Veri Haberleşmesi ve Bilgisayar Ağları

"Ağ Güvenliği"

Dr. Cahit Karakuş, 2020

CRITICAL INFRASTRUCTURE

- Electric power plants
- Banking and finance
- Telecommunications
- Information technology
- Water
- Food Industry
- Railroads
- Chemical
- Airport
- Oil and Gas and Liquefied Natural Gas Storage Facilities
- Major Reservoirs
- Refineries
- Dams
- Pipelines
- Thousands of Miles of Borders

INTERNET

- Evrensel haberleşme ağı, bilgisayarlar kullanılarak erişme, telefon hatları, ve/veya modemler (Kablo, Uydu, Kablosuz, fiber)
- Dünya çapında her gün milyonlarca yeni internet kullanıcıları
- Bilgi toplumu, Evrensel serbest erişim, Yüksek hızda işlemler
- İnternet evrenseldir fakat internet suçları da evrenseldir
- İyi: İnternet dünya çapındadır. Laboratuarlar, Üniversiteler, müzeler, sanat galerileri, alış veriş merkezleri, toplantı alanları, mesajlaşma, e-posta, telefon ve görüntülü görüşme hizmetleri
- Kötü: İnternet ayrıca sapıklık, baştan çıkarma, pornografi ve müstehcenliğin sınırsız bir çukurudur. Dolandırıcılık, kumar, uyuşturucu satışı, gizlice izleme, çalınmış mal satışları gibi suçların internet üzerinde belgeleri bulunmaktadır.

INTERNET SUÇLARI

- Bilgisayardaki veya sunuculardaki bilgilere (Veri, WEB, e-posta) erişme, çalma, silme, değiştirme (hacking – bilgi hırsızlığı)
- İzin almadan başkalarına ait dokümanı veya bilgiyi yayınlamak
- Ekonomik casusluk (Ticari sırların çalınması) veya ekonomik sahtekarlık
- SPAM: Bilgisayar kullanıcılarına istenmeyen e-posta göndererek taciz etmek. Özellikle ticari e-postalar görüntüsü ile belirli e-posta adreslerine veya herkese gönderilmesi (SPAMMER)
- WORM: Yasadışı yöntemler ile bilgiyi ele geçirmek
- Uluslararası para aklama
- Sahtekarlık, İzinsiz banka hesaplarına girme, para transferi, Kredi kart sahtekarlığı
- Suiistimal, Çocuklara taciz, Pornografi,
- Karalama, Hakaret
- Tehdit, Usanç, İzleme
- Kumar
- Virüs
- İllegal programlar kullanarak kendisine ait olmayan mesajlaşmaları izleme

BİLGİSAYARLARIN KORUNMASI

- Anti virüs yazılımı ve erişim yetkilendirme, sınırlandırma yazılımları ve ekipmanları kullanın – yazılımları sürekli güncelleyin
- İşletim sisteminizi kritik güvenlik güncellemesi ve düzeltmeleri ile koruyun
- Bilinmeyen kaynaklardan gelen e-mailleri ve ekli dosyaları açmayın
- Bulunması veya tahmin edilmesi zor şifreler kullanın
- Şifrelemede bir sözlükte bulunan kelimeleri, aile bilgilerini kullanmayın
- Şifre çözücü programların ve ekipmanların olduğunu unutmayın
- Bilgisayarınızdaki bilgilerin sürekli yedeğini alın (CD, Disk, Flash ram)
- Yabancılar ile bilgisayarınıza erişimi paylaşmayın
- Eğer kablosuz ağ kullanıyorsa şifreleme ile koruyun
- Kullanmadığınızda internet erişimi kapatın
- Güvenliğinizi muntazam esaslar üzerine değerlendirin
- Çalışanlarınız ve aile bireylerinizin bu bilgiyi bildiğinizi unutmayın!
- Gizli veya stratejik ticari bilgilerinizin bulunduğu bilgisayar sistemleriniz hiçbir zaman internet erişimine bağlamayın

