

Bilgi Güvenliđi

Dr.Öđr.Üyesi Ahmet Naci ÜNAL
Bahçeşehir Üniversitesi



T.C. ÇEVRE, ŞEHİRCİLİK VE
İKLİM DEĞİŞİKLİĐİ BAKANLIĐI

Takdim Plânı

- Giriş
- Kavramsal Olarak Bilgi Güvenliđi ve Siber Güvenlik
- Siber Güvenlik Tehditleri
- Deđerlendirme



Giriş

Yönetim:

Bir işletmenin veya örgütün amaçlarını gerçekleştirmek için sahip olduđu üretim kaynaklarını etkili ve verimli olarak kullanması sürecidir.



Giriş



Giriş

Karar Vermek:

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



Giriş

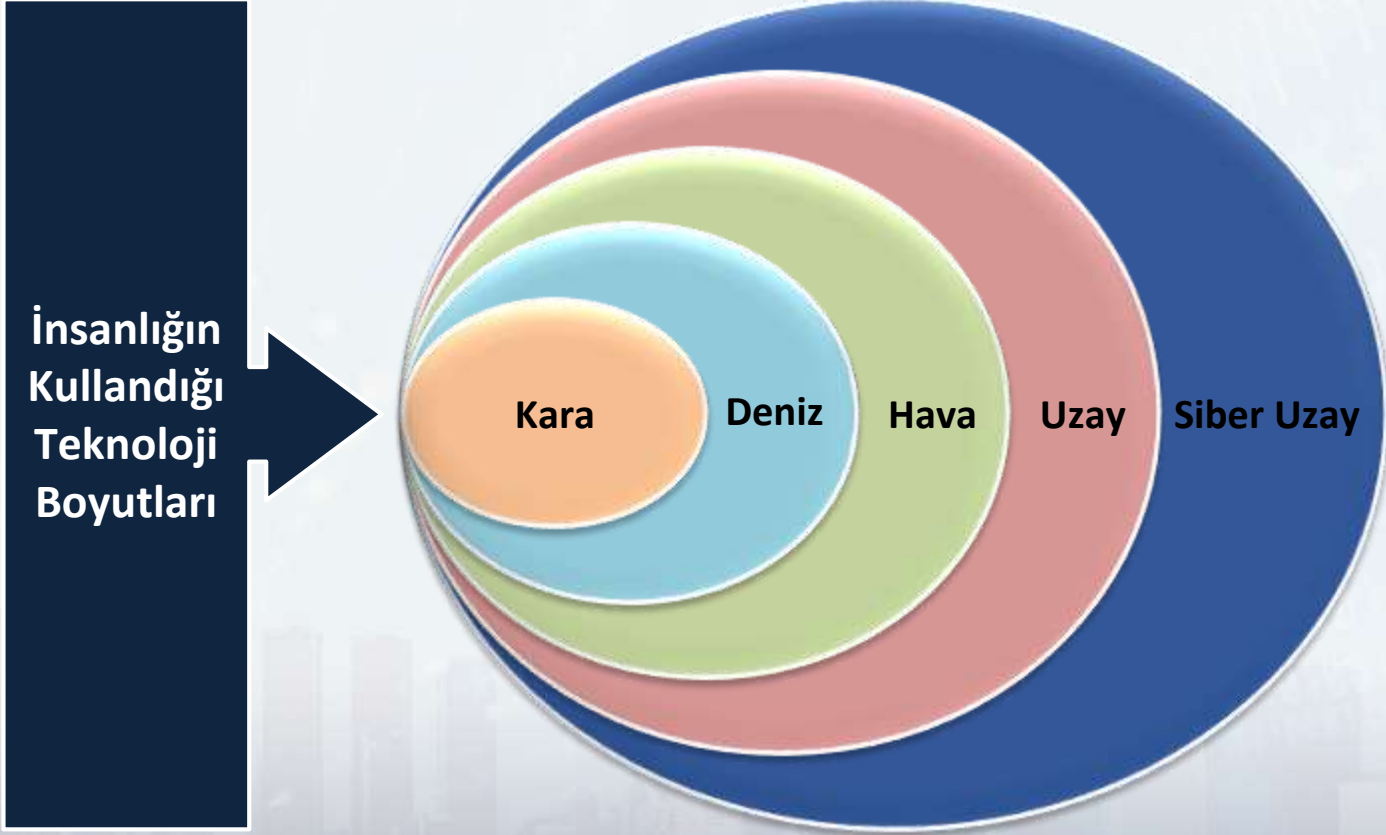


Siber Uzay

İnternet, iletişim ađları, bilgisayar sistemleri, gömülü işlemciler ve denetleyiciler de dâhil olmak üzere bilgi teknolojisi altyapılarının birbirlerine bađlı olduđu ađdan oluřan küresel bir ortamdır.



Giriş



Kavramsal Olarak Bilgi Güvenliđi ve Siber Güvenlik



Kavramsal Olarak Bilgi Güvenliđi ve Siber Güvenlik



Kavramsal Olarak Bilgi Güvenliđi ve Siber Güvenlik



Eriřilebilirlik: Bilgi ve bilgi sistemlerinin yetkisiz bozulmalara karřı korunmasıdır. Bilgi ve bilgi sistemlerine zamanında ve güvenilir bir şekilde eriřilmesidir.

Bütünlük: Bilgilerin yetkisiz düzenlenmesinin veya silinmesinin önlenmesidir. Bilgi ve bilgi sistemlerinin dođru, tam ve bozulmamıř olmasının sađlanmasıdır.

Gizlilik: Bilginin yetkisiz eriřime veya açıklanmaya karřı korunması anlamına gelir. Bilgiye eriřme hakkına sahip olanların bunu yapabilmelerini sađlarken, yetkilendirilmemiř kiřilerin bunu yapmalarını engellenmesidir.

