SİBER GÜVENLİK TEMELLERİ

Ankara Üniversitesi

Bölüm Tanıtımı

- Bu bölümde siber suçların tarihçesi ve güvenlik esasları anlatılmaktadır.
- Ayrıca siber güvenliğin önemi, teknik ve teknik olmayan açılardan siber saldırıların neden arttığı ve olası karşı önlemler tartışılacaktır.

Siber Suçlar ve Siber Güvenlik Tarihi

- Dijital dünyada verileri korumaya çalıştığımızda *veri güvenliği, bilgi güvenliği, ağ güvenliği, siber güvenlik* gibi farklı tanımlamalar yapılmıştır.
- **Veri güvenliği**, dijital verilerin tüm yaşam döngüsü boyunca yetkisiz erişim, değişiklik veya ifşadan korunmasıdır.
- **Bilgi güvenliği**, fiziksel veya elektronik bilgilerin yetkisiz erişimini, kullanımını, ifşasını, değiştirilmesini, gözden geçirilmesini, kaydedilmesini veya imha edilmesini önleme uygulamasıdır. **Bilgi güvenliğinin temel amacı**, verilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini korumaktır.

Siber Suçlar ve Siber Güvenlik Tarihi

- **Ağ güvenliği**, iletişim ortamlarında iletilen verilerin yanı sıra bilgisayar ağlarının gizliliğini, bütünlüğünü ve erişilebilirliğini korumaktır.
- **Siber güvenlik**, bilgisayarları, sunucuları, mobil cihazları, elektronik sistemleri, bilgisayar ağlarını ve verileri kötü niyetli saldırılardan koruma uygulamasıdır.
- **Veri-, bilgi- ve ağ güvenliği**, saklanan verilere veya iletilen verilere yetkisiz erişimi, kullanımı, değişikliği veya imhayı önlemeyi amaçlarken; **siber güvenlik**, uçtan uca bilgi akışlarını kapsayan çok daha geniş bir uygulama alanına sahiptir.

Siber Suçlar ve Siber Güvenlik Tarihi

- Siber suçlar çok eski tarihe sahip değildir. O zamanlar dijital dünyayı savunmak daha kolaydı çünkü dijital ortamda makine sayısı azdı ve saldırılar bugünkü saldırılar kadar karmaşık değildi.
- Ancak zamanla teknolojik gelişmeler, siber suçluların karmaşık siber saldırılar başlatabilen otomatik araçlar oluşturmasına olanak sağladı. Bunun yanı sıra akıllı telefonlar, tabletler, IoT cihazları, bulut platformları, sosyal medya platformları ve daha pek çok farklı makine ve platform internete eklenmektedir. Tüm bu nedenler, siber suçları basit bir şakadan, dijital ortamda dünya ekonomisine her yıl trilyonlarca dolara mal olan karmaşık saldırılara dönüştürmüştür.

Siber Suçlar ve Siber Güvenlik Tarihi

Tablo1. Yıllara göre siber suçların sınıflandırılması

Zaman Periyodu	Siber Suçlar
1940	Bilgisayar suçlarının olmadığı yıllar
1950	On yıllık telefon hırsızlığı
1960	Bilgisayar korsanlığı ve güvenlik açığı terimleri görülmeye başlanmıştır
1970	Bilgisayar güvenliğinin doğuşu
1980	ARPANET'in İnternet'e geçiş yılları
1990	Bilgisayar virüsleri ve solucanları popüler hale gelmiştir
2000	İnternetin aşırı büyümesi
2010	Siber suçlular bilgisayar sistemlerinde birkaç güvenlik ihlali keşfediyor
2020	Siber suçlar bir endüstri haline geldi

Siber Suçlar ve Siber Güvenlik Tarihi

- On yıllar boyunca siber suçların sınıflandırılması Tablo 1'de özetlenmiştir. İlk bilgisayar 1940'ların başında ortaya çıkmıştır. O zamanlar internet bağlantısı yoktu ve bilgisayarların yalnızca sınırlı kullanımı mümkündü.
- Bilgisayarlar arasında bilgi paylaşımı olmadığı için bu dönemde bilgisayara herhangi bir tehdit veya saldırı olmamıştır.
- Telefon dolandırıcılığı 1950'lerde başlamıştır. Telefon dolandırıcıları, telefon sistemlerinde ücretsiz görüşme yapmak için kullanılan protokolleri ele geçirmeye veya uzun mesafe için telefon görüşme ücretini düşürmeye çalışıyordu. O zamanlar, birkaç telefon şirketi telefon dolandırıcılığının oluşmasını engelleyemedi. Gelecekte, bilgisayar sistemlerini hacklemek için telefon dolandırıcılığına benzer teknikler kullanılacaktır.

