Bilgi Güvenliği
Rehberlik Sunumu

Dr. Öğr. Üyesi Ahmet Naci ÜNAL

TÜRKİYE CUMHURİYETİ
ÇEVRE VE ŞEHİRCİLİK BAKANLIĞI

Takdim Plânı

- Temel Tanımlar
- Mevzuat
- Kavramsal Olarak Bilgi Güvenliği ve Siber Güvenlik
- Siber Güvenlik Tehditleri
- Değerlendirme

Temel Tanımlar

Temel Tanımlar

Veri:

Genel Tanımı:

Olgu, kavram ya da komutların, iletişim, yorum ve işlem için elverişli, biçimsel ve uzlaşımsal gösterimi.

Bilişim Teknolojileri Yönüyle Tanımı:

Anlamlı hale dönüştürülmemiş bitler.

Temel Tanımlar

Siber Uzay

İnternet, iletişim ağları, bilgisayar sistemleri, gömülü işlemciler ve denetleyiciler de dâhil olmak üzere bilgi teknolojisi altyapılarının birbirlerine bağlı olduğu ağdan oluşan küresel bir ortamdır.

Temel Tanımlar

Karar Vermek:
Hedeflenen amaca ulaşmak için iki veya daha fazla olası çözümden birinin sistematik yöntemlerle seçilmesi anlamına gelen bir süreçtir.

Temel Tanımlar

Bilgisayar Güvenliği

Dost bilgi sistemlerine karşı kötü amaçlı kullanımlar ile yetkisiz erişimlerin engellenmesine yönelik alınan tüm tedbirlerdir.

Temel Tanımlar

Bilgi Güvencesi

- Bilgi ve bilgi sistemlerini; kullanılabilirliği, bütünlüğü, kimlik doğrulaması, gizliliği ve inkâr edilemezliğinin sağlanmasına yönelik koruyucu ve savunucu tedbirlerdir.
- Ayrıca bilgi sistemlerinin geliştirilmesi için içerik koruma, algılama/bulma ve tepki kabiliyetinin sağlanmasını da içerir.

Temel Tanımlar

Bilgi Güvenliği

Bilgi ve bilgi sistemlerinin; ister kötü amaçlı yetkisiz erişimlere ve bilgide değişiklik yapılmasına, isterse erişime yetkili personelin yetkisiz depolama, işleme veya taşıma gibi durumları inkârına karşı korunması faaliyetidir.

Temel Tanımlar

Temel Tanımlar

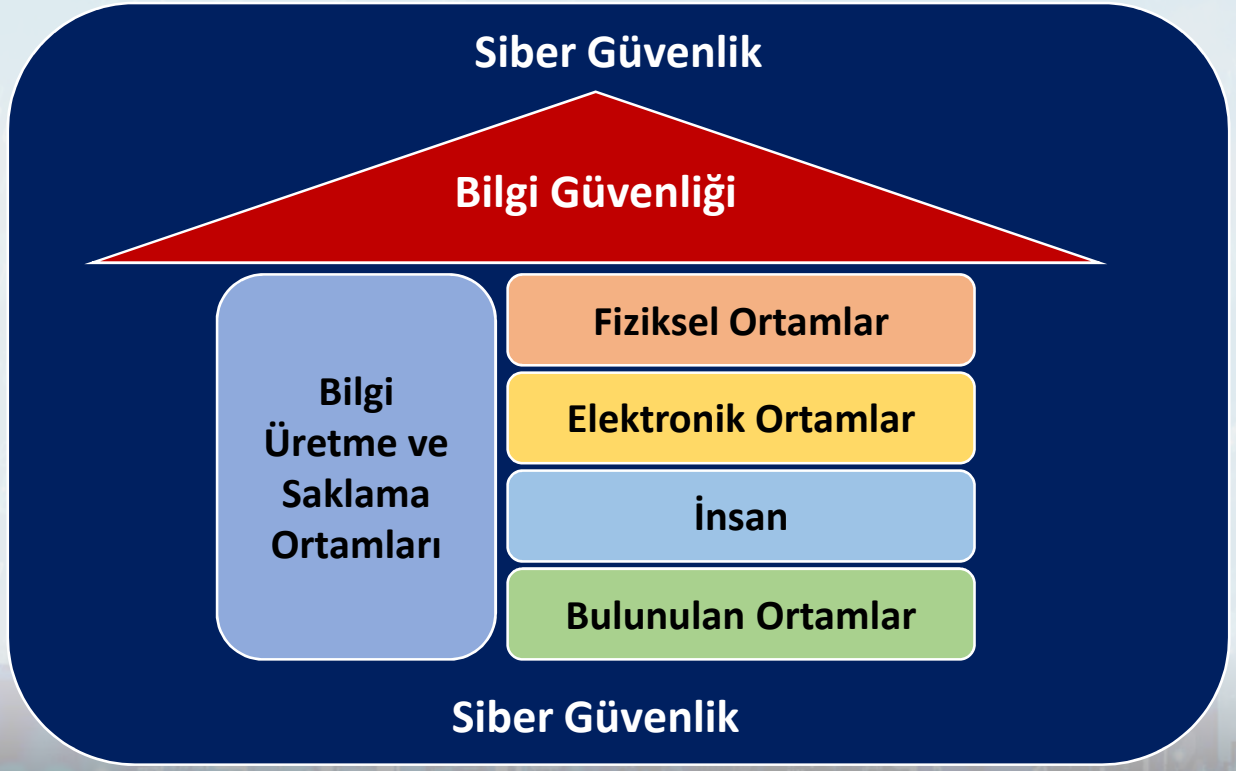
Erişilebilirlik: Bilgi ve bilgi sistemlerinin yetkisiz bozulmalara karşı korunmasıdır. Bilgi ve bilgi sistemlerine zamanında ve güvenilir bir şekilde erişilmesidir.

Bütünlük: Bilgilerin yetkisiz düzenlenmesinin veya silinmesinin önlenmesidir. Bilgi ve bilgi sistemlerinin doğru, tam ve bozulmamış olmasının sağlanmasıdır.

