



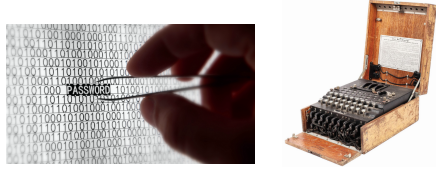
MEB - Öğretmen Yetiştirme ve Geliştirme Genel Müdürlüğü Siber Güvenliğe Giriş Eğitimi 4.DERS 14.04.2020



08.04.2020 – Bölüm 3: Verilerinizi ve Gizliliğinizi Koruma

3.Ders Öğrendiklerimiz! Farkındalıklarımız!

Parola ve Şifre?



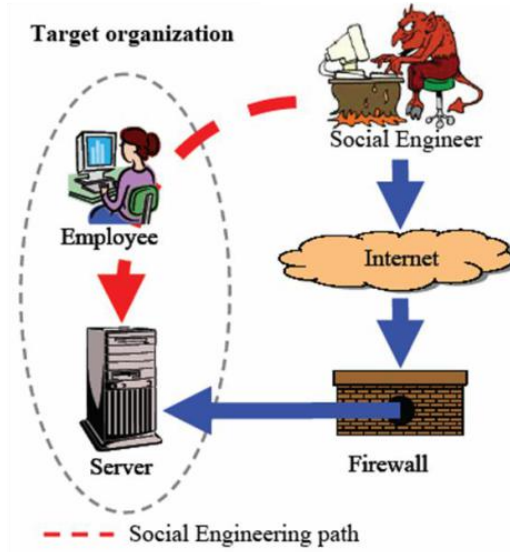
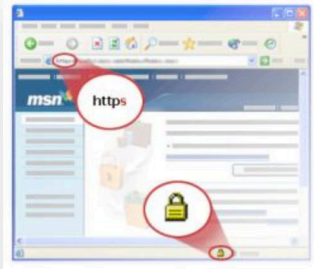
Siber 3.ders tekrar ediyoruz! Si3.teed!

Normal bir siteye girdiğimizde adres çubuğunda gördüğümüz HTTP başlığı interaktif bankacılık gibi kritik işlem yapılan bir siteye girdiğimizde yerini HTTPS olarak değiştirir. Buradaki "S" güvenli (secure) anlamına gelmektedir.

Tarayıcınızın altında bulunan çubukta da kilit ikonu çıkacaktır.

Bunların yanı sıra şifreli iletişimlerde (SSL- Secure Socket Layer) sitenin sahip olduğu **sertifika ve sertifikanın geçerliliği** kontrol edilmelidir.

Örnekler : 1: Firefox - 2: Internet Explorer



Şüpheli davranın!

<https://haveibeenpwned.com/>



Sosyal Mühendislik!

Kevin Mitnick. 56 yaşında (06-08-1963). Gelmiş geçmiş en büyük hacker olarak kabul ediliyor.

5 yıl hapiste kaldıktan sonra 2000 yılında koşullu olarak serbest bırakıldı.

Koşullardan birisi telefona ve bilgisayara dokunmamaktı.

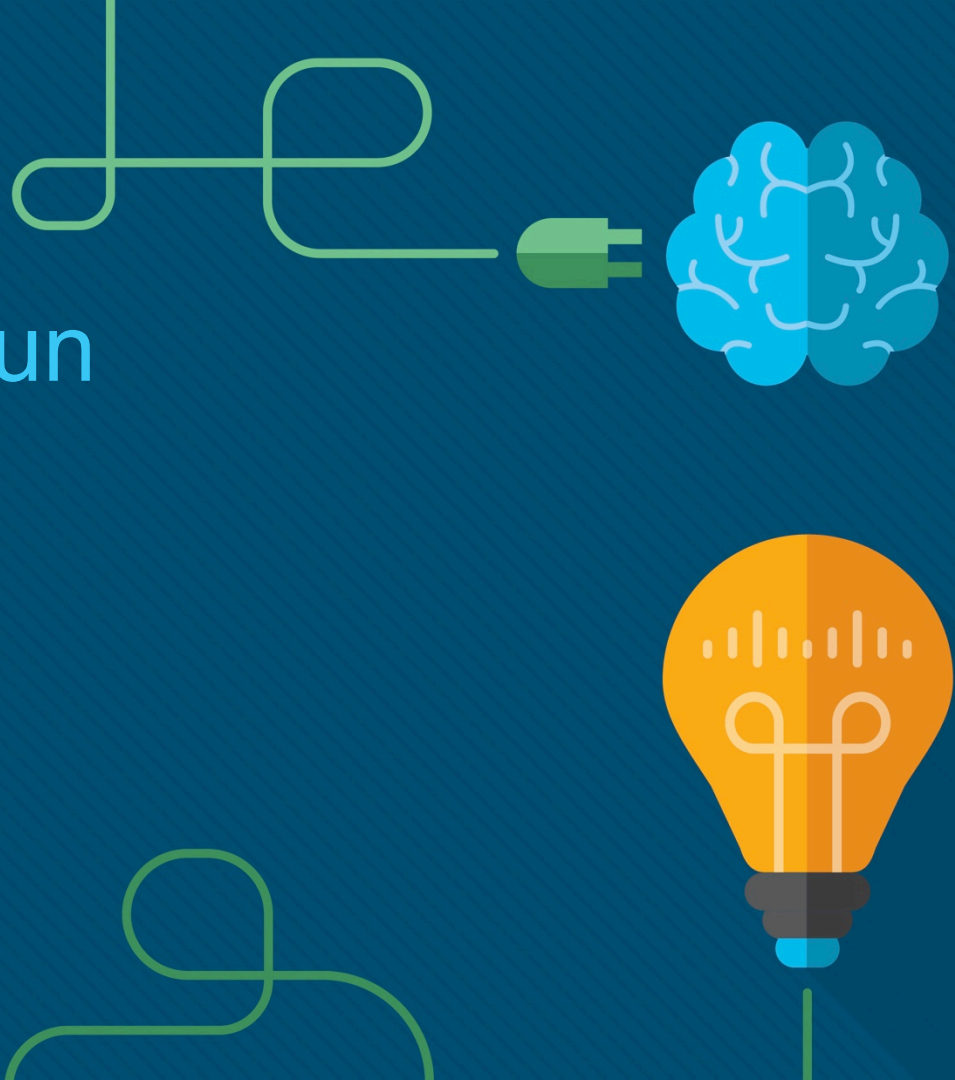
➤Kevin Mitnick!

- “Sosyal Mühendislik Cephaneadaki En Güçlü Silahlardan Biri”
- “İnsan Unsuru Aslında Güvenliğin En Zayıf Halkasıdır”
- “Sorun Makinelerde Değil, İnsan Unsurunda”



Bölüm 4: Kurumun Korunması

Introduction to Cybersecurity v2.1



Bölüm 4 - Bölümler ve Hedefler

- 4.1 Güvenlik duvarları
 - **Kurumları siber saldırılara karşı koruyan teknikleri açıklayın.**
 - Çeşitli güvenlik duvarı türlerini tanımlayın.
 - Farklı tipteki güvenlik cihazlarını tanımlayınız.
 - Gerçek zamanlı saldırı tespiti için farklı yöntemleri tanımlayın.
 - Kötü amaçlı yazılımları tespit etme yöntemlerini açıklayın.
 - Kurumlat için en iyi güvenlik uygulamalarını açıklayın.
- 4.2 **Siber Güvenliğe Davranışsal Yaklaşım**
 - Siber güvenliğe davranışsal yaklaşımı açıkla.
 - Botnet terimini tanımlayın.
 - Öldürme Zinciri (Kill Chain) terimini tanımlar.
 - Davranış tabanlı güvenliği tanımlayın.
 - NetFlow'un siber saldırılara karşı savunmaya nasıl yardımcı olduğunu açıklayın.