KABLOSUZ ERİŞİM SİSTEMLERİNE (Wi-Fi) SALDIRI

- Hotspots a neden olmak için antenler kullanılır
- Hotspots – Internet Erişim (genellikle erişim serbest)
- Kablosuz ağ teknolojilerin % 60-70 şifresiz, denetimsiz çalışmaktadır.
- Wi-Fi teknolojileri neden korumasız;
  - Çoğu kullanıcılar verinin önemsiz olduğunu söyler
  - Fakat… Suçlular suçlarını işlemek için kablosuz ağ sistemleri ararlar
  - Ve… Yetkililer sizin kapınıza geleceklerdir.
- Korumasız kablosuz erişim bulmaya kendilerine iş edinmiş profesyoneller
- Bilgi hırsızları
- Dış ortam antenleri benzer ve kablosuz erişim olduğu görünmektedir.
- Yetkilendirme şifreleri ve veri kodlama sistemleri kullanın.
- Erişim yetkilendirmesi filtreleri kullanın
- İzinsiz erişimleri izleyin

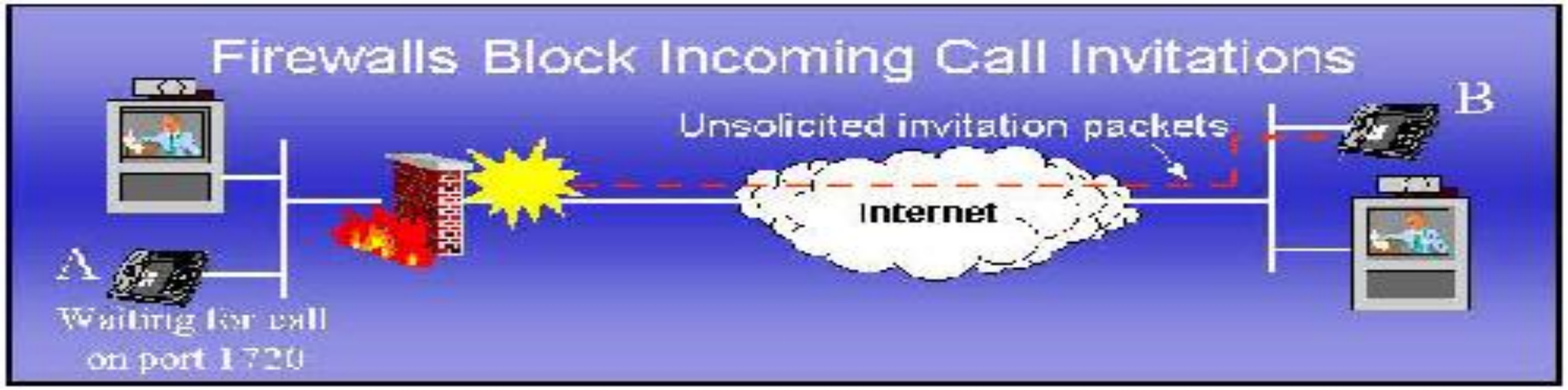
NETWORK GÜVENLİK TEHDİTLERİ

- TCP/IP
- Routing and Hostnames
- IP Security
- Network Redirection
- E-Posta
- E-Posta sahtekarlığı
- Network Flooding
- Distributed Flooding
- Cross-Site Scripting
- Staged Attack
- Intruder Trends

KORUMA SİSTEMLERİ

- Firewall
  - Block access
  - Selected prevention
  - Monitor
  - Record
  - Encryption
- Wrappers, Proxies and Honeypots
- Telecom Security
- Modems and Security
- Additional Security;
  - Call-back modems,
  - Password modems,
  - Encrypting modems,
  - Caller-ID modems

- Border router; Ingress and egress filtering
- Firewalls; Is high availability a *business* requirement?
- Authentication; Check credentials *before* allowing through
- Encryption; VPNs, IPSec ESP tunnel mode



Ağ teknolojilerinde bilgi güvenliği

- Ağ teknolojileri üzerinden güvenlik izlenmesi
- Yetkilendirme, Doğrulamak, Muhasebe
- Ağ teknolojileri üzerinden görüntü iletişimi ile güvenliğin izlenmesi
- Ağ teknolojileri üzerinden güvenilir veri kanalı oluşturulması
- Çalışanların erişim yetkilendirilmesi ve yetki denetimi
- Sistemlere izinsiz girişlerin önceden algılanıp engellenmesi, alarm üretilmesi
- Tek merkezden denetim; İzleme, Kayıt, Uyarı, Alarm
- Uzaktan müdahale; iş süreçlerinde oluşan aksaklıkların süratle giderilmesi; Bakım, kontrol, test, Onarma
- Tek merkezde toplanan bilgisayar programlarının ve işletim sistemlerinin eşit paylaşımı ile ekonomiklik, kontrol edilebilirlik, izlenebilirlik

Bir bilgisayar ağının güvenliğini nasıl sağlayabilirsiniz?