Gizlilik: Bilginin yetkisiz erişime veya açıklanmaya karşı korunması anlamına gelir. Bilgiye erişme hakkına sahip olanların bunu yapabilmelerini sağlarken, yetkilendirilmemiş kişilerin bunu yapmalarını engellenmesidir.

Temel Tanımlar

Temel Tanımlar



Temel Tanımlar

Siber Güvenlik

Siber çevre, organizasyonlar ve kullanıcının varlıklarını korumak için kullanılabilir araçlar, politikalar, güvenlik konseptleri, güvenlik önlemleri, kurallar, risk yönetimi, eylemler, eğitimler, uygulamalar ile teknolojiler bütünüdür.

Temel Tanımlar

Virüs

Bilgisayarlara sessizce yerleşen, kendisini kopyalayabilen, iletişim halindeki diğer bilgi sistemlerine bulaşabilen ve sistemlerde bulunan verilere zarar verebilen yazılımlardır.

Temel Tanımlar

Truva Atı (Trojan)

Adından da anlaşılacağı gibi sistem içerisine sızdıktan sonra pasif olarak bekleyen ve aktif hale geçince de sistem kaynaklarına zarar veren/çökerten yazılımlardır. Kendi kendilerine çoğalamazlar.

Temel Tanımlar

Solucan (Worm)

Solucanlar; bilgi sistemlerine girdikten sonra kendi başıma ilerleyebilen, sürekli çoğalan, ağ kaynaklarını hedefleyerek ağ trafiğini yavaşlatan ve fırsat bulduğunda diğer sistemlere de bulaşabilen zararlı yazılımlardır.

Mevzuat

- 2813 sayılı Bilgi Teknolojileri ve İletişim Kurumumun Kuruluşuna İlişkin Kanun
- 5809 Sayılı Elektronik Haberleşme Kanunu
- 5070 Sayılı Elektronik İmza Kanunu
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
- 6475 sayılı Posta Hizmetleri Kanunu

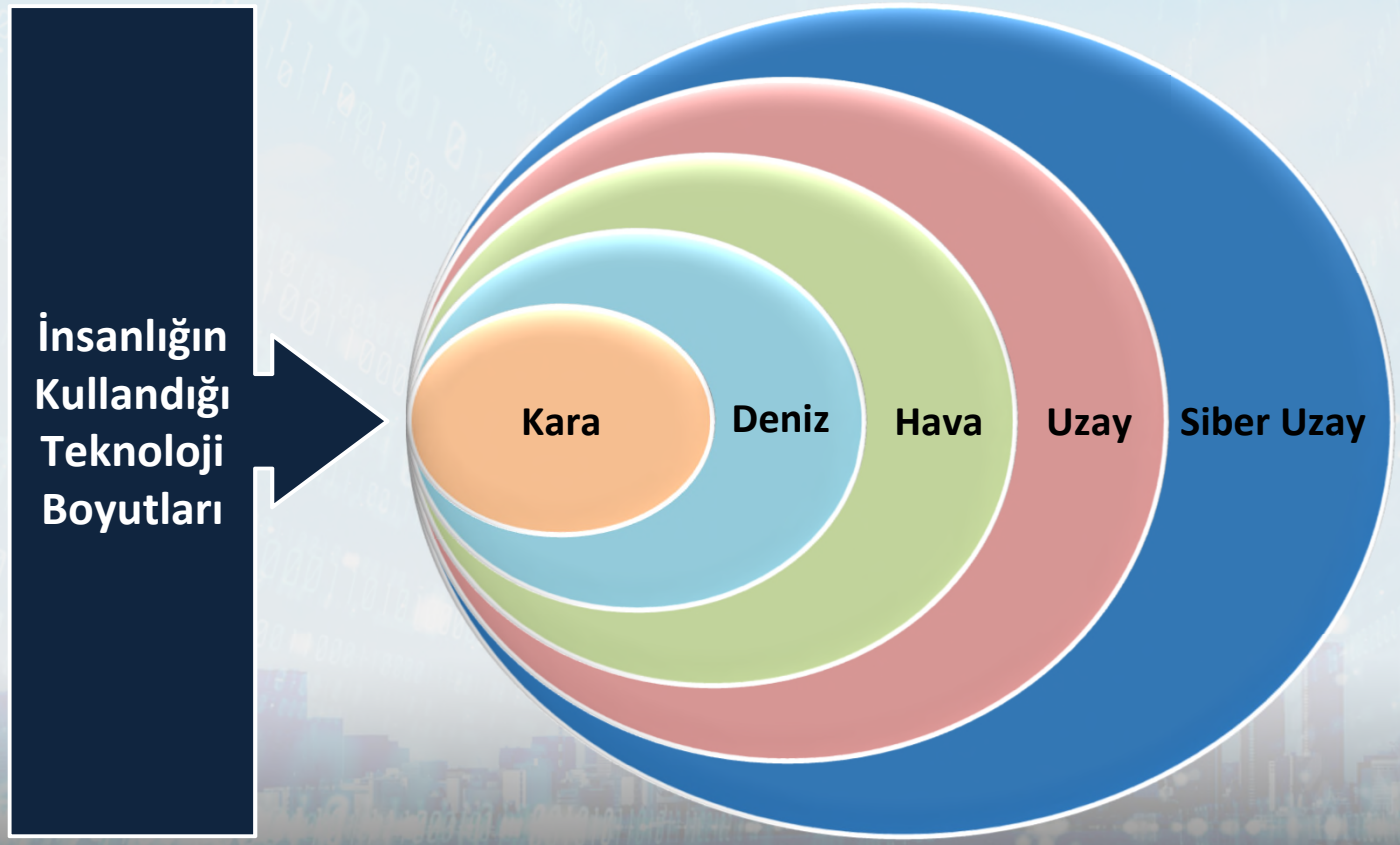
Mevzuat

- 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun
- 6362 sayılı Sermaye Piyasası Kanunu 115. Madde
- 5271 sayılı Ceza Muhakemesi Kanunu 5. Bölüm
- 6102 sayılı Türk Ticaret Kanunu'nun 1525 inci maddesi
- 6698 sayılı Kişisel Verilerin Korunması Kanunu
- 655 sayılı Ulaştırma, Denizcilik ve Haberleşme Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname

Mevzuat

- Bilişim Suçları Türk Ceza Kanununda (5237) (Md.243-245) arasında aşağıdaki gibi düzenlenmiştir:
  - Bilişim Sistemine Girme Suçu (TCK m.243),
  - Sistemi Engelleme, Bozma, Erişilmez Kılma, Verileri Yok Etme veya Değiştirme Suçu (TCK m.244),
  - Banka veya Kredi Kartının Kötüye Kullanılması Suçu (TCK m.245),
  - Yasak Cihaz veya Program Kullanma Suçu (TCK m.245/a).

