



MEB - Öğretmen Yetiştirme ve Geliştirme Genel Müdürlüğü Siber Güvenliğe Giriş Eğitimi 1.DERS 01.04.2020



Introduction to Cybersecurity v2.1

MEB - Öğretmen Yetiştirme ve Geliştirme Genel Müdürlüğü

Siber Güvenliğe Giriş Eğitimi

(01.04.2020 – 17.04.2020)

Ben Kimim?

Arzu KİLİTÇİ CALAYIR

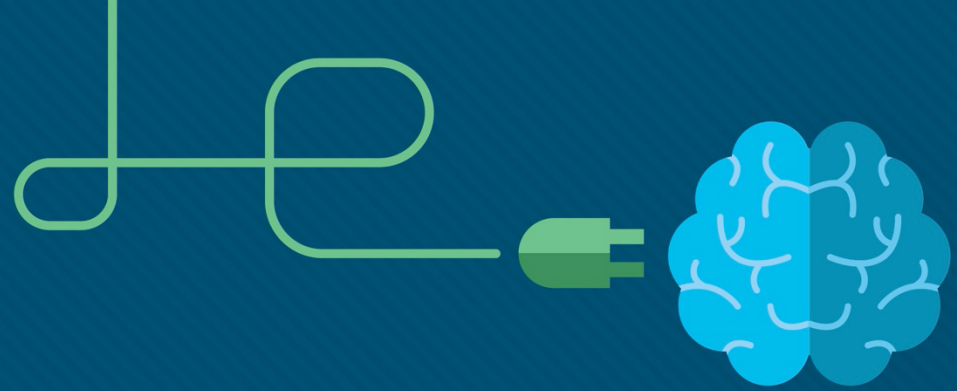
CCNA #13397441

Cisco Ağ Akademisi Eğitmen Eğiticisi



www.arzukilitci.com





Bölüm 1: Siber Güvenlik Gereksinimi

Introduction to Cybersecurity v2.1



Bölüm 1 - Bölümler ve Hedefler

■ 1.1 Kişisel Veri

- Kişisel verilerin özelliklerini ve önemini açıklayın.
 - Kişisel verileri tanımlayın.
 - Kişisel verilerin bilgisayar korsanları (hacker) için neden karlı olduğunu açıklayın.

■ 1.2 Kurum Verileri

- Kurum içindeki verilerin özelliklerini ve önemini açıklayın.
 - Hükümetler ve Kurumlar tarafından kullanılan veri türlerini açıklayın.
 - Güvenlik ihlallerinin etkisini açıklayın.

■ 1.3 Saldırganlar ve Siber Güvenlik Uzmanları

- Siber saldırganların özelliklerini, motivasyonlarını ve siber güvenlik profesyonellerinin yasal ve etik konularını açıklayın.
 - Bir saldırganın özelliklerini ve motivasyonunu açıklayın.

■ 1.4 Siber Savaş (Cyberwarfare)

- Siber savaşın özelliklerini ve amacını açıklayın.
 - Siber savaşı açıklayın

1.1 Kişisel Veri

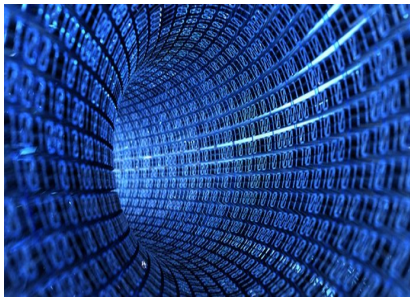
Kişisel Veri

Kişisel Verilere Giriş

Çevrimiçi ve Çevrimdışı Kimliğiniz

- Çevrimdışı Kimliğiniz
 - Evde, okulda veya işte düzenli olarak etkileşim kuran kimliğiniz
- Çevrimiçi Kimliğiniz
 - Siber alandayken kimliğiniz
 - Hakkınızda yalnızca sınırlı miktarda bilgi açıklamalısınız
 - Kullanıcı adı veya takma ad
 - Hiçbir kişisel bilgi içermemelidir
 - Uygun ve saygılı olmalı
 - İstenmeyecek şekilde dikkat çekmemelidir





Siber Nedir?

Siber terimi sibernetik kökeninden gelmektedir. İlk olarak 1958 yılında, canlılar ve/veya makineler arasındaki iletişim disiplini inceleyen Sibernetik biliminin babası sayılan Louis Couffignal tarafından kullanılmıştır.