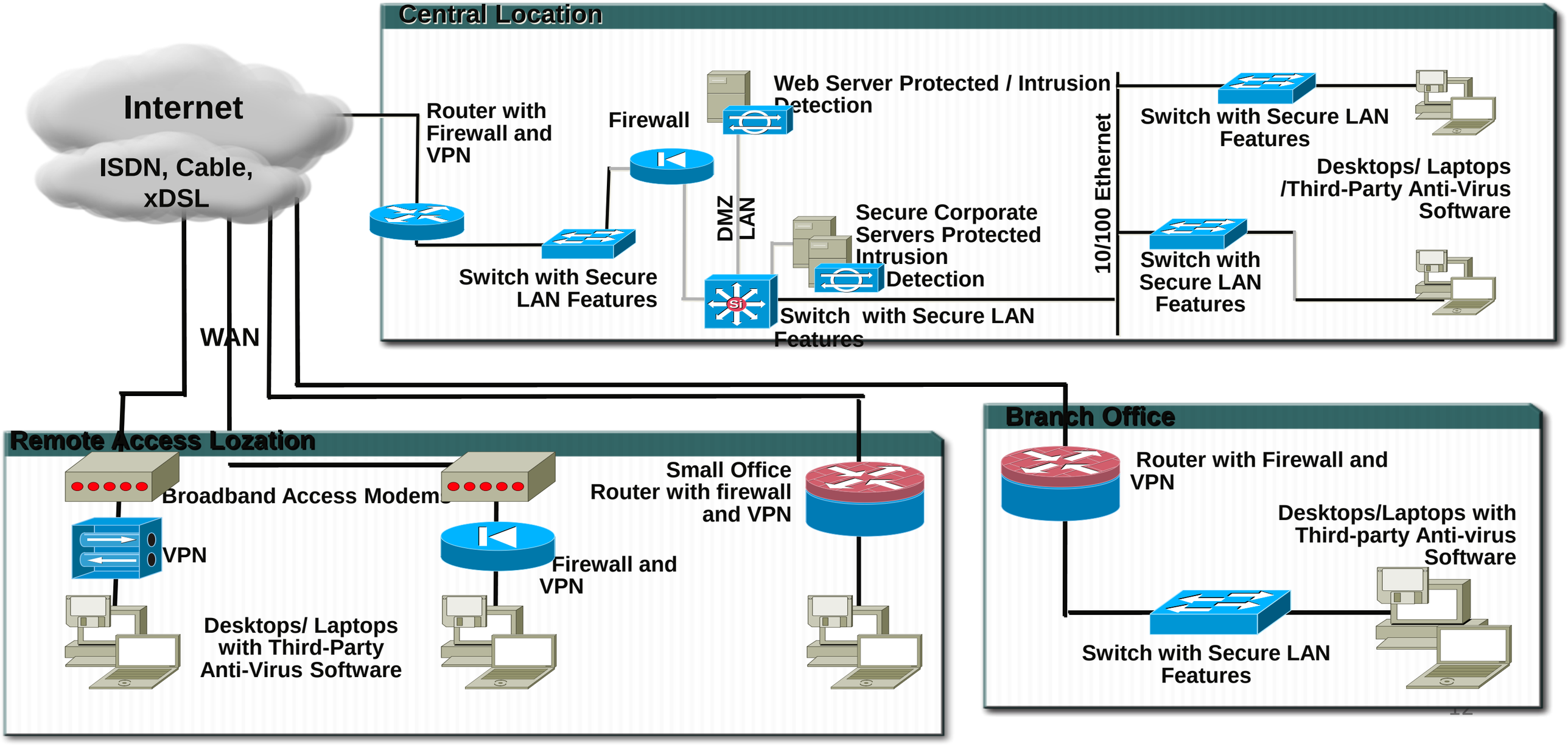
Aşağıdaki yollarla güvenli bir bilgisayar ağı elde edebilirsiniz:

- Ağ genelinde güvenilir ve güncel bir virüsten koruma programı yüklenir.
- Güvenlik duvarlarının doğru şekilde kurulduğundan ve yapılandırıldığından emin olunur.
- Güvenlik duvarı performansını izlenir.
- Kullanıcı kimlik doğrulamasını sağlanır.
- Şifreler her üç ayda bir düzenli olarak güncellenir.
- Sanal bir özel ağ (VPN) oluşturulur.