Kavramsal Olarak Bilgi Güvenliği ve Siber Güvenlik



Kavramsal Olarak Bilgi Güvenliği ve Siber Güvenlik

Kavramsal Olarak Bilgi Güvenliği ve Siber Güvenlik

Kavramsal Olarak Bilgi Güvenliği ve Siber Güvenlik

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Plânı

"İşlediği bilginin gizliliği, bütünlüğü veya erişebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılardır."

Kavramsal Olarak Bilgi Güvenliği ve Siber Güvenlik

Avrupa Birliği Kritik Alt Yapı Tanımlaması

"Zarar görmesi veya ortadan kalkması halinde, vatandaşların hayati toplumsal fonksiyonlarına, sağlığına, emniyetine, güvenliğine, sosyal refahına ve üye devletlerin etkin işleyişine ciddi seviyede olumsuz etkisi olabilecek varlık, sistem ve hizmetlerdir."

Amerika Birleşik Devletleri Kritik Alt Yapı Tanımlaması

"Yetersizliği veya ortadan kalkması halinde, güvenlik, ulusal ekonomi güvenliği, ulusal halk sağlığı ve emniyeti ya da bu unsurların herhangi bir kombinasyonuna olumsuz etkisi olan fiziksel veya sanal sistemler ve varlıklar."

Siber Güvenlik Tehditleri

En Temel Siber Güvenlik Tehditleri

Virüsler

Belleği bozabilir. Bilgisayarda sistem öz kaynaklarını gereksiz olarak kullanır. Kendini kopyalayarak çoğalabilir.

Truva Atları

Bilgisayar programına bağlanarak gizlenebilir. Verileri silebilir, izinsiz iletebilir, değiştirebilir, kopyalayabilir. Kendisini çoğaltamaz.

Solucanlar

Bilgisayara girdikten sonra kendi başına ilerleyebilir ve sürekli çoğalır. Ağ kaynaklarını hedefleyerek, ağ trafiğini yavaşlatır. Bulunduğu sistemden diğer sistemlere de bulaşabilir.

Siber Güvenlik Tehditleri

Siber Güvenlik Tehditleri

Siber Güvenlik Tehditleri

Siber Güvenlik Tehditleri

Sosyal Mühendislik

Nedir?

Kötü amaçlı kişilerin;

hedefteki insanların kendi verilerini kullanarak, yine aynı kişileri aldatmasıdır.

Siber Güvenlik Tehditleri

Sosyal Mühendislik

Nasıl ikna ederler?

Siber Güvenlik Tehditleri

Sosyal Mühendislik

Ne yapabiliriz?

Siber Güvenlik Tehditleri

Siber Güvenlik Tehditleri

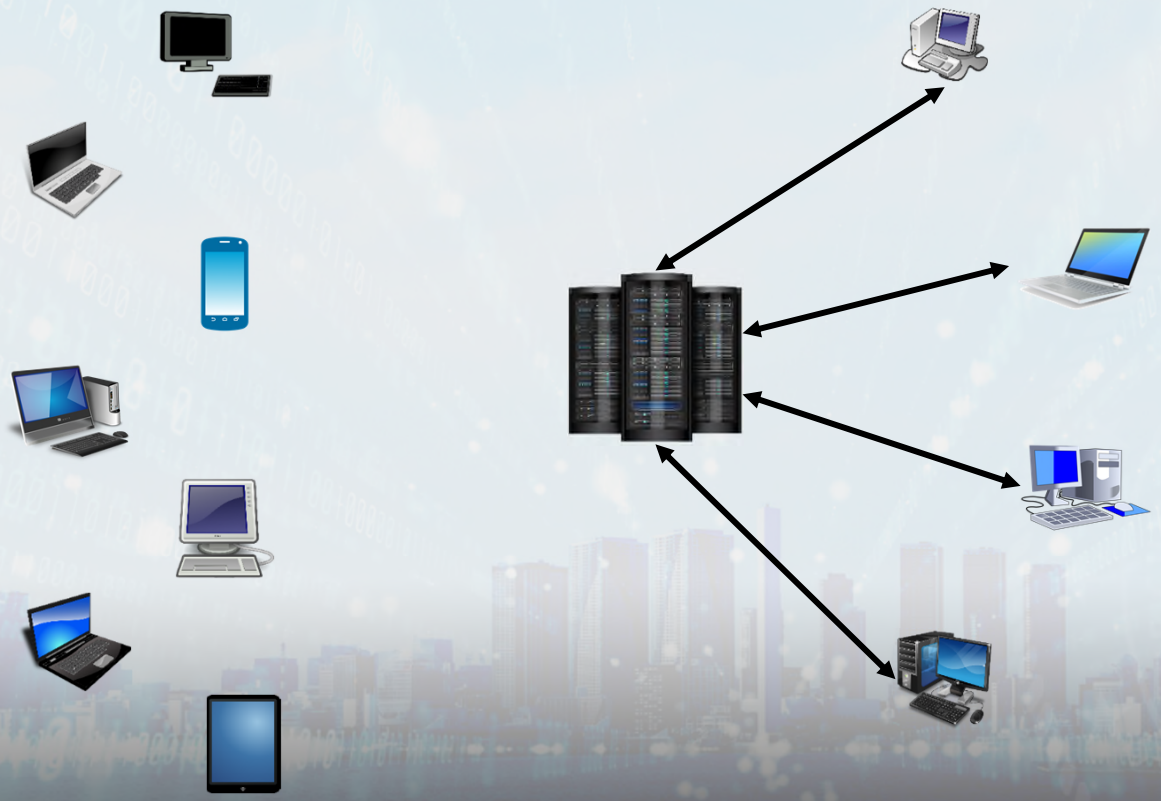
DDoS Saldırıları

DoS : Denial of Service (Hizmet Engelleme)