Siber sadece Internet DEĞİLDİR, çok daha fazlasıdır.

Ağlar Internet'e bağlı olabildiği gibi olmayabilir de,
(bu bir zorunluluk değildir!)

Örnekler:

- SCADA (Süreç Kontrol Ağları) ,GPS Uydu Sistemleri, Metro ..vb

Siber Uzay Nedir?

- ❖ Her çeşit dijital ve elektronik aktiviteler,
- ❖ Ağa bağlı aktiviteler,
- ❖ Bir dijital ağ üzerinden yapılan aktiviteler,
- ❖ Dijital ağlar aracılığıyla erişilen içerikler / bilgiler

Kişisel Veri

Kişisel Verilere Giriş

- Verileriniz
 - Tıbbi Kayıtlar
 - **Elektronik Sağlık Kayıtları (EHR)** - fiziksel, zihinsel ve diğer kişisel bilgiler
 - Reçeteler
 - Eğitim Kayıtları
 - Notlar, sınav puanları, alınan dersler, ödüller ve dereceler
 - Devamlılık
 - Disiplin raporları
 - İstihdam ve Finansal Kayıtlar
 - Gelir ve giderler
 - Vergi kayıtları - maaş çekleri, **kredi kartı ekstreleri**, kredi notu ve bankacılık ekstreleri
 - Geçmiş istihdam ve performans



Kişisel Veri

Kişisel Verilere Giriş

- Verileriniz Nerede?
 - Tıbbi kayıtlar: doktor ofisi, sigorta şirketi
 - Mağaza sadakat kartları
 - Mağazalar alışverişlerinizi topluyorlar
 - Pazarlama iş ortakları profil bilgilerini size özel reklam için kullanıyor
 - Çevrimiçi resimler: arkadaşlar, öğrenciler,yabancılarda da bir kopyası olabilir
- Bilgisayarlarınız ve Cep Telefonlarınız
 - Veri depolama ve çevrimiçi verilerinize açılan portal
 - Bilgi işlem cihazlarınızın bazı örneklerini sıralayın



KVKK Madde 10: Veri sorumlusunun aydınlatma yükümlülüğü



- Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere; a) Veri sorumlusunun ve varsa temsilcisinin kimliği, b) Kişisel verilerin hangi amaçla işleneceği, c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabilceği, ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi, d) 11 inci maddede sayılan diğer hakları, konusunda bilgi vermekle yükümlüdür.

KVKK Madde 11 : İlgili kişinin hakları

Herkes, **veri sorumlusuna başvurarak kendisiyle ilgili**; a) Kişisel veri işlenip işlenmediğini öğrenme, b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme, c) Kişisel verilerin **işlenme amacını** ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, ç) **Yurt içinde veya yurt dışında** kişisel verilerin aktarıldığı üçüncü kişileri bilme, d) Kişisel verilerin **eksik veya yanlış işlenmiş** olması hâlinde bunların düzeltilmesini isteme, 12305 e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme, f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme, g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme, ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme, haklarına sahiptir.

KVKK Madde 12: Veri güvenliğine ilişkin yükümlülükler

- (1) Veri sorumlusu; a) Kişisel verilerin **hukuka aykırı olarak işlenmesini önlemek**, b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek, c) Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır. (2) Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur. (3) Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır. (4) Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılımlarından sonra da devam eder. (5) İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.

KVKK Yaptırımları:

- Suçlar MADDE 17- (1) Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk **Ceza Kanununun 135 ila 140 ıncı madde hükümleri uygulanır.** (2) Bu Kanunun 7 nci maddesi hükmüne aykırı olarak; **kişisel verileri silmeyen veya anonim hâle getirmeyenler** 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır. (Yetkisiz başkasına verilmesi :2-4 Yıl)
- Kabahatler MADDE 18- (1) Bu Kanunun; a) **10 uncu maddesinde öngörülen aydınlatma yükümlülüğünü** yerine getirmeyenler hakkında 5.000 Türk lirasından 100.000 Türk lirasına kadar, b) **12 nci maddesinde öngörülen veri güvenliğine ilişkin yükümlülükleri** yerine getirmeyenler hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar, c) 15 inci maddesi uyarınca Kurul tarafından verilen kararları yerine getirmeyenler hakkında 25.000 Türk lirasından 1.000.000 Türk lirasına kadar, ç) 16 ncı maddesinde öngörülen Veri Sorumluları Siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler hakkında 20.000 Türk lirasından 1.000.000 Türk lirasına kadar, idari para cezası verilir. (2) Bu maddede öngörülen idari para cezaları veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanır. (3) Birinci fıkrada sayılan eylemlerin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi hâlinde, Kurulun yapacağı bildirim üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılır ve sonucu Kurula bildirilir

Kişisel Veri

Siber Güvenlik nedir?