Siber Suçlar ve Siber Güvenlik Tarihi

- Bilgisayar sistemleri için hackleme terimi ilk olarak 1960'larda ortaya çıktı.
- 1965 yılında IBM 7094 Uyumlu Zaman Paylaşım Sistemi (CTSS) makinesinde ilk güvenlik açığı bulundu.
- 1967'de IBM, IBM'in yeni tasarlanmış bilgisayarını keşfetmeleri için bir grup öğrenciyi işe aldı. Öğrenciler bilgisayar sisteminin dilini öğrendiler ve sistemin farklı bölümlerine erişim sağladılar. Bu örnek, bilgisayar sistemlerinin bazı güvenlik açıklarının olduğunu kanıtladı ve bu durum etik hacking uygulamasının ilk örneği oldu.

Siber Suçlar ve Siber Güvenlik Tarihi

- Siber güvenliğin temelleri 1970'li yılların başında "Gelişmiş Araştırma Projeleri Ajans Ağı" (ARPANET) adlı proje ile başlamıştır. Bu, internetten önceki ilk paket anahtarlamalı ağdı.
- 1971'de Bob Thomas, bir ARPANET ağı üzerinden hareket edebilen "Creeper" adlı ilk virüsü yarattı. "Creeper"ın ardından Ray Tomlinson, ARPANET üzerinde de hareket edebilen "Reaper"ı yarattı ve "Creeper"ı sildi.
- "Reaper" antivirüs programının ilk örneğiydi.
- 1979 yılında ünlü bir bilgisayar korsanı olan Kevin Mitnick, ilk siber suçlu davranışı nedeniyle tutuklandı.

Siber Suçlar ve Siber Güvenlik Tarihi

- 1980'lerde bilgisayarla ilgili birkaç saldırı görüldü. Bu on yılda çoğunlukla bilgisayar virüsleri kullanılmıştır. Siber casusluk terimi bu dönemde kullanılmaya başlandı çünkü en büyük korku diğer hükümetlerden gelen tehditti.
- 1985 yılında Amerika Birleşik Devletleri (ABD) Savunma Bakanlığı, daha sonra "Turuncu Kitap" olarak adlandırılan «Güvenilir Bilgisayar Sistemi Değerlendirme Kriterleri» adlı bilgisayar güvenlik yönergeleri oluşturdu. Bu yönergeler, bilgisayar sistemleri için ilk güvenlik rehberiydi.
- 1986'da Alman hacker Marcus Hess, ABD, Doğu Asya ve Avrupa hükümetlerinin sistemlerine sızdı. Yaklaşık 400 askeri bilgisayara erişebiliyordu. Hacklenen bilgiler uzay, uydu ve uçak teknolojilerini içeriyordu. Şu anda güvenlik şirketler için önemli bir endişe haline geldi.
- Ticari olarak ilk antivirüs yazılımı ise1987'de yayınlandı.

Siber Suçlar ve Siber Güvenlik Tarihi

- 1990'larda bilgisayar sistemleri ve internette muazzam bir büyüme yaşandı. Bilgisayar virüsü ve farklı versiyonları çok popüler oldu.
- Makro virüsleri 1996'da piyasaya sürüldü.
- 1990'ların sonlarında Melissa ve ILOVEYOU virüsleri birçok ülkede milyonlarca bilgisayarı etkiledi.
- 1995 yılında Netscape, bir bilgisayar ağı üzerinden kullanıcılar arasındaki bağlantıları güvence altına alan güvenli yuva katmanı (SSL) protokolünü tanıttı.

Siber Suçlar ve Siber Güvenlik Tarihi

- 2000'li yıllarda internet aşırı büyüdü. Bilgisayarlar evlerin yanı sıra iş yerlerinde de kullanılmaya başlandı. Bilgisayarların birçok yerde kullanılması verimliliği artırırken, birçok kullanıcı için güvenlik riskini de beraberinde getirdi. Yani bilgisayar kullanımının artması siber suçları da artırdı.
- İlk organize hacker grubu 2000'li yıllarda ortaya çıktı. Önce bilgisayar solucanı, ardından Trojan popüler oldu. Sadece web sitesini açmak, gerçek dosyaları indirmeden virüs bulaşması için yeterliydi.
- 2004 yılında, dağıtılmış hizmet reddi (DDoS) saldırılarına neden olan ve uzaktan erişime izin veren MyDoom solucanı yayıldı.
- 2007'de, banka, sosyal ağlar ve e-posta hesapları dahil olmak üzere oturum açma kimlik bilgilerini çalmak için bir bulaşma vektörü olarak sürücüden indirmeleri ve spam e-postayı kullanan Zeus Truva atı ortaya çıktı.