DDoS : Distributed Denial of Service (Dağıtık Hizmet Engelleme)

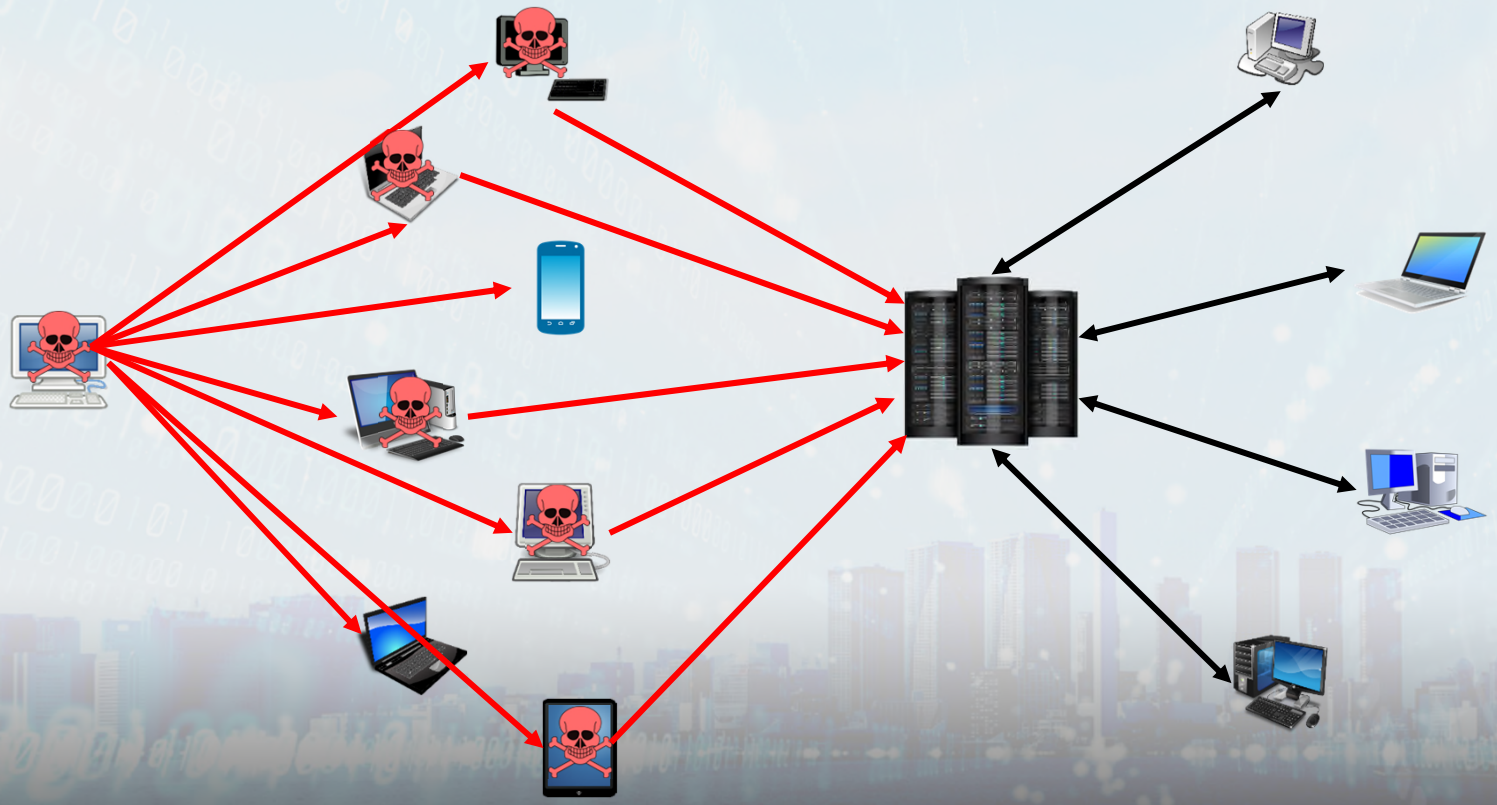
Siber Güvenlik Tehditleri

DDoS Saldırıları



Siber Güvenlik Tehditleri

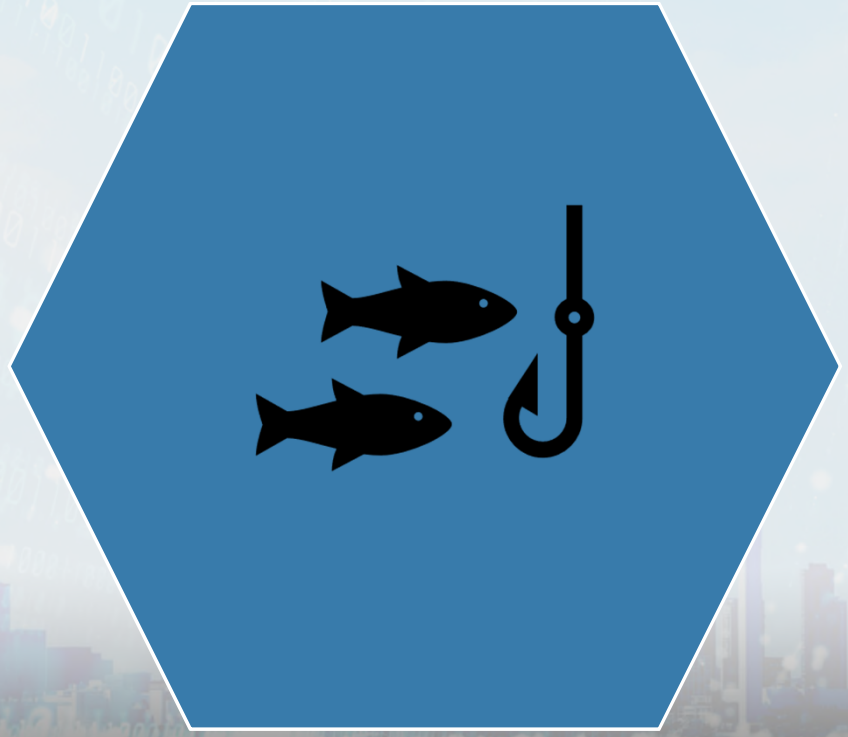
DDoS Saldırıları



Siber Güvenlik Tehditleri

Siber Güvenlik Tehditleri

Oltalama/Yemleme (Phishing)



Facebook - Giriş Yap veya Kaydol

http://tr-tr.fasebook.com

Uygulamalar

facebook

E-posta veya Telefon | Şifre | Giriş Yap

Hesabını mı unuttun?