Kavramsal Olarak Bilgi Güvenliđi ve Siber Güvenlik



Kavramsal Olarak Bilgi Güvenliđi ve Siber Güvenlik

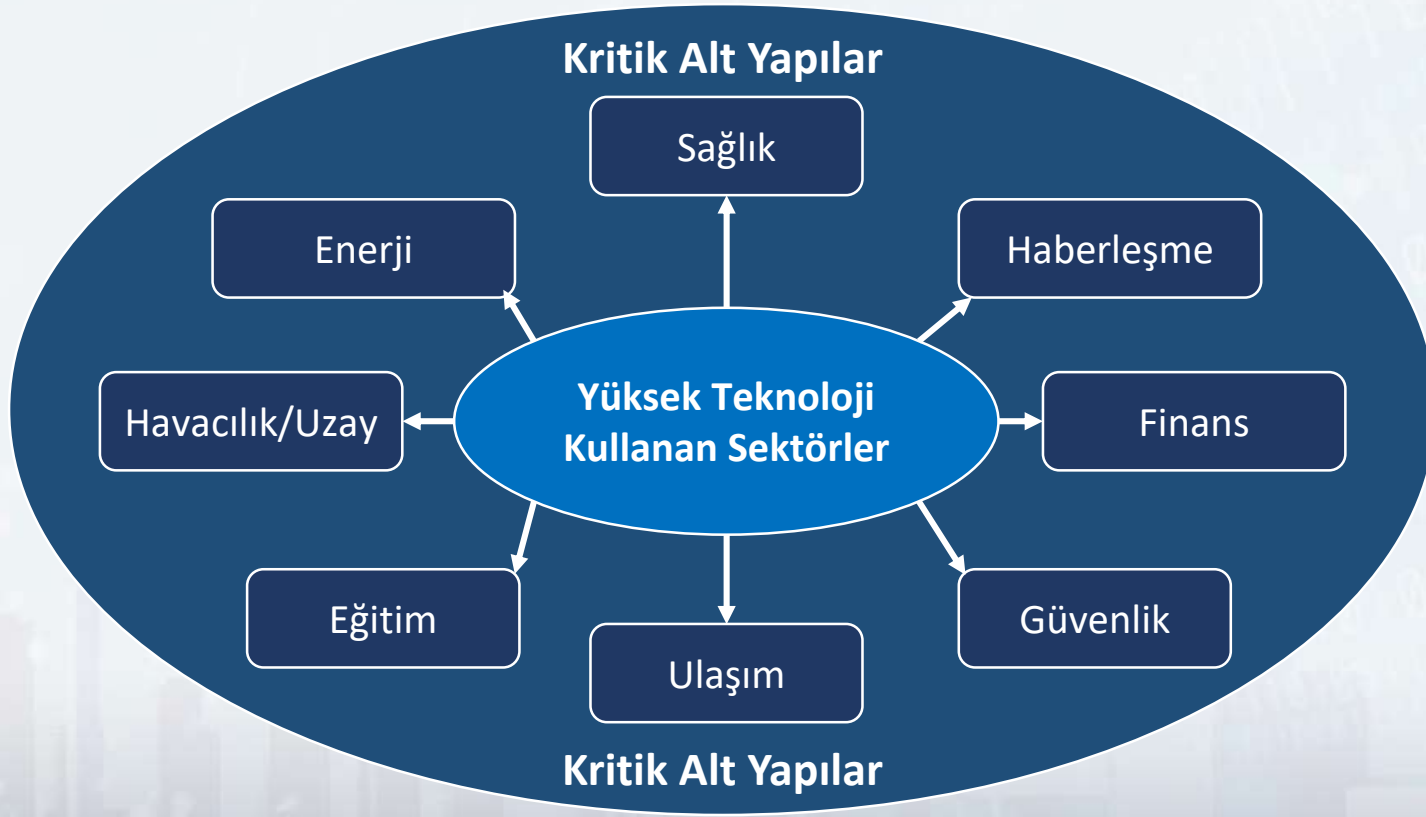


Siber Güvenlik:

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



Kavramsal Olarak Bilgi Güvenliđi ve Siber Güvenlik



Kavramsal Olarak Bilgi Güvenliđi ve Siber Güvenlik

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Plânı

“İşlediđi bilginin gizliliđi, bütünlüğü veya erişebilirliđi bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılardır.”



Kavramsal Olarak Bilgi Güvenliđi ve Siber Güvenlik

Avrupa Birliđi Kritik Alt Yapı Tanımlaması

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

Amerika Birleşik Devletleri Kritik Alt Yapı Tanımlaması

“Yetersizliđi veya ortadan kalkması halinde, güvenlik, ulusal ekonomi güvenliđi, ulusal halk sađlıđı 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

Belleđi bozabilir. Bilgisayarda sistem öz kaynaklarını gereksiz olarak kullanır. Kendini kopyalayarak çođalabilir.



Truva Atları

Bilgisayar programına bağlanarak gizlenebilir. Verileri silebilir, izinsiz iletebilir, deđiştirebilir, kopyalayabilir. Kendisini çođaltamaz.



Solucanlar

Bilgisayara girdikten sonra kendi başına ilerleyebilir ve sürekli çođalır. Ađ kaynaklarını hedefleyerek, ađ trafiđini yavaşlatır. Bulunduđu sistemden diđer sistemlere de bulaşabilir.

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 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.