Ağa bağlı sistem ve verilerin yetkisiz kullanım veya zarardan korunması

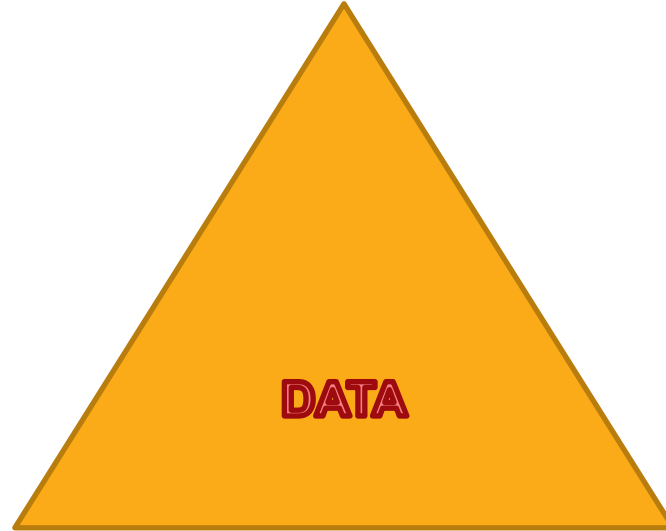
Bilginin Güvenliği Nedir ve Neden Gereklidir?

Bilgi güvenliği, bir varlık türü olarak bilginin **izinsiz** veya **yetkisiz** bir biçimde erişim, kullanım, değiştirilme, ifşa edilme, ortadan kaldırılma, el değiştirme ve hasar verilmesini önlemek olarak tanımlanır.

Kısaca bir bilginin istenmeyen kişilerin eline geçmemesi ve bizim için bir zafiyet oluşturmaması için gereklidir, önemlidir.

Bilgi Güvenliği Üçgeni

Gizlilik
Confidentiality



Bütünlük

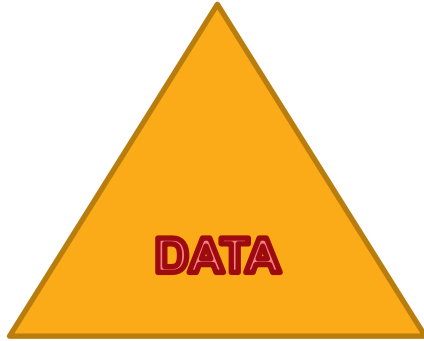
Integrity

Kullanılabilirlik

Availability

Gizlilik

Confidentiality



Bütünlük Kullanılabilirlik

Integrity

Availability

Gizlilik :

Bilginin yetkisiz kişilerin eline geçmemesidir.

Bütünlük :

Bilginin yetkisiz kişiler tarafından değiştirilmemesidir.

Kullanılabilirlik :

Bilginin ilgili ya da yetkili kişilerce ulaşılabilir ve kullanılabilir durumda olmasıdır.

Veri Ne Zaman Güvenli Kabul Edilir?

- Gizlilik
- Bütünlük
- Erişilebilirlik



Amaç bunların sağlanması,
Yani bunları engellemek isteyenler var!