SAHTE

Facebook tanıdıklarınla iletişim kurmanı v
hayatında olup bitenleri paylaşmanı sağlar.

Hesap Aç

Ücretsizdir ve her zaman ücretsiz kalacaktır.

Adın | Soyadın

Cep telefonu numarası veya e-posta

Facebook - Giriş Yap veya Kaydol

https://tr-tr.facebook.com

Uygulamalar

facebook

E-posta veya Telefon | Şifre | Giriş Yap

Hesabını mı unuttun?

Facebook tanıdıklarınla iletişim kurmanı ve
hayatında olup bitenleri paylaşmanı sağlar.

Hesap Aç

Ücretsizdir ve her zaman ücretsiz kalacaktır.

Adın | Soyadın

Cep telefonu numarası veya e-posta

Yeni şifre

Siber Güvenlik Tehditleri

Siber Güvenlik Tehditleri

Fidye Yazılımı Saldırısı (Ransomware)

Fidye Yazılımı (Ransomware)

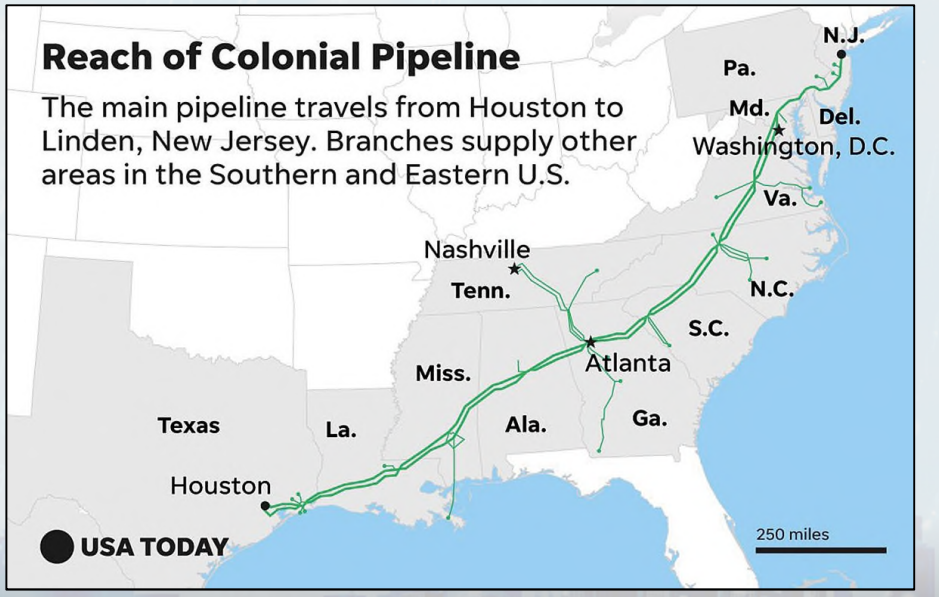
Bilgisayarlardaki dosyaları şifreler

Şifreyi kaldırmak için programı geliştirenler para isterler

Bilgisayarın kendisini şifreler

Siber Güvenlik Tehditleri

Yaşanmış Siber Saldırılar



Mayıs 2021

Siber Güvenlik Tehditleri

Yaşanmış Siber Saldırılar

2017
150+ ülkede 300.000+ kişi

Siber Güvenlik Tehditleri

Yaşanmış Siber Saldırılar

2010

Siber Güvenlik Tehditleri

Siber Savunma Hazırlık Süreci

Gerekli güvenlik yatırımları planlanır ve gerekli kararlar alınır.

Siber güvenlik strateji planı hazırlanır.

Bu görevin başarılması için hazırlık düzeyi belirlenir.

Savunma görevinin aşamaları tehditlere göre sınıflandırılır.