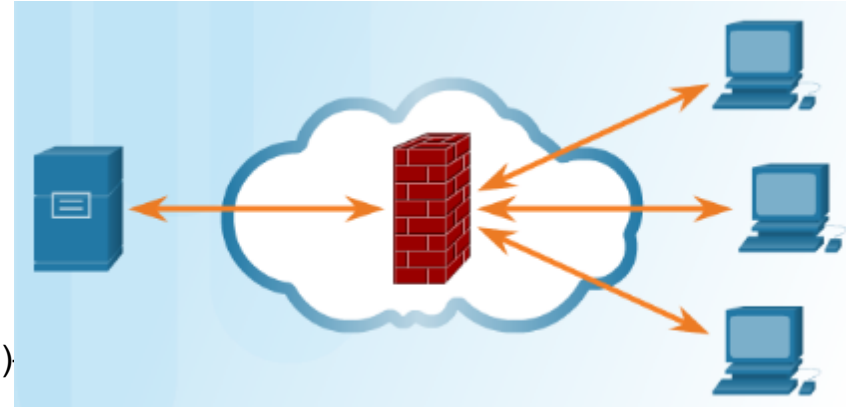
Bölüm 4 - Bölümler ve Hedefler (devam)

- 4.3 Cisco'nun Siber Güvenliğe Yaklaşımı
 - Cisco'nun Siber güvenliğin sağlanmasındaki yaklaşımını açıklayın.
 - Cisco'da CSIRT işlevini tanımlayın.
 - Güvenlik oyun kitabının amacını açıklayın.
 - Olay önleme ve algılama için kullanılan araçları belirleyin.
 - IDS ve IPS'yi tanımlayın.

4.1 Güvenlik Duvarları

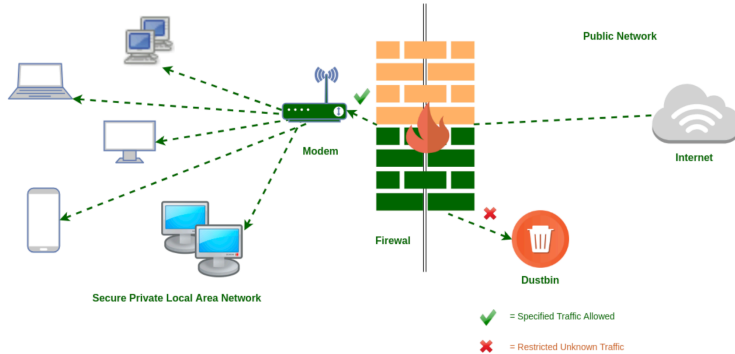
Güvenlik Duvarı Türleri

- Bir ağda veya cihazda gelen veya giden iletişimleri kontrol etme veya filtreleme
- Genel güvenlik duvarı türleri
 - **Ağ Katmanı Güvenlik Duvarı (Network Layer Firewall)**– kaynak ve hedef IP adresleri
 - **Taşıma Katmanı Güvenlik Duvarı (Transport Layer Firewall)**– kaynak ve hedef port numaraları ve bağlantı durumları
 - **Uygulama Katmanı Güvenlik Duvarı (Application Layer Firewall)**– uygulama, program veya hizmet
 - **Bağlam Duyarlı Uygulama Güvenlik Duvarı (Context Aware Application Firewall)** – kullanıcı, cihaz, rol, uygulama türü ve tehdit profili
 - **Proxy Sunucusu**–web içerik istekleri
 - **Ters Proxy Sunucusu (Reverse Proxy Server)**– Web sunucularına erişimi koruyun, gizleyin, boşaltın ve dağıtın
 - **Network Address Translation (NAT) Güvenlik Duvarı** – ağ ana bilgisayarlarının özel adreslerini gizler veya maskeler
 - **Bilgisayar tabanlı Güvenlik Duvarı (Host-based Firewall)** portları ve sistem hizmeti çağrılarının tek bir bilgisayar işletim sisteminde filtrelenmesi



Firewall – 7/24!

Firewall, Network üzerinde kendisine gelen paketlerin ulaşması gereken yerlere (önceden tanımlanmış kurallarla) gidip gidemeyeceğine karar verir. Güvenlik duvarı üzerinde belirtilmiş kuralla uymayan trafiği engelleyerek koruma sağlanır. Ayrıca birçok firewall, kullanıcıların istek paketlerini ağa gitmeden önce karşılayacağı bir Proxy sunucusuna sahip olabilir veya bir Proxy ile birlikte çalışabilirler.



"Güvenlik duvarı bir kokteyle gelen kişilerin davetli olup olmadığını kontrol eden görevli gibidir. Davetli olmayan uygulamaların bilgisayarımıza geçirmesini ve bunların bize zarar vermesini engeller."

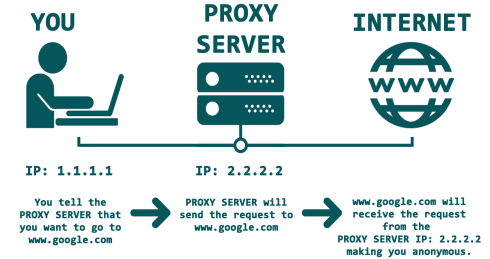
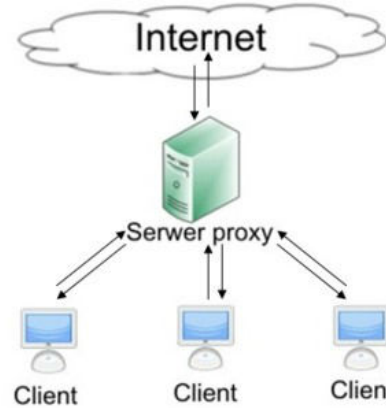
Proxy Sunucusu!

Proxy Nedir?

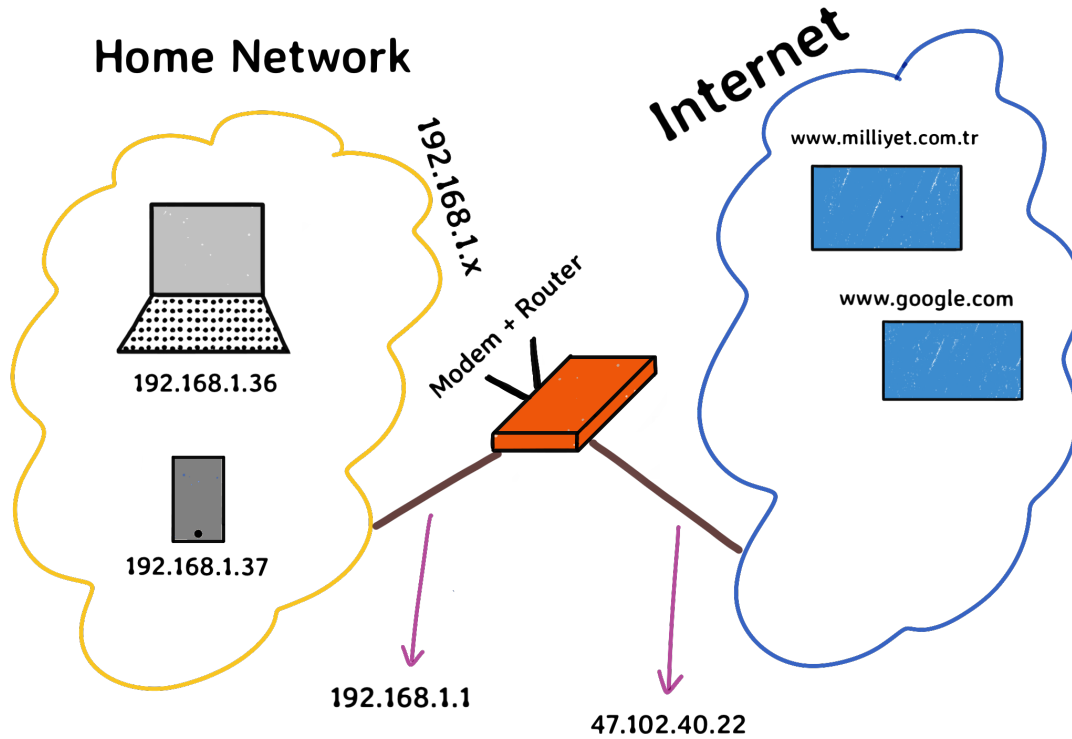
Türkçe kelime anlamı olarak elçi – VEKİL anlamına gelen proxy, herhangi bir ağ sisteminde (internet gibi) cihazların birbirlerine bağlanırken arada bir sunucunun kullanılması işlemine denir ve bu sunucuya geçit (gateway) adı verilir.