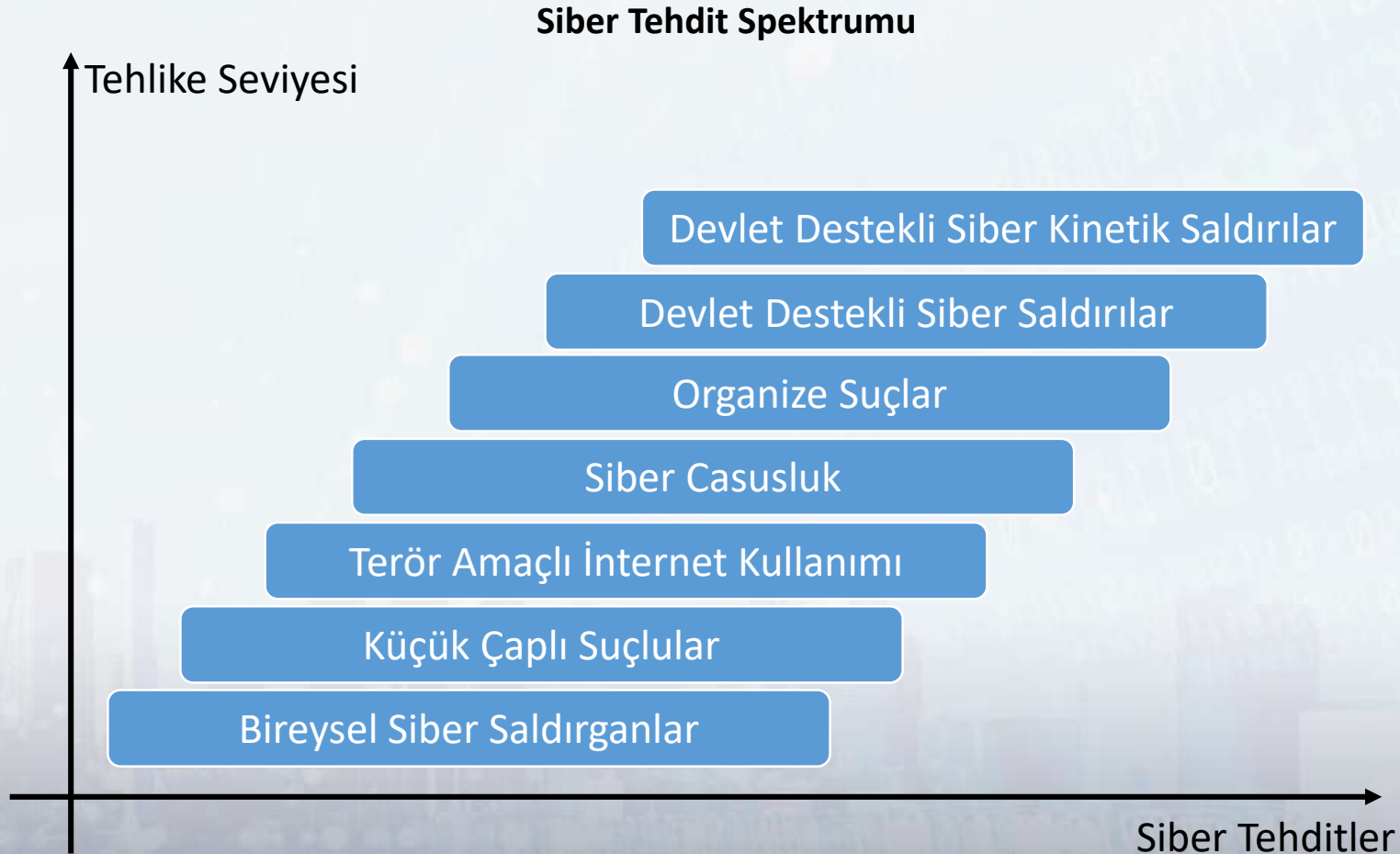


Siber Tehditlerin Sınıflandırılması

- 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 Tehditlerin Sınıflandırılması



Siber Tehditlerin Sınıflandırılması

Siber Tehdit Seviyeleri

Seviyeler	Saldırgan Tipleri	Saldırganların Amaç ve Hedefleri	Kullanılabilecek Yöntemler
Seviye 1 Siber Vandalizm	Küçük saldırgan gruplar	Organizasyon yapısını bozmak	<ul style="list-style-type: none">• Hassas verilere erişim• Denemeler yapmak• Global erişime sahip sistemlerdeki dosyaları hedeflemek• Ağ saldırıları yapmak için sosyal mühendislik faaliyetleri yapmak

Siber Tehditlerin Sınıflandırılması

Siber Tehdit Seviyeleri

Seviyeler	Saldırgan Tipleri	Saldırganların Amaç ve Hedefleri	Kullanılabilecek Yöntemler
Seviye 2 Siber Dolandırıcılık	Bireysel veya küçük saldırı grupları	<ul style="list-style-type: none">• Politik-ideolojik amaçlar• Dolaylı casusluk	<ul style="list-style-type: none">• Kurum içi yardımla fiziksel erişim sağlanması• Açık kaynak istihbaratı• Veri trafiğinin izlenmesi• Bilgi sistemi cihazlarının incelenmesi• Dış bilgi sistemleri ve ağlarının izlenmesi