Siber Güvenlik Tehditleri

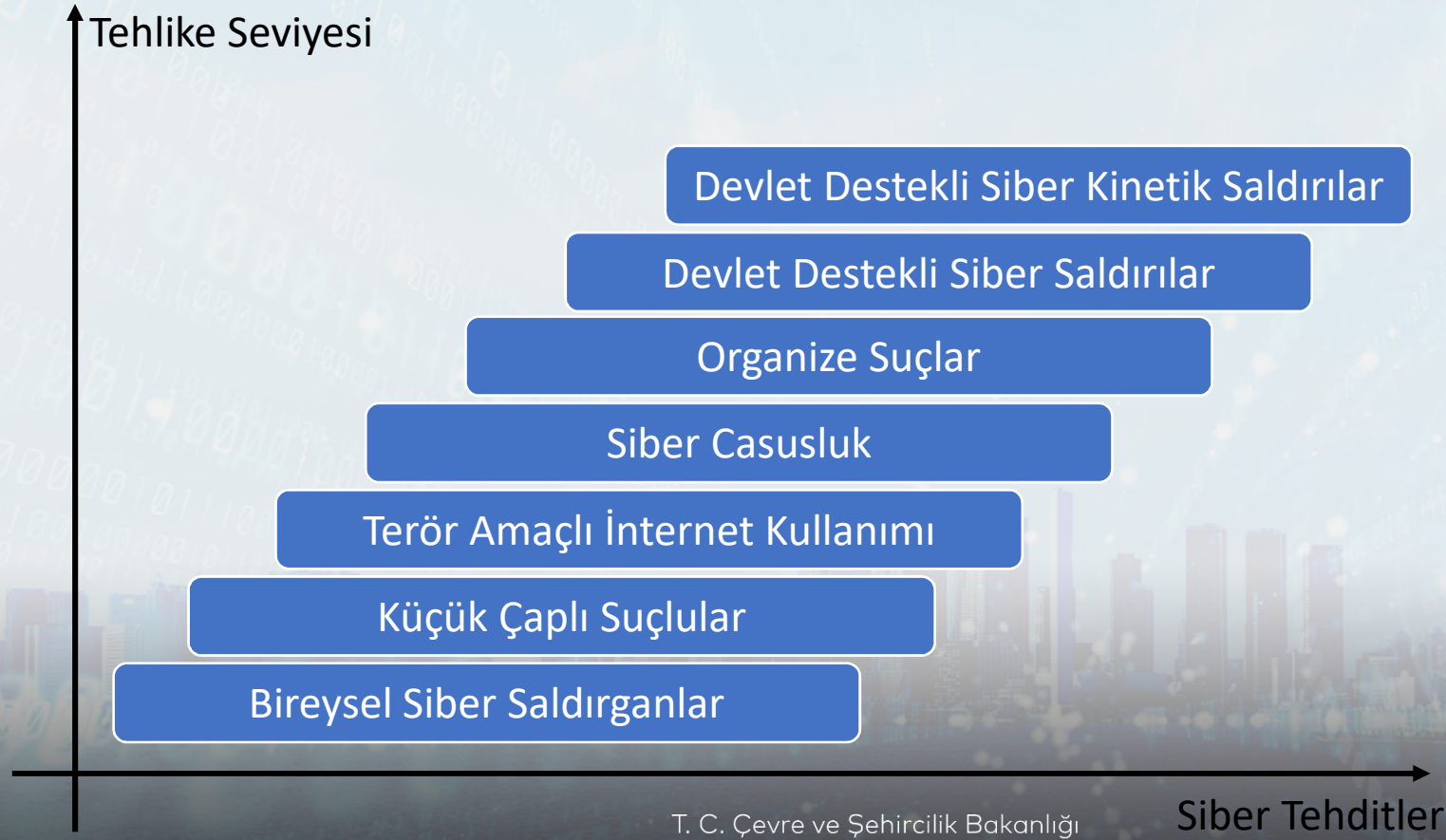
Siber Tehditlerin Sınıflandırılması

- Sorununun/Problemin kök nedenlerine inilir.
- Kök neden ile problem arası süreci doğru modelleyerek sınıflandırma yapılır.
- Bu sınıflandırma sayesinde yoğunlaşılacak alan daraltılır.
- Böylece sorun/probleme odaklanarak kullanılacak enerji doğru planlanabilir.

Siber Tehdit Spektrumu

Siber Güvenlik Tehditleri

Siber Tehditlerin Sınıflandırılması



Siber Güvenlik Tehditleri

Siber Tehdit Seviyeleri

Seviyeler	Saldırgan Tipleri	Saldırganların Amaç ve Hedefleri	Kullanılabilecek Yöntemler
Seviye 1 Siber Vandalizm	Küçük saldırgan gruplar	Organizasyon yapısını bozmak	• Hassas verilere erişim • Denemeler yapmak • Global erişime sahip sistemlerdeki dosyaları hedeflemek • Ağ saldırıları yapmak için sosyal mühendislik faaliyetleri yapmak

Siber Güvenlik Tehditleri

Siber Tehdit Seviyeleri

Seviyeler	Saldırgan Tipleri	Saldırganların Amaç ve Hedefleri	Kullanılabilecek Yöntemler
Seviye 2 Siber Dolandırıcılık	Bireysel veya küçük saldırı grupları	• Politik-ideolojik amaçlar • Dolaylı casusluk	• Kurum içi yardımla fiziksel erişim sağlanması • Açık kaynak istihbaratı • Veri trafiğinin izlenmesi • Bilgi sistemi cihazlarının incelenmesi • Dış bilgi sistemleri ve ağlarının izlenmesi

Siber Güvenlik Tehditleri

Siber Tehdit Seviyeleri

Seviyeler	Saldırgan Tipleri	Saldırganların Amaç ve Hedefleri	Kullanılabilecek Yöntemler
Seviye 3 Siber Gözetim	• Büyük saldırı grupları • Terör örgütleri • Organize suç örgütleri	• Genel altyapı bilgisine sahip olmak • Büyük ölçekli saldırılar için temel verileri elde etmek	• Veri aktarımını kolaylaştırmak için casus yazılımlar eklemek • İç ağlara genel amaçlı bilgi toplayıcılar eklemek • Kurum ağların taranması

Siber Güvenlik Tehditleri

Siber Tehdit Seviyeleri

Seviyeler	Saldırgan Tipleri	Saldırganların Amaç ve Hedefleri	Kullanılabilecek Yöntemler
Seviye 4 Siber Casusluk	Profesyonel istihbarat kuruluşları	Ülkelerin özel görev ve programları	• Tedarik zincirine donanım ekipmanı eklemek • Oturum bilgilerini ele geçirmek • Görüntüleme içeriğini kurumsal bilgi sistemlerine ve ağlarına yüklemek • Ana bilgisayarları ve kritik noktaları hedeflemek • Kurumsal bilgi sistemlerini günlük saldırılarla etkilemek

Siber Güvenlik Tehditleri

Siber Tehdit Seviyeleri

Seviyeler	Saldırgan Tipleri	Saldırganların Amaç ve Hedefleri	Kullanılabilecek Yöntemler
Seviye 5 Siber Savaş	Askeri birlikler	Hedefin bilgi altyapısını yok etmek	• Kritik bilgi sistemi bileşenlerini ve işlevlerini hedeflemek • Üretim ve/veya dağıtım bileşenlerini kullanarak organizasyonu tehdit etmek • Koordineli, dahili ve tedarik zinciri saldırılarını kullanarak organizasyona saldırılar düzenlemek • Tedarik zincirine kötü amaçlı yazılım enjekte ederek yanlış açık organizasyonlar oluşturmak • Verileri yanlış bir şekilde enjekte etmek • Sistem yapılandırmalarına bağlı olarak özel, yönsüz, kötü amaçlı yazılım eklemek • Kablosuz iletişim sistemine erişim sağlamak