Proxy kullanmanın faydaları nelerdir?

- IP adresiniz gizli kalır.
- Engellenmiş içeriklere erişim sağlayabilirsiniz.
- Yükleme süreleri azalabilir.
- Kötü amaçlı web siteleri filtrelenebilir.



Nat! (Network Address Translation)



AAA!

AAA Components

The diagram illustrates the AAA components (Authentication, Authorization, Accounting) in the context of a credit card statement. A callout box labeled 'Authentication' points to the card number on the credit card. A callout box labeled 'Authorization' points to the credit limit on the statement. A callout box labeled 'Accounting' points to the transaction table at the bottom of the statement.

Authentication
Who are you?

Authorization
How much can you spend?

Accounting
What did you spend it on?

Statement of Personal Credit Card Account

Account Number: 1234-567-890 | Statement Closing Date: 01-31-01 | Current Amount Due: \$278.50

JOE EMPLOYEE
456 SKYVIEW DRIVE
HOMETOWN, USA 09900-1234

MAIL PAYMENT TO:
THE BANK
132 VINE STREET
ANYTOWN, USA 07900-0010

672919345 00178255000000003

Detach here and return upper portion with check or money order. Do not staple or fold.

Statement of Personal Credit Card Account
Retain this portion for your files.

Cardmember Name: JOE EMPLOYEE | Account Number: 1234-567-890 | Statement Closing Date: 01-31-01

Statement Date: 02-01-01 | Payment Due Date: 03-01-01

Closing Date: 01-31-01

Credit Limit: \$1,500.00 | Credit Available: \$1221.50

New Balance: \$278.50 | Minimum Payment Due: \$20.00

Account Summary

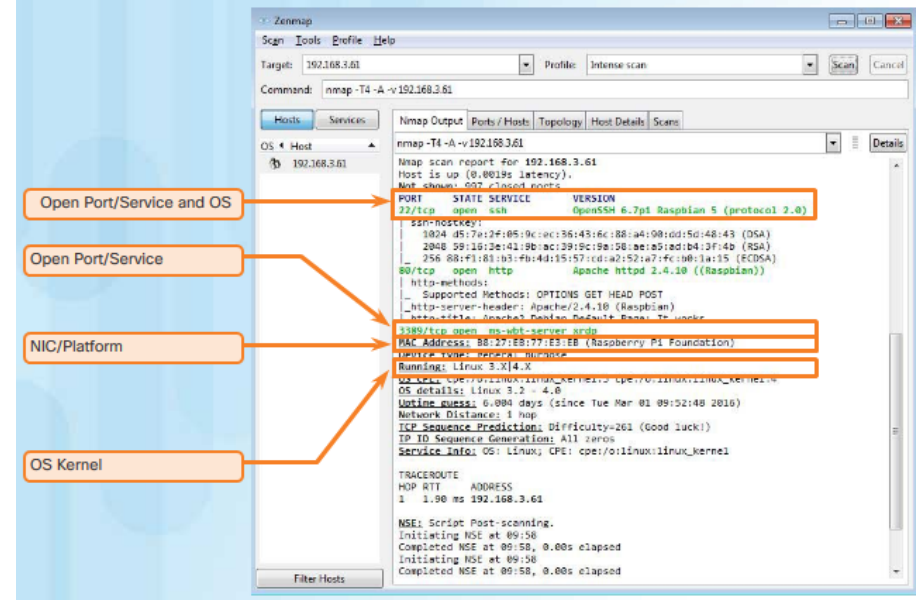
Previous Balance:	+74.24	Transaction Fees:	+3.00
Purchases:	+250.50	Annual Fees:	+25.00
Cash Advances:	+0	Current Amount Due:	+250.50
Payments:	-74.25	Amount Past Due:	+0
Finance Charge:	+0	Amount Over Credit Line:	+0
Late Charge:	+0	NEW BALANCE:	\$278.50

Reference Number	Sold	Posted	Activity Since Last Statement	Amount
43210987	01-03	01-13	Payment, Thank You	-\$74.25
01234567	01-12	01-13	Wings 'N Things Anytown, USA	\$25.25
78901234	01-14	01-17	Record Release Anytown, USA	\$40.00
45678901	01-14	01-17	Sports Stadium Anytown, USA	\$75.25
3210987	01-22	01-23	Tie Tack Anytown, USA	\$20.75
76543210	01-29	01-30	Electronic World Anytown, USA	\$89.25
2345678		01-30	Transaction Fees	\$3.00
34567890		01-01	Annual Fee	\$25.00

Güvenlik Duvarı Türleri

Port Tarama

- Açık port numalarının tespiti için bir bilgisayarı, sunucuyu veya başka bir ağ ana bilgisayarını sorgulama işlemi
- Port numaraları bir aygıtta çalışan her uygulamaya atanır..
- Çalışan işletim sistemini ve hizmetleri tanımlamak için keşif aracı
 - Nmap** – A port scanning tool
- Ortak yanıtlar::
 - Açık veya Kabul Edildi (Open or Accepted)**– port üzerinde bir servis çalışıyor
 - Kapalı, Reddedildi veya Dinlemiyor (Closed, Denied, or Not Listening)** – ilgili porta bağlantılar reddedildi.
 - Filtrelenmiş, Bırakılmış veya Engellenmiş (Filtered, Dropped, or Blocked)** – cihazdan yanıt gelmedi.