Siber Tehditlerin Sınıflandırılması

Siber Tehdit Seviyeleri

Seviyeler	Saldırgan Tipleri	Saldırganların Amaç ve Hedefleri	Kullanılabilecek Yöntemler
Seviye 3 Siber Gözetim	<ul style="list-style-type: none">• Büyük saldırı grupları• Terör örgütleri• Organize suç örgütleri	<ul style="list-style-type: none">• Genel altyapı bilgisine sahip olmak• Büyük ölçekli saldırılar için temel verileri elde etmek	<ul style="list-style-type: none">• Veri aktarımını kolaylaştırmak için casus yazılımlar eklemek• İç ağlara genel amaçlı bilgi toplayıcılar eklemek• Kurum ağlarının taranması

Siber Tehditlerin Sınıflandırılması

Siber Tehdit Seviyeleri

Seviyeler	Saldırgan Tipleri	Saldırganların Amaç ve Hedefleri	Kullanılabilecek Yöntemler
Seviye 4 Siber Casusluk	Profesyonel istihbarat kuruluşları	Ülkelerin özel görev ve programları	<ul style="list-style-type: none">• 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 Tehditlerin Sınıflandırılması

Siber Tehdit Seviyeleri

Seviyeler	Saldırgan Tipleri	Saldırganların Amaç ve Hedefleri	Kullanılabilecek Yöntemler
Seviye 5 Siber Savaş	Askeri birlikler	Hedefin bilgi altyapısını yok etmek	<ul style="list-style-type: none">• 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 Tehdit Sıralaması

Siber Tehdit Sıralaması



Siber Tehdit Sıralaması

Siber Tehdit Sıralaması

Sıralama	2017 Yılı Tehdit Sıralaması	2018 Yılı Tehdit Sıralaması	Sıralamadaki Deđişiklik
1.	Kötü Amaçlı Yazılım	Kötü Amaçlı Yazılım	Aynı
2.	Web Tabanlı Saldırıları	Web Tabanlı Saldırıları	Aynı
3.	Web Uygulama Saldırıları	Web Uygulama Saldırıları	Aynı
4.	Oltalama Saldırıları	Oltalama Saldırıları	Aynı
5.	İstenmeyen e-postalar (Spam)	Hizmet Engelleme (DOS) Saldırıları	Yukarı
6.	Hizmet Engelleme (DOS) Saldırıları	İstenmeyen e-postalar (Spam)	Aşağı
7.	Fidye Yazılımları	Zombi Ağlar	Yukarı
8.	Zombi Ağlar	Veri İhlalleri	Yukarı

Siber Tehdit Sıralaması

Siber Tehdit Sıralaması

Sıralama	2017 Yılı Tehdit Sıralaması	2018 Yılı Tehdit Sıralaması	Sıralamadaki Deđişiklik
9.	İçerdeki Tehditler	İçerdeki Tehditler	Aynı
10.	Fiziksel Manipölasyon /Hasar / Hırsızlık / Kayıp	Fiziksel Manipölasyon /Hasar / Hırsızlık / Kayıp	Aynı
11.	Veri İhlalleri	Bilgi Sızdırma	Yukarı
12.	Kimlik Hırsızlıđı	Kimlik Hırsızlıđı	Aynı
13.	Bilgi Sızdırma	Cryptojacking	Yeni
14.	Exploit Kitleri	Fidye Yazılımları	Aşğı
15.	Siber Casusluk	Siber Casusluk	Aynı

“**Cryptojacking**” kavramı tıpkı zombi ağlar gibi, başkasının bilgisayarının kripto para üretimi kullanmak için yetkisiz bir şekilde kullanılmasıdır.