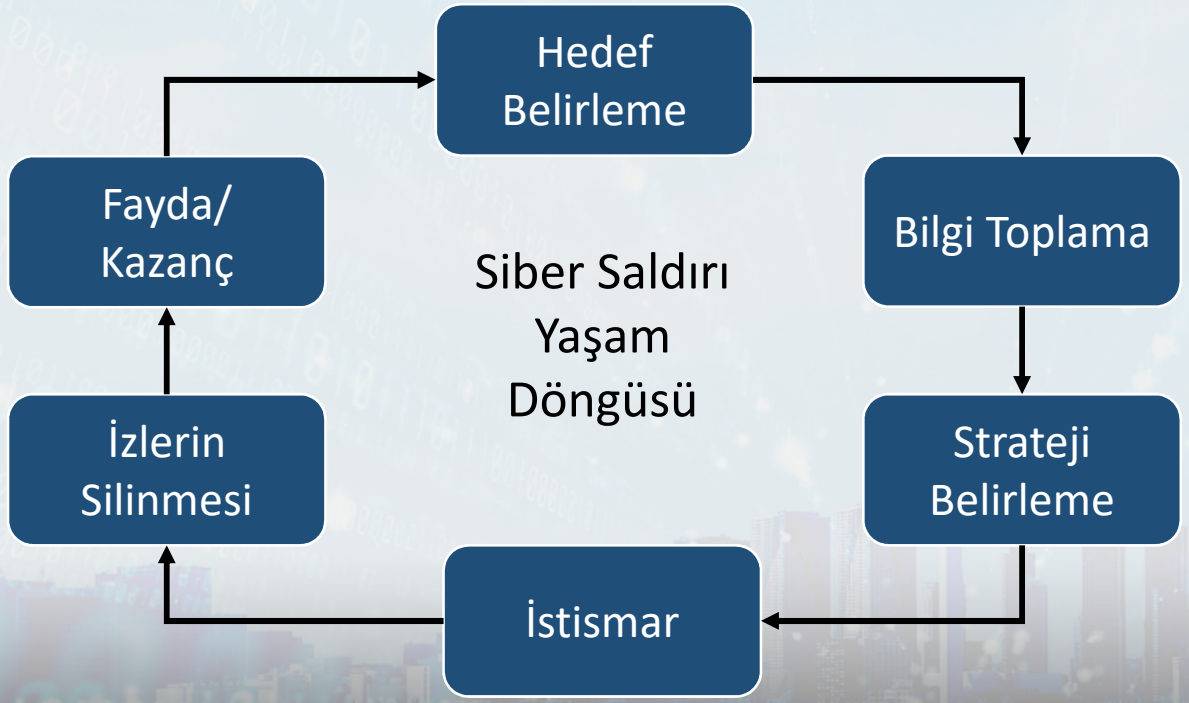
Siber Güvenlik Tehditleri

Siber Güvenlik Tehdit Belirleme Süreci

- Siber uzayı aktif olarak kullanan tüm sektörler için tam (% 100) güvenli bir alandan söz etmek mümkün değildir.
- Güvenlik önlemleri artırıldıkça, tehdit unsurları da sürekli gelişmektedir.
- Bu durum doğal olarak risk seviyesini artırmaktadır. Risk seviyesini düşürecek en önemli etken ise mevcut siber tehditlerin varlığını tespit edebilmektir.
- Tehditin varlığı saptanamazsa adeta hayalet saldırılara hedefsiniz demektir. Bu yüzden tehdit olabilecek verileri saptamak kadar saptanan bu tehdit verilerinin detaylı analizini yaparak tanımlamak önemli bir aşamadır.

Siber Güvenlik Tehditleri

Siber Güvenlik Tehdit Belirleme Süreci



Değerlendirme

- Siber uzaya ulaşma yaşı, okul öncesi dönemden başlayıp insanlar ölünceye kadarki zamanı kapsamaktadır. Bu sebeple kişilerin, toplumların, organizasyonların, devletlerin, kısaca her tür aktörün siber uzay kullanma politikalarını, tehdit değerlendirmelerini ve davranış şekillerini belirlemeleri gerekmektedir.
- Bu tedbirlerle davranış şekilleri belirlenirken, siber uzayda geliştirilecek önlemlerin neredeyse tüm bilim dallarını içeren disiplinlerarası bir yaklaşım olduğunu da göz ardı etmemelidir.
- Siber teknik ve teknolojiler mühendisler tarafından geliştirilse de bu ürünlerin son kullanıcılarının her yaş grubundan insanlar olmaktadır.
- Aynı zamanda siber uzayda gerçekleştirilen her tür faaliyet bir süreci tetiklemekte ve bu süreçler başka süreçlerle bütünleşerek adeta bir kartopu gibi büyüyerek yollarına devam etmektedir.

Öneriler

Parolanızı Oluştururken

Siber Güvenlik

Parola Güvenliği

Öneriler

Parolanızı Oluştururken

- Parolanızı belli aralıklarla güncelleyiniz.
- Parolanızı hiç kimseyle paylaşmayınız.
- Bilgisayarınızı kullanmadığınız zaman ekranı mutlaka kilitleyiniz.