Güvenlik Cihazları

Güvenlik Cihazları

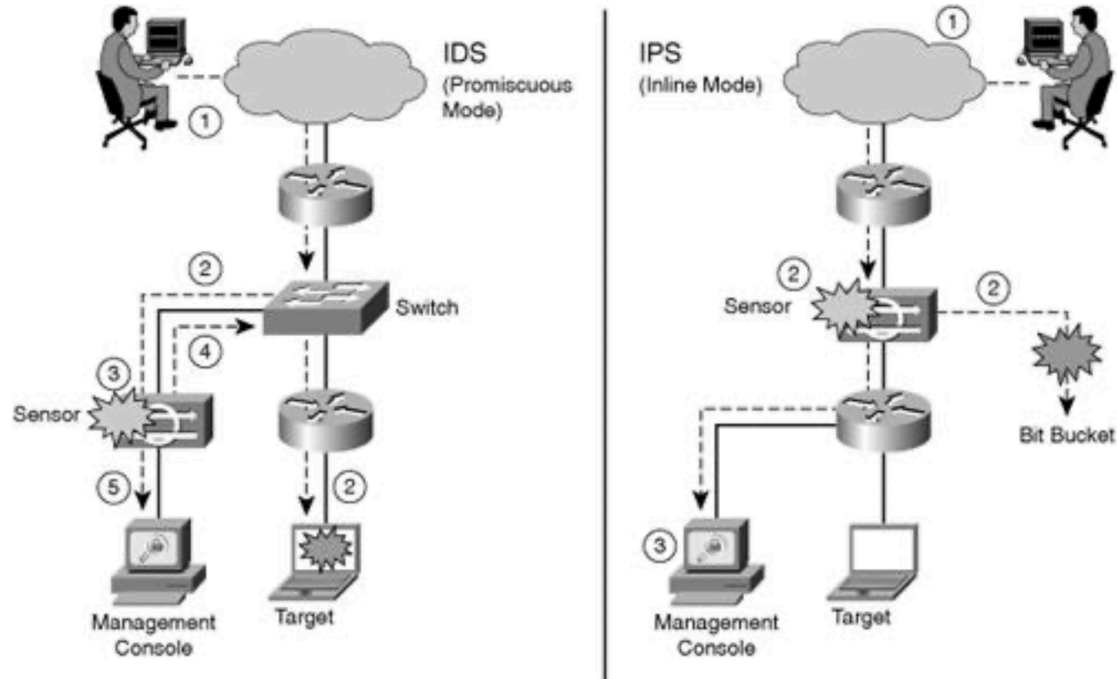
▪ Güvenlik cihazları şu genel kategorilere girer:

- **Yönlendiriciler (Routers)** – birçok güvenlik duvarı özelliğine sahip olabilir: trafik filtreleme, IPS, şifreleme ve VPN.
- **Güvenlik duvarları (Firewalls)** - ayrıca yönlendirici özelliği, gelişmiş ağ yönetimi ve analitiğe sahip olabilir.
- **IPS** – Saldırı Önleme Sistemidir, İzinsiz girişleri önler.
- **VPN** - güvenli şifreli tünelleme için tasarlanmıştır.
- **Kötü Amaçlı Yazılım / Antivirüs (Malware/Antivirus)** - Cisco Advanced Malware Protection (AMP) yeni nesil Cisco yönlendiricileri, güvenlik duvarları, IPS aygıtları, Web ve E-posta Güvenlik Cihazları ile birlikte gelir ve ana bilgisayarlara yazılım olarak da yüklenebilir..
- **Diğer Güvenlik Aygıtları** - web ve e-posta güvenlik aygıtlarını, şifre çözme aygıtlarını, istemci erişim kontrol sunucularını ve güvenlik yönetim sistemlerini içerir.



IPS-IDS!

Monitor for Attacks



Gerçek Zamanlı Saldırı Tespiti

▪ Sıfır gün saldırısı (Zero-day attack)

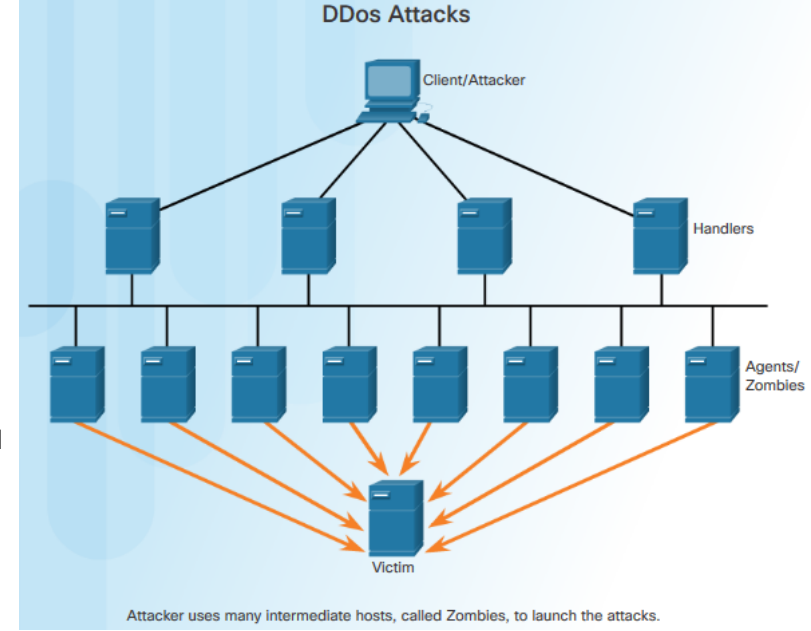
- Bir bilgisayar korsanı, içerik oluşturucusu sorunu çözmeden bir yazılım parçasındaki kusurdan yararlanır.

▪ Uçtan Uca Noktaya Gerçek Zamanlı Tarama (Real Time Scanning from Edge to Endpoint)

- Güvenlik duvarı ve IDS / IPS ağ cihazlarını kullanarak saldırıları aktif olarak tarama
- çevrimiçi küresel tehdit merkezlerine bağlantılar ile saldırı tespiti
- bağlama dayalı analiz ve davranış algılama kullanarak ağ anormalliklerini tespit etme

▪ DDoS Saldırıları ve Gerçek Zamanlı Yanıt (DDoS Attacks and Real Time Response)

- En büyük saldırı tehditlerinden biri olan DDoS, İnternet sunucularını ve ağ kullanılabilirliğini engelleyebilir.
- DDoS, yüzlerce veya binlerce zombi sunucusundan kaynaklanır ve saldırılar yasal trafik olarak görünür.



En İyi Güvenlik Uygulamaları

En İyi Güvenlik Uygulamaları

▪ Yayınlanmış Bazı En İyi Güvenlik Uygulamaları:

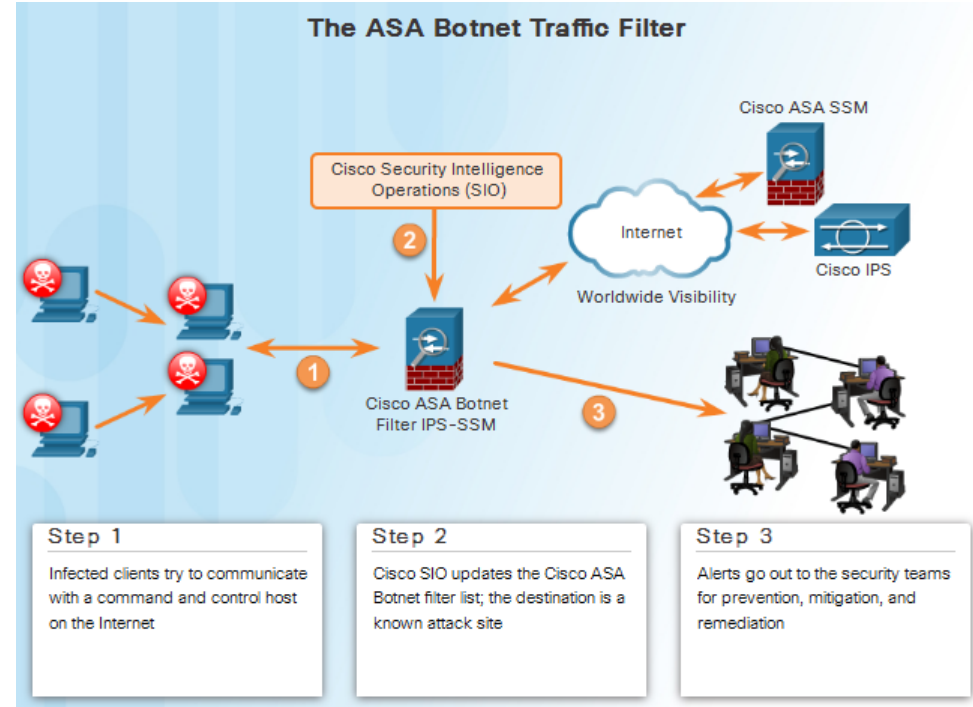
- **Risk Değerlendirmesi Yapın**– Koruduğunuz şeyin değerini bilmek, güvenlik harcamalarını haklı çıkarmanıza yardımcı olacaktır.
- **Ağ Güvenlik Aygıtlarını Kullanın**– Yeni nesil yönlendiricileri, güvenlik duvarlarını ve diğer güvenlik aygıtlarını kullanın..
- **Güvenlik Politikası Oluşturun**– Şirket kurallarını, iş görevlerini ve beklentilerini açıkça belirten bir politika oluşturun..
- **Fiziksel Güvenlik Önlemleri**– Ağ kabinetlerine, sunucu konumlarına ve yangın söndürmeye erişimi kısıtlayın..
- **İnsan Kaynakları Güvenlik Önlemleri** – Çalışanlar arka plan kontrolleri ile iyi bir şekilde araştırılmalıdır.
- **Yedekleme Alma ve Test Etme**– Düzenli yedeklemeler gerçekleştirin ve yedeklemelerden veri kurtarmayı test edin..
- **Güvenlik Yamalarını ve Güncellemeleri Yükleyin**– Sunucu, istemci ve ağ cihazı işletim sistemlerini ve programlarını düzenli olarak güncelleyin.
- **Erişim Denetimlerini Kullanın**– Güçlü bir kimlik doğrulaması kullanın. Kullanıcı rollerini ve yetki seviyelerini tanımlayın.
- **Olay Yanıtını Düzenli Olarak Test Edin**– Bir olay müdahale ekibi oluşturun ve acil müdahale senaryolarını test edin.
- **Ağ İzleme, Analiz ve Yönetim Aracı Kurun**- Diğer teknolojilerle entegre olan bir güvenlik izleme çözümü seçin.
- **Kapsamlı Bir Uç Nokta Güvenlik Çözümü uygulayın** – Kurumsal düzeyde kötü amaçlı yazılımdan koruma ve virüsten koruma yazılımı kullanın..
- **Kullanıcıları Eğitin**– Kullanıcıları ve çalışanları güvenli prosedürlerle eğitin..
- **Verileri şifreleyin**– E-posta dahil tüm hassas şirket verilerini şifreleyin.

4.2 Siber Güvenliğe Davranışsal Yaklaşım

Botnet

Botnet

- Botnet
 - İnternet üzerinden bağlanan bir grup bot
 - Kötü niyetli kişiler veya gruplar tarafından kontrol edilir
- Bot
 - Genellikle bir web sitesini ziyaret ederek, e-posta ekini açarak veya zararlı yazılım içeren bir medya dosyasını açarak bulaşır



Kill Chain (Ölüm Zinciri)

Siber Savunmada Ölüm Zinciri

Kill Chain, bir bilişim sistemleri saldırısının aşamalarıdır.

1. Keşif (Reconnaissance) – Bilgi Toplar

2. Silahlanma (Weaponization)

- Hedefe yönelik istismar ve kötü niyetli yük oluştur

3. İletme (Delivery)

- İstismar ve kötü amaçlı yükü hedefe gönderir

4. Sömürme (Exploitation)

- İstismarı yürütür

5. Yükleme (Installation)

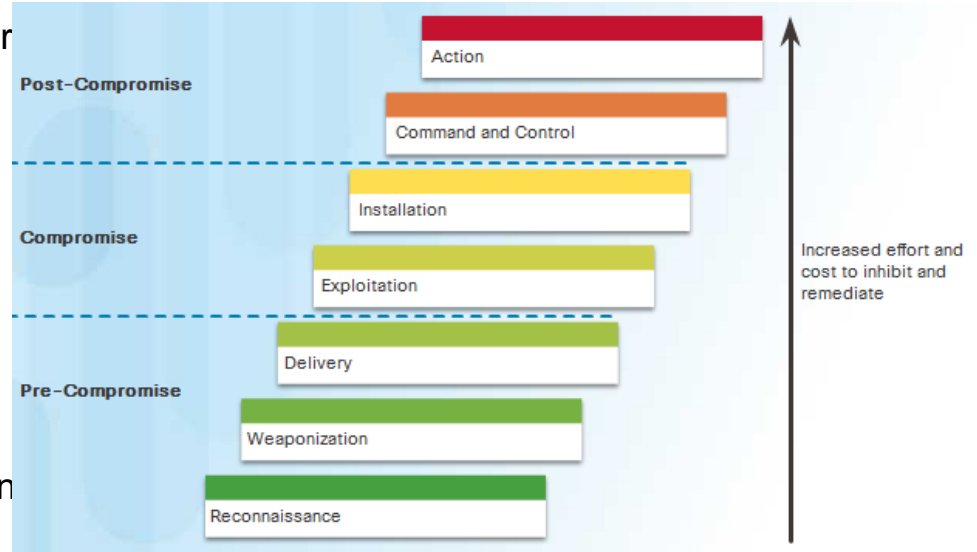
- Kötü amaçlı yazılımları ve arka kapıları yükler

6. Komuta & Kontrol (Command & Control, C2)

- Bir komut ve kontrol kanalından veya sunucudan uzaktan kontrol.

7. Eylem (Actions On Objectives)

- Diğer aygıtlara kötü amaçlı eylemler veya ek saldırılar gerçekleştirir

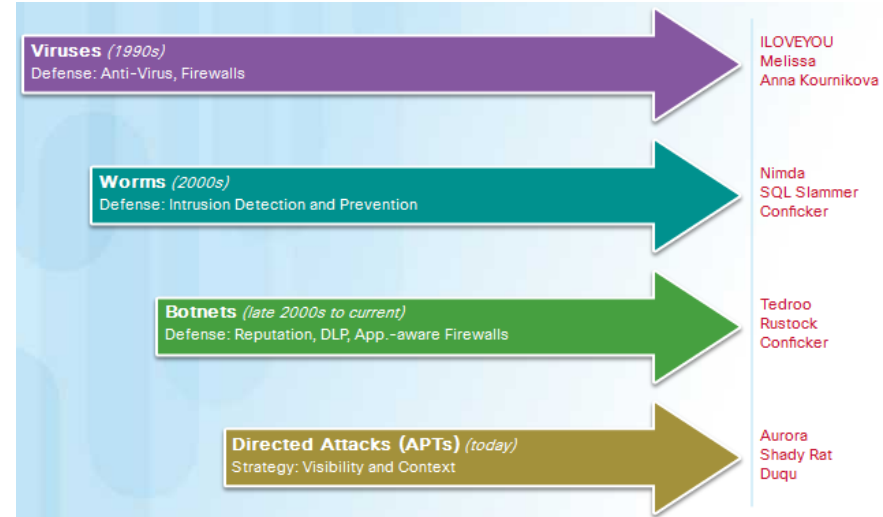


Faz	Açıklama
Keşif	Hedefe ait e-posta adresleri tespit edilir.
Silahlanma	Zararlı doc dosyası hazırlanır.
İletme	E-Posta yolu ile zararlı doc dosyası hedefe gönderilir
Sömürme	CVE-2017-8570 zafiyeti istismar edilir.
Yükleme	Zararlı kendini registry dosyasına ekler.
	HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Run
Komuta & Kontrol	HTTPS ile xx.77.87 ile haberleşir
Eylem	Kurumsal veri içeren dosyaları komuta kontrol merkezine gönderir.