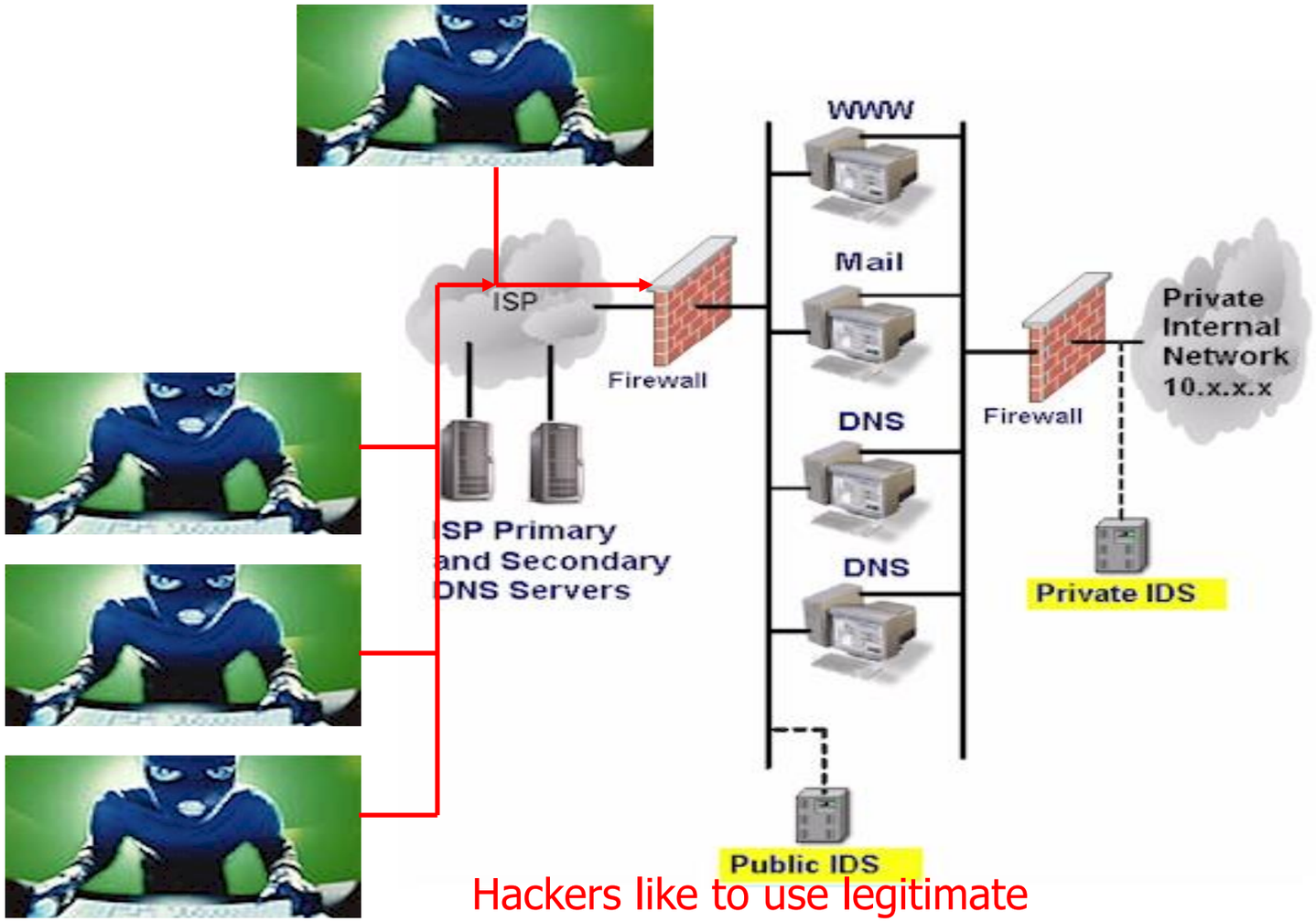
Ağ teknolojilerinde güvenlik Çözümleri

- Router with firewall
- Firewall
- VPN: Kurumlar ya da lokasyonları internet haberleşme ortamında yüksek güvenlikte birbirine bağlayarak yerel ağ haline getiren özel sanal ağ oluşumu.
- Secure LAN Switches
- WEB server protected
- Intrusion detection
- Anti Virus Software