Siber Suçlar ve Siber Güvenlik Tarihi

- 2010'larda siber suçlular, bilgisayar ağ protokollerinin yanı sıra yazılımlarda da birkaç güvenlik ihlali keşfetti. Bu güvenlik ihlalleri sonucunda bireyler her yıl milyonlarca dolar, büyük şirketler ve ülkeler milyarlarca dolar kaybediyor.
- 2016'da Mirai kötü amaçlı yazılımı, DDoS saldırılarını başlatmak için bir IoT cihazı güvenlik açığından yararlandı.
- 2010 ile 2020 arasında, fidye yazılımıyla ilgili saldırılar çok popüler hale geldi. WannaCry Ransomware bilgisayar sistemlerini şifreledi ve dünya genelinde 150 ülkeyi etkiledi. LockerGoga Ransomware, virüslü sistemi bloke etti ve milyonlarca dolarlık hasara neden oldu.

Siber Suçlar ve Siber Güvenlik Tarihi

- 2020'de CovidLock Ransomware, Android cihazlardaki verileri şifreledi ve veri erişimini reddetti. Birkaç Android cihazı etkiledi.
- Bu günlerde, dijital dünyadaki her şeyi hacklemek neredeyse mümkün. Bazı profesyonel web siteleri, bilgisayar korsanlığı için otomatik uygulamalar ve araçlar sağlayan bir hizmettir.
- İlk zamanlarda siber suçluların siber saldırılar başlatmak için bazı basit teknikler kullandıkları söylenebilir. Bununla birlikte, zamanında siber saldırılar, büyük şirketlerin ve bazı hükümetlerin önünde olduğu büyük bir kazanç olarak görülüyor.

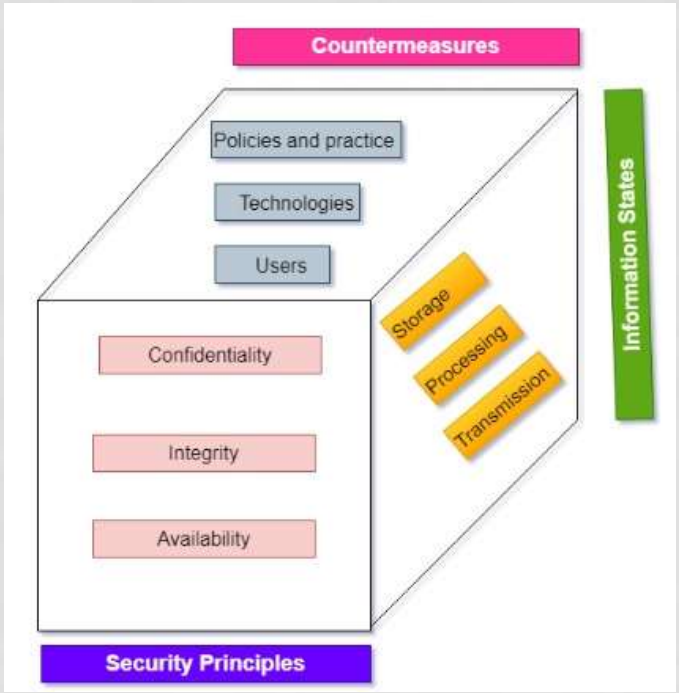
Siber Suçlar ve Siber Güvenlik Tarihi

Tablo2. Yıllara göre popüler siber saldırılar

Siber Saldırı	Yıl	Saldırı Metodu	Sonuçları
Citibank'a Vladimir Levin atağı	1994-1995	bilinmiyor	Yaklaşık 10 milyon dolar çalındı
Melissa Virus	1999	e-posta ekini tıklatmak için kullanıcıların güvenini kullandı	birçok ülkede milyarlarca dolar kaybedildi
ILOVEYOU solucanı	2000	e-posta ekini tıklatmak için kullanıcıların güvenini kullandı	45 milyondan fazla bilgisayara virüs bulaştı
MyDoom solucanı	2004	hatalar, testler vb. gibi dikkat çekici konuları e-posta ile kullandı.	Uzaktan erişime izin vererek DDos saldırıları başlatıldı
Zeus truva atı	2007	Drive-by indirmeleri ile spam e-posta	e-posta ve banka hesapları gibi giriş bilgileri çalındı
Stuxnet solucanı	2010	kaynak kodlarını çalarak programlanabilir mantık birimine saldırı	endüstriyel süreçlerin kontrolü alındı
ABD Doğal Gaz Boru Hattına Saldırı	2012	kimlik avı yoluyla gizli bilgilere erişim	güvenlik kimlik bilgileri çalındı
Mirai Malware	2016	IoT cihazlarının güvenlik açığından yararlanıldı	DDos saldırıları başlatıldı
WannaCry fidye yazılımı	2017	Windows güvenlik açığından yararlanıldı	bilgisayar sabit diskleri şifrelendi ve 150 ülke etkilendi
Emotet truva atı	2018	spam ve kimlik avı kampanyaları biçimindeki e-postalar	kredi kartı bilgileri gibi hassas bilgiler çalındı
MyFitnessPal	2018	yazılım güvenlik açığından yararlanıldı	150 milyon kullanıcı etkilendi
Magellan'a Fidye Yazılımı Saldırısı	2020	spam ve kimlik avı kampanyaları biçimindeki e-postalar	365.000 hastanın sağlık verileri çalındı
CovidLock fidye yazılımı	2020	COVID-19 istatistiğini kullanarak kullanıcıların güvenini kötüye kullandı	Android cihazların verileri şifrelendi ve veri erişimi reddedildi
Accellion Tedarik Zinciri Saldırısı	2021	üçüncü taraf güvenlik açıklarından yararlanıldı	büyük kuruluşlardan gizli veriler çalındı
Kaseya fidye yazılımı	2021	sıfır gün istismarları kullanıldı	kurban başına 50.000 ila 5 milyon dolar fidye talep edilerek yaklaşık 1500 şirketin verileri ele geçirildi

