağ güvenliğini sağlayabilmek için bir ağ güvenlik duvarı (firewall) kullanılır.

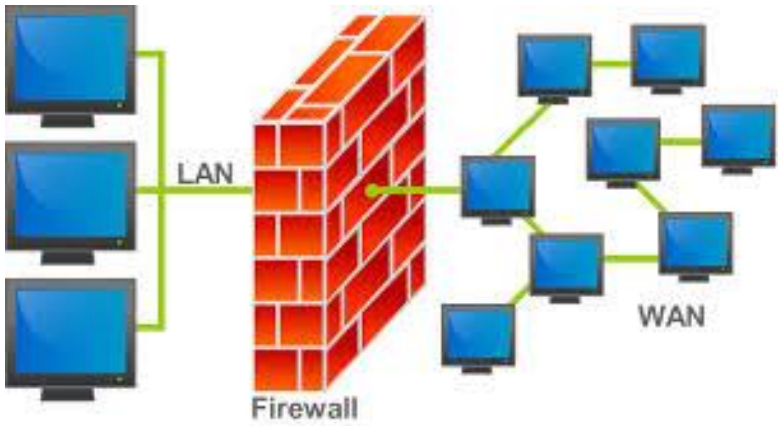
  - Ağ güvenlik duvarı kullanarak ağ dış saldırılardan korunabilir, ağa gelen ve ağdan giden veriler denetlenebilir ve yönetilebilir, istenmeyen istemcilerin (client) İnternet bağlantısı kesilebilir mevcut İnternet bağlantının bant genişliğini yönetilebilir.

  - Güvenlik duvarı yazılımı işletim sistemi dahilinde bulunmakta veya özel bir program yüklenerek de güvelik duvarı kullanılabilir.

Güvenlik Araçları ve Uygulamaları

- Güvenlik duvarı donanım olarak ise yalnızca güvenlik duvarı özelliği ile kullanılan ve geniş bantları karşılayabilen güvenlik çözümleridir.
- Ayrı bellek ve işlemci kullandığı için oldukça hızlıdır.
- Genelde yüz bilgisayar ve üzerindeki ağlarda tercih edilir.
- Çalışma mantığında veriyi ağa girmeden karşılamak olduğu için DoS saldırıları gibi güvenlik problemlerine çözüm sunar.

Güvenlik Araçları ve Uygulamaları



Güvenlik Araçları ve Uygulamaları

- **Spam Filtresi**
  - Spam Filtreleri, sunucuya gelen e-postaları bir süzgeçten geçirerek istenilmeyen epostaları tespit eden ve kullanıcının gelen kutusuna (inbox) düşmesine engel olan programlardır.
  - E-postalar spam filtrelerinde birçok kural ve kriterlere göre değerlendirilir.
  - E-posta adreslerinde spam olarak algılanan mailler genellikle gereksiz posta (junk mail) klasöründe belli bir süre tutulur.

Güvenlik Araçları ve Uygulamaları

- **Yamalar ve Güncellemeler**
  - Yazılımlarda zaman zaman hatalar veya eksiklikler keşfedilir.
  - Bilgisayar sistemlerini dışarıdan gelecek saldırılara (virüs ya da bilgisayar korsanı) açık hale getiren bu zaaflara güvenlik açıklığı denir ve ancak yazılımlar güncellenerek kapatılabilir.
  - Bu açıklıkları giderme amacı ile yazılım ve işletim sistemleri geliştiricileri yeni sürümler, yazılım yamaları ya da hizmet paketleri yayınlar.

Güvenlik Araçları ve Uygulamaları

- **Açılır Pencere Engelleyici**
  - İstenmeden açılan pencereler, tarama sırasında kullanıcıya sormadan kendiliğinden açılan pencerelerdir.
  - Açılır pencereleri engellemek için bilgisayarda kullanılan tarayıcı üzerinde ayarlamaları yapmak yeterli olur.
  - Açılır pencereleri engellemek için özel programlar da kullanılabilir.

Güvenlik Araçları ve Uygulamaları

- **Antivirüs Yazılımları**
  - Bilgisayar sistemlerinin düzgün çalışmalarını engelleyen, veri kayıplarına, veri bozulmalarına ve çeşitli yollarla kendisini kopyalayan kötü amaçlı yazılımlara virüs denir.
  - Her geçen gün yeni virüsler ortaya çıkmakta veya var olanların özellikleri değiştirilerek tekrar piyasaya sürülmektedir.
  - Virüsler; bilgisayar sistemlerinin çalışmasını aksatma ve bozmanın yanı sıra verilerin silinmesi veya çalınması gibi kötü amaçları gerçekleştirmek için hazırlanmaktadır.

https://www.virustotal.com/

http://www.eicar.org/85-0-Download.html

Güvenlik Araçları ve Uygulamaları

- **Antivirüs**, bilgisayarı zararlı yazılımlardan korumak için hazırlanan güvenlik yazılımlarına denir.

- Antivirüs programları genel olarak zararlı programları bulup yok etmekle görevlidir.

- Bunu yaparken kullanıcılarının tercihlerine göre farklılık gösterebilirler.
  - Örneğin tarama sırasında bir virüs bulunduğunda, antivirüs programı kullanıcıya bu dosya üzerinde ne işlem yapılması gerektiğini sorar.

Güvenlik Araçları ve Uygulamaları

- Bazı virüslerin verdiği zararlar geri dönüşümü mümkün olmayan hatalara neden olabilir, bu yüzden her bilgisayarda güncel ve lisanslı bir antivirüs programı bulunması gerekmektedir.

- Antivirüs programları tek başlarına tam bir güvence sağlayamazlar. Bunun yanında firewall (güvenlik duvarı) gibi güvenlik yazılımlarının da bilgisayara kurulmuş ve güncel olması gerekmektedir.