Cyber Kill Chain aşamalarına örnekler

Davranış Odaklı Güvenlik

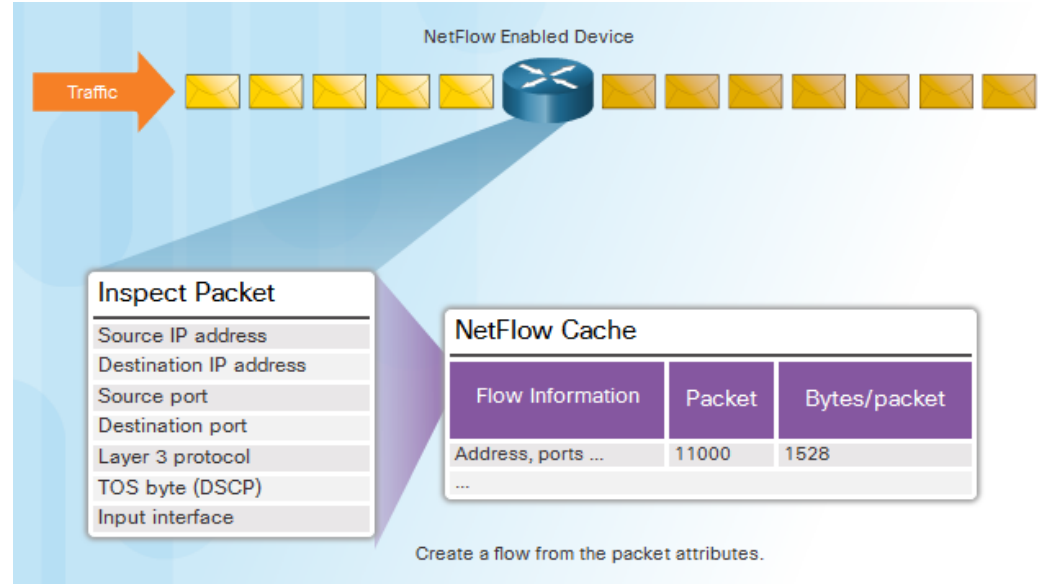
- Honeypots (Bal Küpü)
 - Saldırganın tahmin edilebilir davranışına hitap ederek saldırganı cezbeder
 - Saldırganların davranışlarını yakalar, kaydeder ve analiz eder
 - Yönetici daha fazla bilgi edinebilir ve daha iyi savunma yapabilir
- Cisco'nun Siber Tehdit Savunması Çözüm Mimarisi
 - Davranış tabanlı algılama ve göstergeleri kullanır
 - Daha fazla görünürlük, bağlam (context) ve kontrol sağlar



NetFlow and Siber Saldırıları

Netflow

- Ağ üzerinden akan veriler hakkında bilgi toplama
- Davranış tabanlı tespit ve analizdeki önemli bileşenler barındırır
- Temel davranışları belirler



4.3 Cisco'nun Siber Güvenliğe Yaklaşımı

CSIRT -Computer Security Incident Response Team

▪ CSIRT = SOME (Siber Olaylara Müdahale Ekibi)

- Bilgisayar güvenliği olaylarıyla ilgili kapsamlı araştırmalar yaparak şirket, sistem ve veri korumasının sağlanmasına yardımcı olur
- **proaktif tehdit değerlendirmesi**, etki azaltma planlaması, olay eğilimi analizi ve güvenlik mimarisi incelemesi sağlar



SOC !

SOC Nedir?

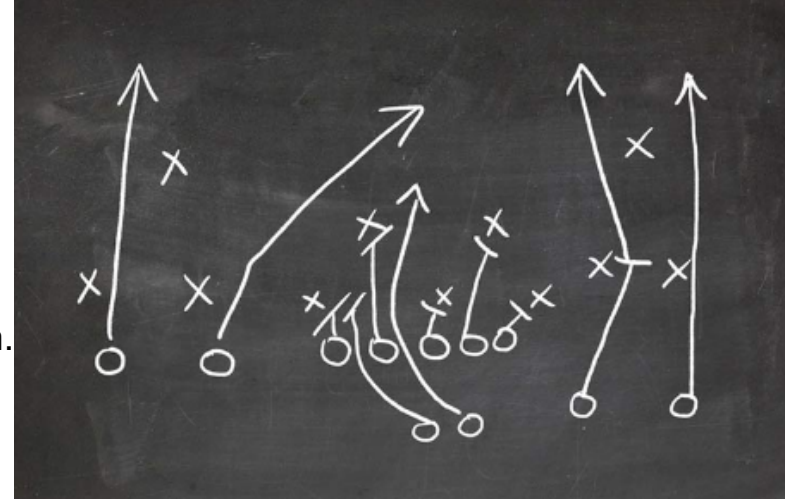
Bir kurumun tüm bilişim alt yapısını 7/24 izleyerek bir anormallik varmı, bir saldırı gerçekleşiyor mu gözlemleme ekibi.



SOC 1975 / Kaynak Wiki

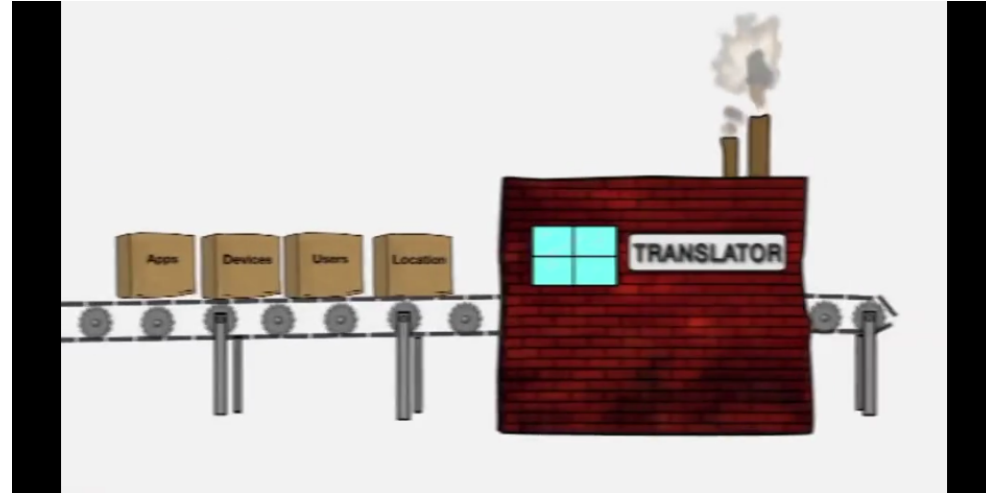
Güvenlik Oyun Kitabı (Security Playbook)

- Olay tespiti ve yanıtına yol açan güvenlik olayı veri kaynaklarına karşı tekrarlanabilir sorguların toplanması
- Neyi başarmaya çalışıyor?
 - Kötü amaçlı yazılım bulaşmış makineleri tespit edin.
 - Şüpheli ağ etkinliğini tespit edin.
 - Düzensiz kimlik doğrulama girişimlerini tespit edin.
 - Gelen ve giden trafiği tanımlayın ve anlayın.
 - Eğilimler, istatistikler ve sayımlar dahil özet bilgiler sağlayın.
 - İstatistiklere ve metriklere kullanılabilir ve hızlı erişim sağlayın..
 - Etkinlikleri tüm ilgili veri kaynaklarıyla ilişkilendirin.