Kişisel Veri

Hedef Olarak Kişisel Veriler

- Neden kimliğini istiyorlar?
 - Uzun vadeli kârlar
 - Tıbbi faydalar
 - Sahte vergi beyannamesi gönderme
 - Kredi Kartı hesapları açma
 - Kredi alma
- Suçlular paranızı nasıl alıyor?
 - Çevrimiçi kimlik bilgileri
 - Hırsızların hesaplarınıza erişmesini sağlar
 - Yaratıcı entrikalar
 - Arkadaşlarınıza veya ailenize para gönderme kandırmacısı



1.2 Kurum Verileri

Kurum Verilerine Giriş

▪ Kurum Veri Türleri

• Geleneksel Veriler

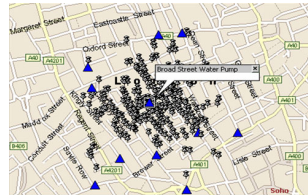
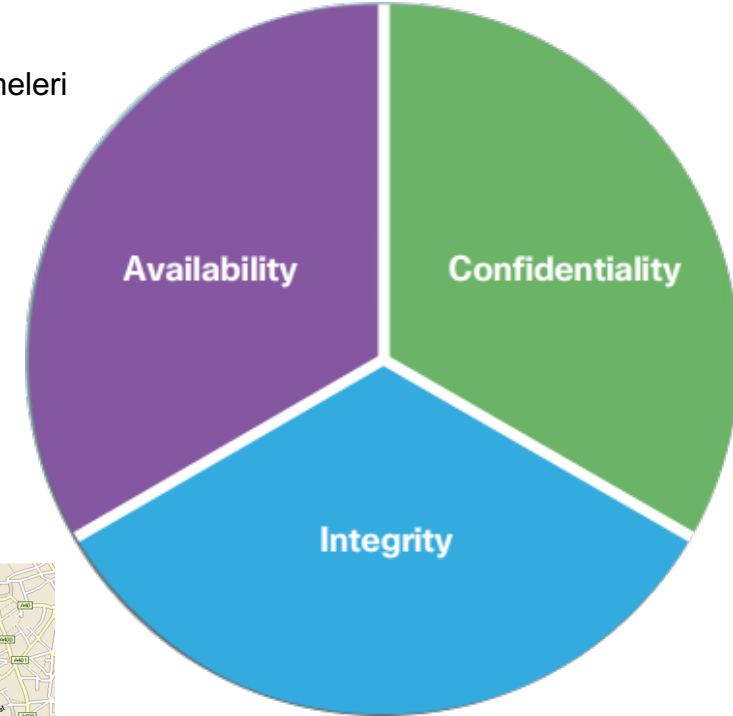
- Personel – başvuru materyalleri, bordro, teklif mektubu, çalışan sözleşmeleri
- Entelektüel – patentler, ticari markalar, ürün planları, ticari sırlar
- Finansal – gelir tabloları, bilançolar, nakit akım tabloları

• Nesnelerin İnterneti (IoT) ve Büyük Veri (Big Data)

- IoT – sensörler gibi geniş fiziksel nesneler ağı
- [Büyük Veri](#) – IoT'den verileri

▪ Gizlilik (C), Bütünlük (I) ve Kullanılabilirlik (A)

- Gizlilik – mahremiyet
- Bütünlük – bilgilerin doğruluğu ve güvenilirliği
- Kullanılabilirlik - bilgiye erişilebilirlik



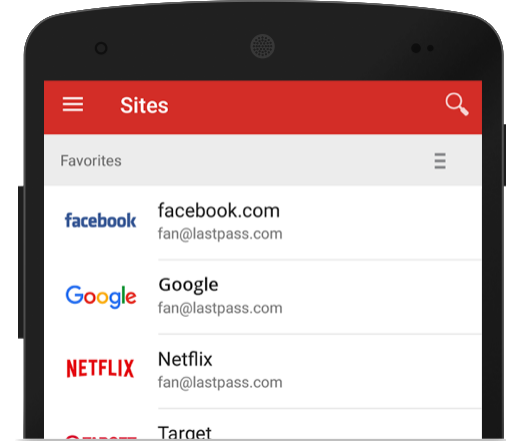
Güvenlik İhlali Etkisi

- Güvenlik İhlali Sonuçları
 - Her saldırıyı önlemek mümkün değil
 - Saldırganlar her zaman yeni yollar bulacaklar
 - Yaralanan itibar, vandalizm, hırsızlık, gelir kaybı, zedelenmiş fikri mülkiyet



Güvenlik İhlali Etkisi

- Güvenlik İhlali Örneği - **LastPass**
 - Çevrimiçi bir şifre yöneticisi
 - Çalıntı e-posta adresleri, şifre hatırlatıcıları ve kimlik doğrulama sağlamaları
 - Bilinmeyen bir cihazdan giriş yaparken e-posta doğrulaması veya **çok faktörlü kimlik** doğrulaması gerektirir
 - Kullanıcılar karmaşık ana parolayı kullanmalı, ana parolayı düzenli olarak değiştirmeli ve kimlik avı (phishing) saldırılarına dikkat etmelidir
 - Web güvenliği açığı tespit edilmiştir.