AĞ GÜVENLİK ÇÖZÜMLERİ



NETWORK GÜVENLİK TEHDİTLERİ



Hackers like to use legitimate traditional ports (21, 25, 80)

Ağ teknolojilerinde güvenlik çözümleri

- Router with firewall and VPN
- Firewall
- VPN
- Secure LAN Switches
- WEB server protected
- Intrusion detection
- Anti Virus Software

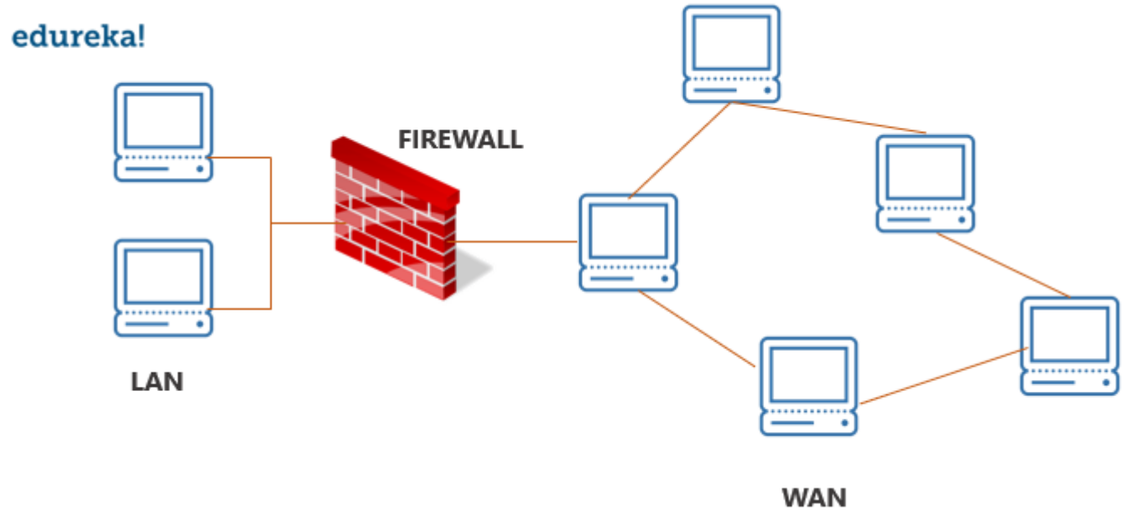
Bir bilgisayar ağının güvenliğini nasıl sağlayabilirsiniz?

Aşağıdaki yollarla güvenli bir bilgisayar ağı elde edebilirsiniz:

- Ağ genelinde güvenilir ve güncel bir virüsten koruma programı yüklenir.
- Güvenlik duvarlarının doğru şekilde kurulduğundan ve yapılandırıldığından emin olunur.
- Güvenlik duvarı performansını izlenir.
- Kullanıcı kimlik doğrulamasını sağlanır.
- Şifreler her üç ayda bir düzenli olarak güncellenir.
- Sanal bir özel ağ (VPN) oluşturulur.

Güvenlik Duvarı (Firewall) nedir?

- Güvenlik duvarı, önceden tanımlanmış bazı kurallara dayalı olarak ağ trafiğini izlemek ve kontrol etmek için kullanılan bir ağ güvenlik sistemidir.Güvenlik duvarları ilk savunma hattıdır ve güvenilmeyen dış ağlardan gelebilecek saldırıları önlemek için iç ve dış ağlar arasında bariyerler oluşturur. Güvenlik duvarları donanım, yazılım veya bazen her ikisi olabilir.
- Güvenlik duvarı, bilgisayar ağlarını yetkisiz erişime karşı korumak için kullanılan bir ağ güvenlik sistemidir. Dışarıdan bilgisayar ağına kötü amaçlı erişimi önler. Dış kullanıcılara sınırlı erişim sağlamak için bir güvenlik duvarı da oluşturulabilir.
- Güvenlik duvarı bir donanım cihazı, yazılım programı veya her ikisinin birleşik yapılandırmasından oluşur. Güvenlik Duvarı üzerinden geçen tüm iletiler belirli güvenlik ölçütlerine göre incelenir ve ölçütleri karşılayan iletiler ağ üzerinden başarıyla taşınır veya bu iletiler engellenir.