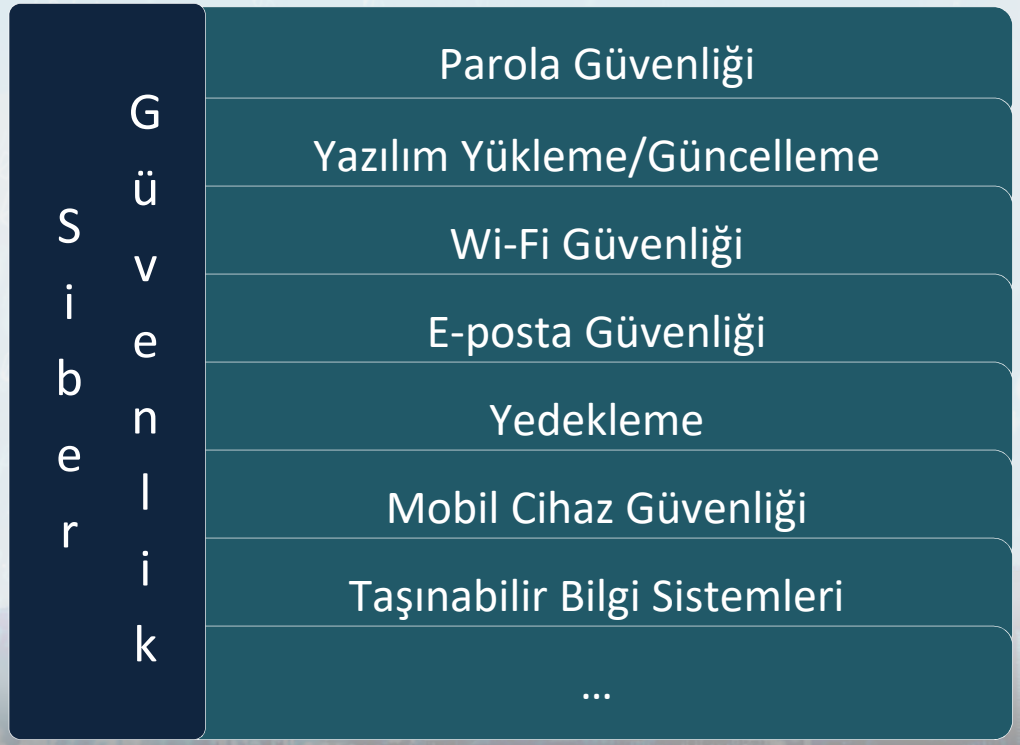
Öneriler

Parolanızı Oluştururken

- Büyük Harfleri (A, B C, D, …)
- Küçük Harfleri (a, b c, d, …)
- Rakamları (1,2, 3, 4, …)
- Özel Işaretleri (!, %, @, ?, *, …)

- Hepsini ve karışık olarak kullanınız [Alfanümerik (Alfasayısal]
- En az 12 karakterden oluşmasına dikkat ediniz.

Öneriler


Siber Güvenlik
Parola Güvenliği
Yazılım Yükleme/Güncelleme
Wi-Fi Güvenliği
E-posta Güvenliği
Yedekleme
Mobil Cihaz Güvenliği
Taşınabilir Bilgi Sistemleri
...

Değerlendirme

Değerlendirme

Tanımlama:

Siber güvenlik riskini yönetmek için insanların, sistemlerin, varlıkların, verilerin ve yeteneklerin kurumsal bir anlayış içinde geliştirilmesini kapsar.

Değerlendirme

Koruma:

Kritik hizmetlerin sunulmasını sağlamak için potansiyel bir siber güvenlik olayının etkisini sınırlandırmayı veya gerekli önlemlerin geliştirilerek uygulanmasını içerir. Bu durumu gerçekleştirebilmek için dijital ve fiziksel varlıklara erişim kontrol edilmeli, verilerin güvence altına alınması için süreçler oluşturulmalı ve koruyucu teknoloji kullanmalıdır.

Değerlendirme

Algılama/Tanıma:

Siber güvenlik ihlallerinin hızlı bir şekilde tanımlanması faaliyetlerini belirtir. Algılama işlemi, siber güvenlik olaylarını oluşturan anomalilerin zamanında fark edilmesini kapsar.

Değerlendirme

Cevap Verme:

Tespit edilen bir siber güvenlik olayıyla ilgili önlem almak için uygun faaliyetleri geliştirmeyi ve uygulamayı ifade eder. Bunun için bir cevap planı hazırlanmalı, dost iletişim hatları tanımlanmalı, etkinlikler hakkında bilgi toplamalı ve analiz edilmeli, kötücül olayı ortadan kaldırmak için gerekli tüm aktiviteler gerçekleştirmelidir.

Değerlendirme

Kurtarmak:

Siber güvenlik olayı nedeniyle bozulmuş olan tüm yetenekleri veya hizmetleri geri yüklemek için uygun aktiviteler geliştirmeyi ve uygulamayı kapsar.

Değerlendirme

• Tüm kurum ve bireylerin siber güvenlik stratejilerini ve siber güvenlik uygulama politikalarını güncel tutmaları, üretilen politika ve stratejiler kapsamında kısa, orta ve uzun vadeli siber güvenlik uygulama planlarını oluşturmaları büyük önem kazanmaktadır.

Değerlendirme

- Bu planlamaların toplumdaki siber uzaya erişim sağlayan tüm yaş grupları ve bilgi seviyelerine göre sosyal katmanları kapsamalıdır. Bu katmanlarda; siber güvenlik farkındalığı ile siber güvenlik bilinci oluşturacak ve katmanlar arasında da etkileşimi sağlayacak şekilde değişik seviyelerde siber güvenlik eğitimleri tasarlanmalıdır. Bu eğitimler uygulamalı bir şekilde gerçekleştirilmelidir.

Değerlendirme

- Kritik alt yapı donanım ve yazılımları başta olmak üzere, hassas teknoloji için gerekli tüm yazılımların milli kaynak kodları içermesi ve mevcut yazılım oluşturma standartlarına uygun bir şekilde yazılması sağlanmalıdır.

Değerlendirme

• Günümüz siber saldırılarının –çoğunlukla- yapay zekâ yazılımları yardımıyla gerçekleştirilmesi, bu sızma faaliyetlerinin hedef bilgi sistemleri tarafından zamanında saptanamamasına sebep olabilmektedir. Bu kapsamda hedef bilgi sistemi korumasında da yapay zekâ yöntemleri kullanımına öncelik verilerek “tehdit belirleme hızı”nın artırılması yönünde projeler geliştirilmesi üzerinde durulmalıdır.

Değerlendirme

Siber uzaydaki tüm faaliyetlerde en zayıf halkanın **insan** olduğunu unutmayınız!

Teşekkürler

TÜRKİYE CUMHURİYETİ
ÇEVRE VE ŞEHİRCİLİK BAKANLIĞI