LastPass...

The Last Password You'll Ever Need.

Güvenlik İhlali Etkisi

- Güvenlik İhlali Örneği – **Vtech (~6 Milyon)**
 - Vtech çocuklar için yüksek teknoloji oyuncak üreticisidir
 - Müşteri adları, e-posta adresleri, şifreler, resimler ve sohbet günlükleri gibi hassas bilgilerin çalınmasına maruz kaldı.
 - Vtech bilgileri düzgün bir şekilde korumadı.
 - Bilgisayar korsanları, e-posta hesapları oluşturabilir, kredi başvurusunda bulunabilir ve çocukların bilgilerini kullanarak suç işleyebilir.
 - Bilgisayar korsanları, ebeveynlerin çevrimiçi hesaplarını da ele geçirebilir.



Kurum Verileri

Güvenlik İhlali Etkisi

- Güvenlik İhlali Örneği – **Equifax (2,4 Milyon)**
 - Equifax bir tüketici kredisi raporlama Kurumudur.
 - Saldırganlar web uygulama yazılımındaki bir güvenlik açığından yararlandı.
 - Equifax, kötü tarafların kimlik avı (phishing) düzeni için yetkisiz web siteleri oluşturmalarına izin veren yeni bir alan adıyla özel bir web sitesi kurdu



1.3 Saldırganlar ve Siber Güvenlik Uzmanları

Kim bunlar?



Kim bunlar?



Hacker/attacker/lamer: Sisteminize izinsiz olarak giren ve kendi amaçları için kullanmak isteyen kişi!

Hacker Ne Demek ?

- Türk Dil Kurumuna göre yetkisiz erişen kişi.
- Hacker, Elindeki gereçleri **kendine fayda sağlamak** veya **karşı tarafa zarar vermek** için bilgisayar bilgisi iyi seviyede olan kişidir.
- Bilgisayar veya elektronik cihazlara uzaktan bağlanarak;
 - Cihazları amacı dışında kullanan,
 - İçinden bilgi alan,
 - Bilgiye ulaşmamızı engelleyen veya
 - Bilgiye zarar veren
Kişi veya gruplardır.



Bir Siber Saldırganın Profili

Saldırgan Türleri

▪ Amatörler

- Betik becerisi az olan veya hiç olmayan amatörler (lamer-script kiddies)
- Saldırıları için çevrimiçi olarak bulunan mevcut araçları veya talimatları kullanırlar.

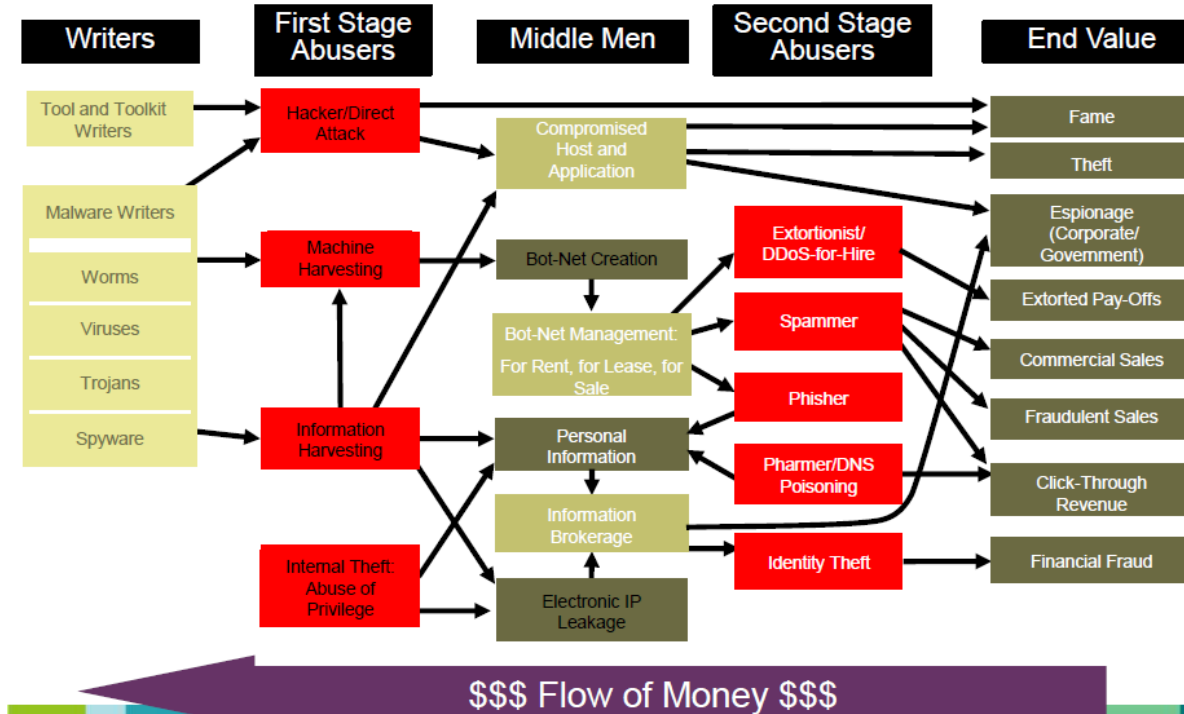
▪ Bilgisayar korsanları (Hacker'lar) - erişim elde etmek için bilgisayarlara veya ağlara giriş yaparlar