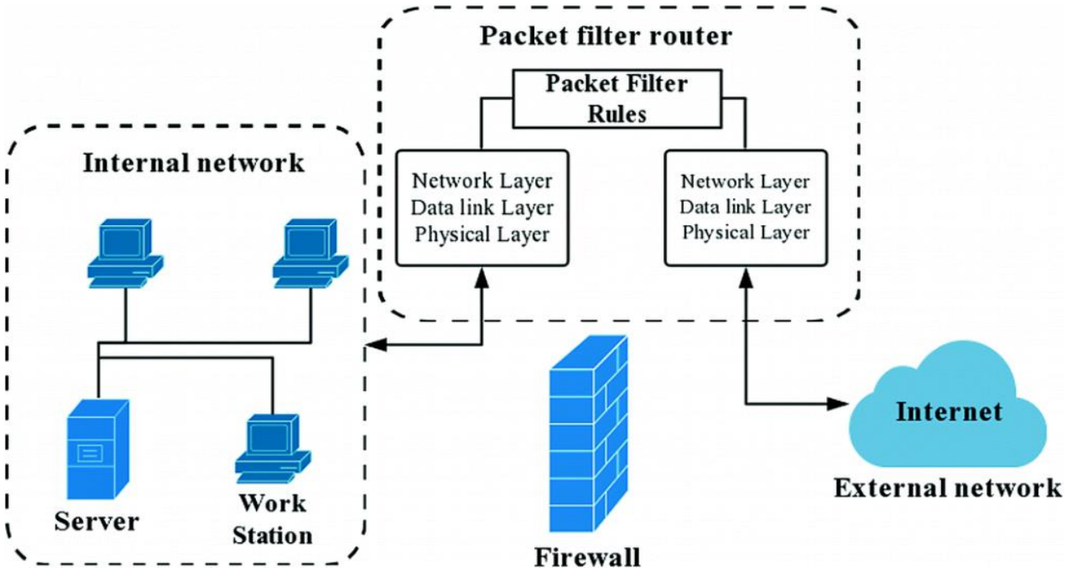


Firewalls

- Güvenlik duvarı, ağ trafiğini yönetmekten sorumlu bir ağ güvenlik sistemidir. Uzaktan erişimi ve içerik filtrelemeyi önlemek için bir dizi güvenlik kuralı kullanır. Güvenlik duvarları, sistemleri veya ağları virüslerden, solucanlardan, kötü amaçlı yazılımlardan vb. korumak için kullanılır.
- Güvenlik duvarları genellikle iki türdür –Fiziksel – Fiziksel bir güvenlik duvarı veya donanım güvenlik duvarı, harici ağ ile sunucu arasında yer alan fiziksel bir cihazdır. Gelen trafiği analiz eder ve cihaza yönelik tüm tehditleri filtreler. Kurumlarda ve büyük şirketlerde yaygın olarak kullanılmaktadır.
- Mantıksal – Mantıksal veya yazılımsal bir güvenlik duvarı, alt ağ üzerinde herhangi bir yerde bulunabilir ve ana bilgisayarları yeniden kablolamaya gerek kalmadan alt ağ üzerinde herhangi bir yerde korur. Yalnızca yüklendikleri bilgisayarı korurlar ve çoğu durumda işletim sisteminin kendisine entegre edilirler.

Güvenlik duvarı nasıl çalışır?

- Güvenlik duvarı, hangi bilgi paketlerinin bilgisayar sisteminden ayrılmaya veya sisteme girmeye çalıştığını "dinler". Engelleme, gittikleri IP, onları göndermek için kullanılan bağlantı noktası türü veya menşe uygulaması gibi çeşitli kriterlere göre yapılabilir.
- Güvenlik duvarlarını kullanmanın en karmaşık yönlerinden biri, yapılandırmalarında, hangi tür bağlantıların engellenip hangilerinin engellenmeyeceğine karar vermede yatmaktadır.