Olay Önleme ve Tespit Araçları

- SIEM – Tehdit ve Olay Yönetimi (Security Information and Event Management)
 - Ağdaki güvenlik cihazlarından güvenlik uyarılarını, günlükleri ve diğer gerçek zamanlı ve geçmiş verileri toplayan ve analiz eden yazılım
- DLP – Veri Kaybını Önleme (Data Loss Prevention)
 - Hassas verilerin çalınmasını veya ağdan kaçmasını engeller
 - Verileri izlemek ve korumak için üç farklı durum tasarımı içerir
- **Cisco Identity Services Engine** (Cisco ISE) ve **TrustSec**
 - Rol tabanlı erişim kontrol politikalarını kullanır



IDS ve IPS

IDS ve IPS

▪ IDS - Saldırı Tespit Sistemi (Intrusion Detection System)

- Genellikle çevrimdışı çalıştırılır.
- Saldırıları engellemez.
- Saldırıları Tespit Eder, Log Gönderir ve Raporlar

▪ IPS – Saldırı Önleme Sistemi (Intrusion Prevention System)

- Pozitif bir kurala veya imza eşleşmesine dayalı olarak trafiği engelleme veya reddetme yeteneği barındırır.

▪ IDS/IPS sistemleri

- **Snort**
- **Sourcefire (Cisco)**

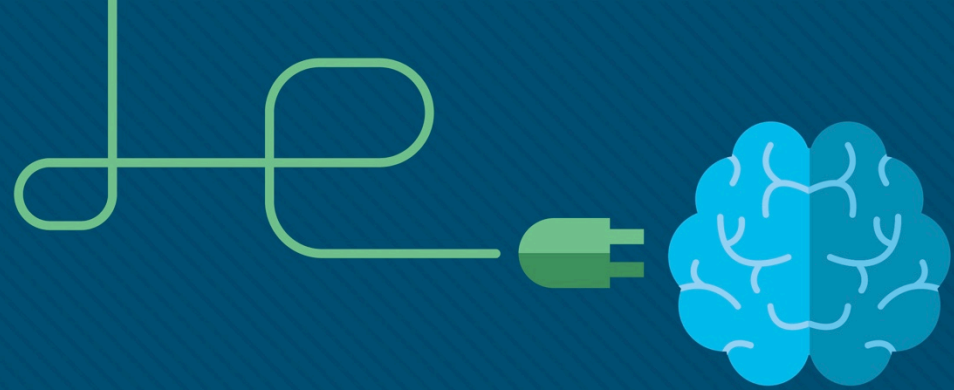


4.4 Bölüm Özeti

Özet

Bölüm Özeti

- Çeşitli güvenlik duvarı tiplerini ve güvenlik cihazlarını tanımlayın.
- Gerçek zamanlı olarak kötü amaçlı yazılımları ve saldırıları tespit etmek için kullanılan farklı yöntemleri açıklayın.
- Kuruluşlar için en iyi güvenlik uygulamalarını açıklayın.
- Botnet, kill chain ve davranışa dayalı güvenliği tanımlayın.
- Netflow'un siber saldırılara karşı savunmaya nasıl yardımcı olabileceğini açıklayın.
- Cisco'da CSIRT işlevini tanımlayın.
- Security Playbook'un amacını açıklayın.
- Olay önleme ve olay algılama için kullanılan araçları tanımlayın.
- IDS (Saldırı Tespit Sistemi) ve IPS'i (Saldırı Önleme Sistemi) tanımlayın.



Bölüm 5: Geleceğiniz Siber Güvenlikte mi Olacak??

Introduction to Cybersecurity v2.1

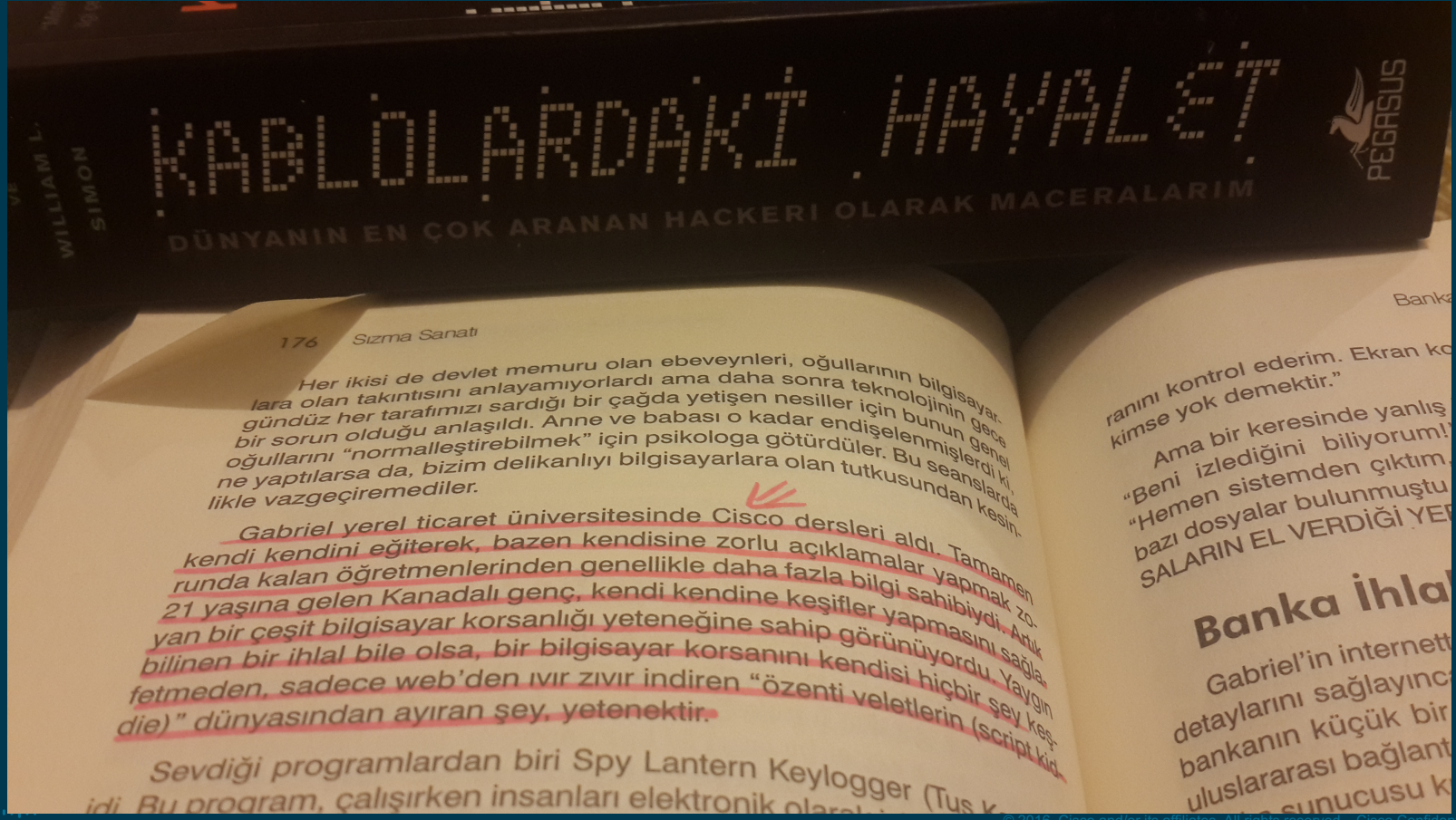


Bölüm 5 - Bölümler ve Hedefler

- 5.1 Siber Güvenlik Eğitimi ve Kariyer
 - Siber güvenlik profesyonellerinin karşılaştığı yasal ve etik sorunları açıklayın
 - Bir siber güvenlik uzmanının karşılaştığı yasal ve etik sorunları tanımlayın..

5.1 Siber Güvenlik Eğitimi ve Kariyer

KİTAP! – SIZMA SANATI!