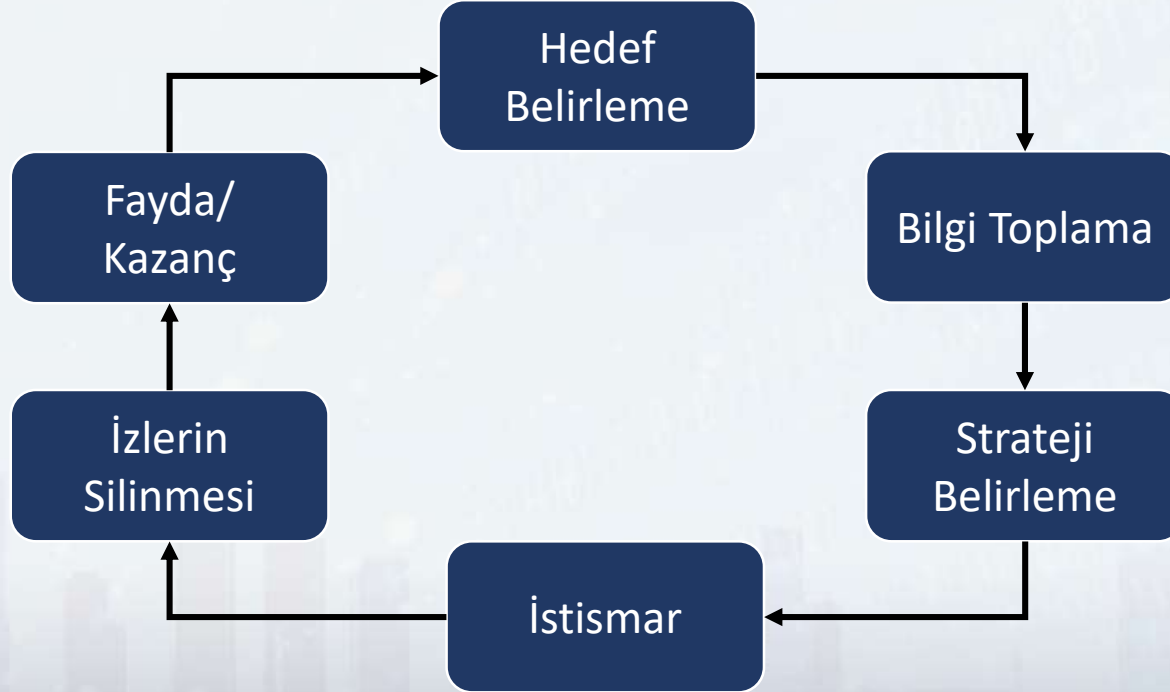
Siber Güvenlik Tehdit Belirleme Süreci

- 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 Gvenlik Tehdit Belirleme Sreci

Siber Saldırı Yařam Dngs



Deđerlendirme

- 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 deđerlendirmelerini 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.

Deđerlendirme



Deđerlendirme

Tanımlama:

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

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 kullanılmalıdır.

Deđerlendirme

Algılama/Tanıma:

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

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.

Deđerlendirme

Kurtarmak:

Siber gvenlik olayı nedeniyle bozulmuř olan tm yetenekleri veya hizmetleri geri yklemek iin uygun aktiviteler geliřtirmeyi ve uygulamayı kapsar.



Deđerlendirme

- Tm kurum ve bireylerin siber gvenlik stratejilerini ve siber gvenlik uygulama politikalarını gncel tutmaları, retilen politika ve stratejiler kapsamında kısa, orta ve uzun vadeli siber gvenlik uygulama planlarını oluřturmaları byk nem kazanmaktadır.
- Bu planlamaların toplumdaki siber uzaya eriřim sađlayan tm yař grupları ve bilgi seviyelerine gre sosyal katmanları kapsamalıdır. Bu katmanlarda; siber gvenlik farkındalıđı ile siber gvenlik bilinci oluřturacak ve katmanlar arasında da etkileřimi sađlayacak řekilde deđiřik seviyelerde siber gvenlik eđitimleri tasarlanmalıdır. Bu eđitimler uygulamalı bir řekilde gerekleřtirilmelidir.



Deđerlendirme

- 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.
- 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.



Deđerlendirme

Siber uzaydaki tm faaliyetlerde en zayıf halkanın insan olduđunu unutmayınız!



Teşekkürler



T.C. ÇEVRE, ŞEHİRCİLİK VE
İKLİM DEĞİŞİKLİĞİ BAKANLIĞI