- **Beyaz şapkalılar**– sistemlerin güvenliğini artırılması için zayıflıkları keşfetme izni ile sisteme girerler
- **Gri şapkalılar** – izinsiz olarak sistemlere girme
- **Siyah şapkalılar** – yasadışı, kişisel, finansal veya politik kazançlar için herhangi bir güvenlik açığından yararlanma

▪ Organize Bilgisayar korsanları (Hacker'lar) - siber suçlular, hacktivistler, teröristler ve devlet destekli bilgisayar korsanları Kurumları.



Para Döngüsü



Bir Siber Saldırganın Profili

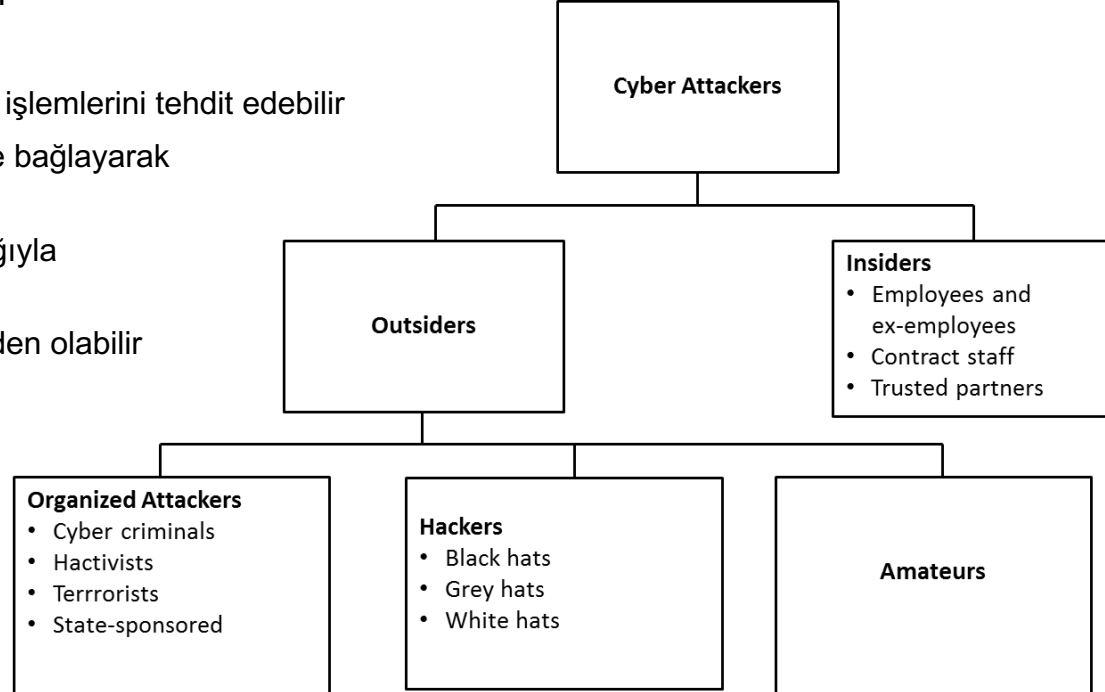
İç ve Dış Tehditler

İç Güvenlik Tehditleri

- Çalışan veya sözleşmeli iş ortağı olabilir
 - Gizli verileri yanlış kötü kullanabilir
 - Dahili sunucuları veya ağ altyapı cihazlarının işlemlerini tehdit edebilir
 - Zararlı USB belleği şirket bilgisayar sistemine bağlayarak dışarıdaki saldırıları kolaylaştırır
 - Kötü amaçlı e-posta veya web siteleri aracılığıyla zararlı yazılımları yanlışlıkla ağa dahil eder
 - Doğrudan erişim nedeniyle büyük hasara neden olabilir

Dış Güvenlik Tehditleri

- ağ veya bilgi işlem cihazlarındaki güvenlik açıklarından faydalanabilir
- erişim kazanmak için sosyal mühendisliği kullanabilir



Başımıza Ne Gelebilir?



Türkiye’de yaşanan olay...

Siber Güvenlik Uzmanları

Siber dünyada kurumlara sızmayı engelleyen kişilerdir.



SIZMA TESTİ



**AÇIKLARI BUL
ve KAPAT!**