Siber Güvenlik Kariyerlerinde Yasal ve Etik Sorunlar

Siber Güvenliğin Hukuki Sorunları

- Kişisel Yasal Sorunlar
 - Be responsible with your skills
- Kurumsal Yasal Konular
 - İşletmelerin siber güvenlik yasalarına uymaları gerekmektedir.
 - Yasayı çiğnerseniz, işinizi kaybedebilirsiniz ve şirketiniz cezalandırılabilir.
 - Emin olmadığınızda hukuk departmanına danışmalısınız.
- Uluslararası Hukuk ve Siber Güvenlik
 - ETKİ
 - dünya hükümetleri, endüstrileri ve akademinin küresel ortaklığı
 - Siber tehditlerle uğraşırken küresel yeteneklerin geliştirilmesi



Etik nedir?

Genellikle medyada bir meslek kurallarına gönderme yaparken duyarız.

- “ Etik olarak doğru mu ? “
- Etik kelimesi köken olarak Eski Yunan'a kadar gider .
- Türkçe' de buna karşılık Ahlak ve Töre kelimesi kelimeleri vardır
- Etik evrenseldir. Evrensel kabul gören kurallardır.

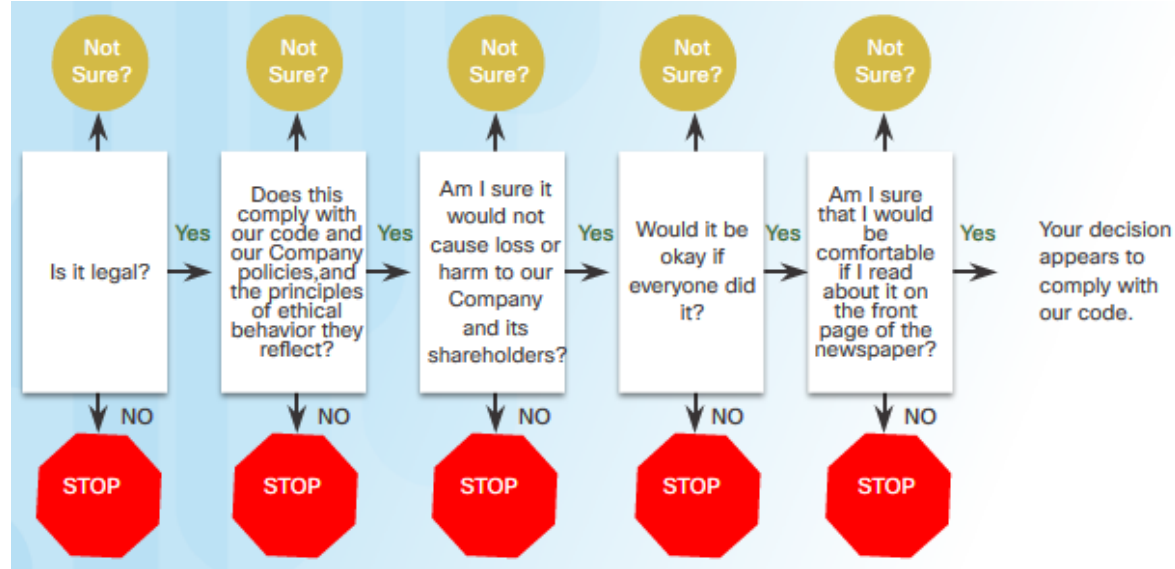
Örnekler

- Okulda kopya çekmek bir suçtur. Peki yakalanmazsa bile bu yaptığı etik olacak mıdır?
(Öğrenci etiği)
- Bir kaza görüp yardım etmemek, teknik olarak suç değil ancak etik mi?
- Kilidi açık bırakılan bir telefonu sahibinden habersiz kurcalamak, etik mi?

Siber Güvenlik Kariyerlerinde Yasal ve Etik Sorunlar

Siber Güvenlikte Etik Konular

- Kişisel Etik Konular
 - Yasal davranış hala etik dışı olabilir.
- Kurumsal Etik Konular
 - Etik bazen yasalar tarafından uygulanan davranış kodlarıdır.
 - Yayınlanmış Etik Kodları Olan Kuruluşlar:
 - **The CyberSecurity Institute (CSI)**
 - **The Information Systems Security Association (ISSA)**
 - **The Association of Information Technology Professionals (AITP)**



Siber Güvenlik Kariyerlerinde Yasal ve Etik Sorunlar

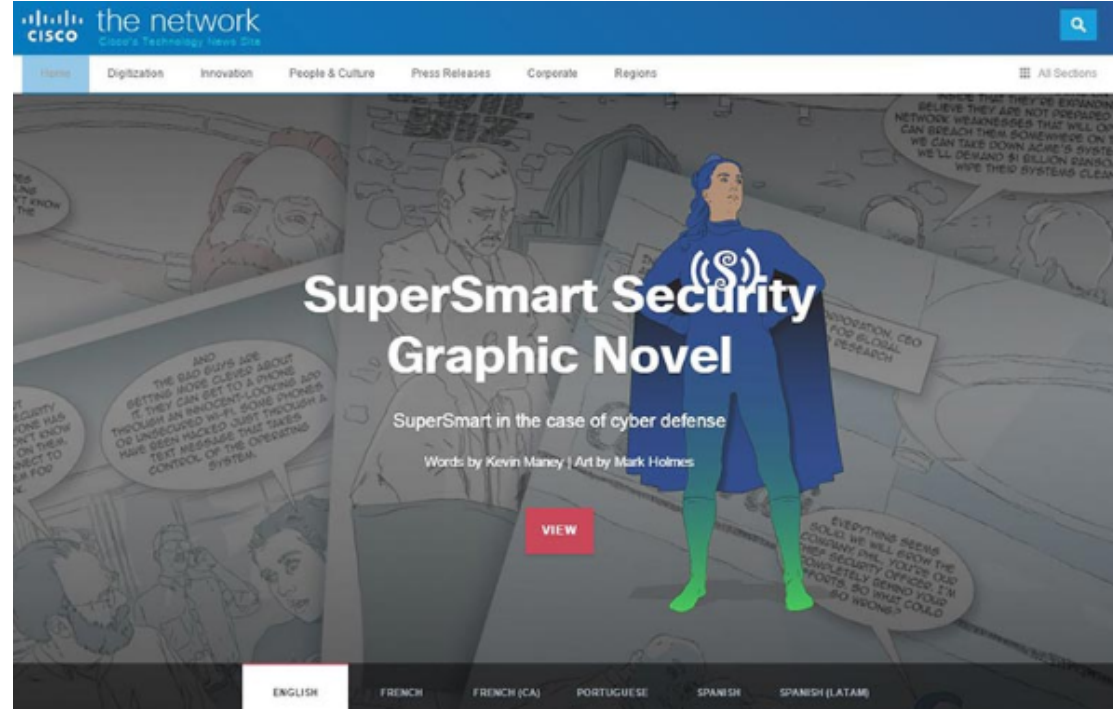
Siber Güvenlikte Kariyer

- Bazı çevrimiçi iş arama motorları

- **ITJobMatch**
- **Monster**
- **CareerBuilder**

- Farklı siber güvenlik işleri

- Sızma testi / etik hacker
- Güvenlik yöneticisi
- Ağ yöneticisi
- Sistem yöneticisi



5.1 Bölüm Özeti

Özet

Bölüm Özeti

- Yasal ve etik konuları açıklar.

TEŞEKKÜRLER
Arzu KİLİTÇİ CALAYIR

<https://medium.com/@arzukilitcicalayir>



Kaynak : Cisco Ağ Akademisi
(<https://www.netacad.com/portal/teaching>)

Kaynak - Çeviri: Ağ Yöneticileri Derneği
(<http://www.agyoneticileri.org/>)

http://www.bilgimikoruyorum.org.tr/?b400_internet-ve-ag-guvenligi

14.04.2020