Firewall and Antivirus

- Güvenlik Duvarı ve Antivirüs, ağda kullanılan güvenlik uygulamalarıdır.
- Bir güvenlik duvarı, özel ağlarda intranet olarak yetkisiz erişimi engeller. Ancak virüslere, casus yazılımlara veya reklam yazılımlara karşı koruma sağlamaz.
- Antivirüs, bilgisayarı herhangi bir kötü amaçlı yazılımdan, virüsten, casus yazılımdan veya reklam yazılımdan koruyan bir yazılımdır.
- Bu tür ağ oluşturma mülakat sorularını temel olarak düşünebilirsiniz, ancak görüşülen kişiler hazırlanırken genellikle bu tür ağ oluşturma görüşme sorularını geride bıraktıklarından, bu tür sorular görüşmecilerin favorisidir.

How will you recover data from a Virus-infected system?

- We will install an OS and updated antivirus in a system that is free of any viruses, and then connect the hard drive of the infected system as a secondary drive.
- The hard drive will then be scanned and cleaned. Data can now be copied into the system.

VPN

What is a Virtual Private Network (VPN)?

- A VPN or Virtual Private Network is an encrypted connection (secure tunnel) built on the internet from a device to a network.
- It helps in the creation of a protected network between different networks using the internet (public network), ensuring that sensitive data is safely transmitted.
- This makes it difficult for third parties to gain unauthorized access, track your activities online, or steal data.
- By using the VPN, a client can connect to the organization’s network remotely.

What are the advantages of using a VPN Connection?

Some of the advantages of using VPN Connection are:

- Remote Access
- Protected File Sharing
- Anonymity
- Enhanced Security
- Improved Performance
- Anonymity
- Network Scalability
- Prevents Data Throttling

The different types of VPN.

There are two types of VPNs:

- 1. Remote Access Virtual Private Network
- 2. Site-to-Site or Router-to-Router Virtual Private Network:

Remote Access Virtual Private Network

- A Remote Access VPN securely connects a device (endpoints like laptops, tablets, or smartphones) outside the corporate office. It allows a client to associate with a private network and access every one of its resources and services remotely.
- The connection between the private network and the user happens securely through the Internet.
- It is a low-cost solution and is helpful for both business and home users.

Site-to-Site or Router-to-Router Virtual Private Network:

This VPN is mostly used in large organizations with branches in different locations to connect the network of one office to another in different locations. It has two sub-categories:

- Intranet VPN: Intranet VPN allows several offices of the same company to connect using the Site-to-Site VPN type. It is commonly used for connecting remote offices in different geographical locations using shared infrastructure (internet connectivity and servers) with the same accessibility policies as a private WAN (wide area network).
- Extranet VPN: Extranet VPN allows companies to use Site-to-site VPN type to connect to the office of another company. It uses shared infrastructure over an intranet, suppliers, customers, partners, etc., and connects them using dedicated connections.

Kaynaklar

- Analog Electronics, Bilkent Unıversity
- Electric Circuits Ninth Edition, James W. Nilsson Professor Emeritus Iowa State University, Susan A. Riedel Marquette University, Prentice Hall, 2008.
- Fundamentals of Electrical Engineering, Don H. Johnson, Connexions, Rice University, Houston, Texas, 2016.
- Introduction to Electrical and Computer Engineering, Christopher Batten - Computer Systems Laboratory School of Electrical and Computer Engineering, Cornell University, ENGRG 1060 Explorations in Engineering Seminar, Summer 2012.
- Basics of Electrical Electronics and Communication Engineering, K. A. NAVAS Asst.Professor in ECE, T. A. Suhail Lecturer in ECE, Rajath Publishers, 2010.
- https://www.ics.uci.edu/

Usage Notes

- These slides were gathered from the presentations published on the internet. I would like to thank who prepared slides and documents.
- Also, these slides are made publicly available on the web for anyone to use
- If you choose to use them, I ask that you alert me of any mistakes which were made and allow me the option of incorporating such changes (with an acknowledgment) in my set of slides.

Sincerely,

Dr. Cahit Karakuş

cahitkarakus@gmail.com