1.4 Siber Savaş (Cyberwarfare)

Overview of Cyberwarfare

Siber Savaş nedir

- Siber Savaş nedir?

- Siber alan çakışması
- Stuxnet zararlı yazılımı
 - İran'ın nükleer zenginleştirme tesisine zarar vermek üzere tasarlandı
 - Bir PLC için özel geliştirildi
 - İnternete kapalı bir ortama sızıldı



Siber Savaşın Amacı

- Düşmanlara, uluslara veya rakiplere göre avantaj elde etmek için kullanılır
 - Diğer ulusların altyapısını sabote edebilir
 - Saldırganlara devlet personeline şantaj yapma olanağı sağlar
 - Vatandaşlar, hükümetin onları koruma yeteneğine olan güvenini kaybettirebilir
 - Hedeflenen ülkeyi fiziksel olarak işgal etmeden vatandaşların hükümetlerine olan inancını etkiler

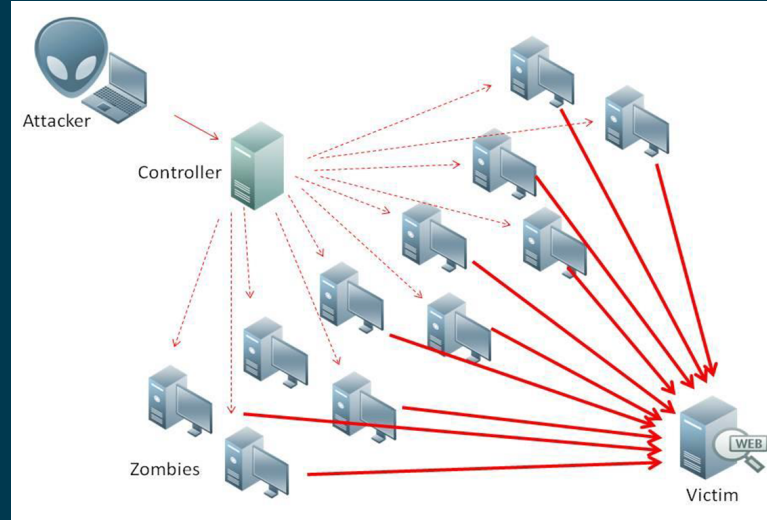


Bölüm Özeti

Özet

- Kişisel verileri tanımlayın.
- Kişisel verilerin özelliklerini ve önemini açıklayın.
- Kurum içindeki verilerin özelliklerini ve önemini açıklayın.
- Güvenlik ihlallerinin etkisini açıklayın.
- Bir saldırganın özelliklerini ve motivasyonunu açıklayın.
- Bir siber güvenlik uzmanının karşılaştığı yasal ve etik sorunları tanımlayın.
- Siber savaşın özelliklerini ve amacını açıklayın.

Bir Sonraki Bölüm:



Nasil Sadiriyorlar ?



Kaynak : Cisco Ağ Akademisi
(<https://www.netacad.com/portal/teaching>)
Çeviri: Ağ Yöneticileri Derneği
(<http://www.agyoneticileri.org/>)