Bilgi Güvenliği İlkesi

- Siber güvenliğin ilk boyutu, bilgileri saldırganlardan korumaktır. Bu aynı zamanda bilgi güvenliği ilkesi olarak adlandırılmıştır. Bu ilkeler **gizlilik, bütünlük ve kullanılabilirliktir** (CIA).
- Siber güvenliğin ikinci boyutu tüm durumlarda verileri korumaktır. Bu durumlar **depolamadaki veriler, transit veriler ve işlemdeki verilerdir**. Kablolu ağlar ve kablosuz ağlar gibi cihazlar arasında veri aktarmak için çeşitli yöntemler vardır. Siber güvenlik, cihazlarda depolanan veriler veya farklı ağ cihazları ve ana bilgisayarlar arasında iletildiğinde veri gizliliğini, bütünlüğünü ve kullanılabilirliğini korumalıdır.
- Siber güvenliğin üçüncü boyutu, **politikalar ve uygulama, yeni teknolojiler ve kullanıcıların** siber uzayı korumaya yardımcı olmak için ek şeylerin kullanılmasıdır.



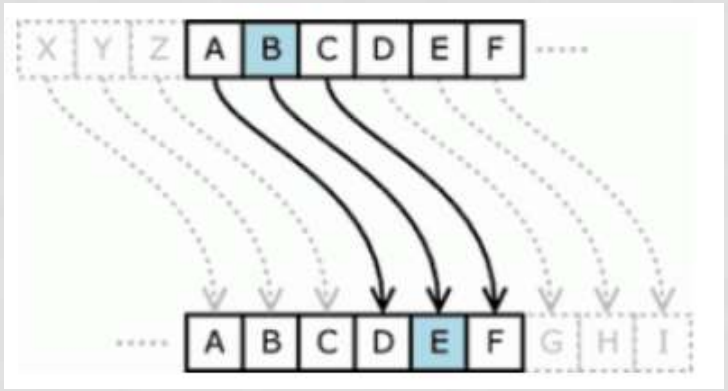
Bilgi Güvenliği İlkesi-Gizlilik

- Gizlilik, dijital dünyadaki yetkisiz kullanıcılar ve programlardan bilgilerin korunmasıdır. Veriler gizli, çok gizli, özel ve sınıflandırılmamış olarak ayrılmaktadır.
- Çok gizli ve gizli veriler, en yüksek koruma seviyesine ihtiyaç duyan çok önemli verilerdir. Bu verilerin açıklanması ulusal güvenliğe büyük zarar verebilir, bu nedenle bu verilere erişim kesinlikle kısıtlanmalıdır.
- Özel veriler de açıklanmaması gereken şekilde hassastır. Öte yandan, sınıflandırılmamış veriler hassas değildir ve herhangi biri için herkese açıktır. Sınıflandırılmamış verilerin açıklanması ulusal güvenliği etkilemez. Hükümetler, kuruluşlar ve şirketler, siber saldırganlardan çok gizli, gizli ve gizli bilgiler de dahil olmak üzere değerli varlıklarını korumak için çalışanlarını eğitmelidir. Verilerin gizliliğini korumak için şifreleme, kimlik doğrulama ve erişim kontrolü kullanabiliriz.

Bilgi Güvenliği İlkesi-Gizlilik

- **Şifreleme**: Orijinal verileri okunamayan bir versiyonuna dönüştürerek orijinal bilgileri gizleyen matematiksel tekniktir. Şifreleme, siber güvenlikte bilgisayar sistemlerini ve verilerini kaba kuvvet saldırılarına, casus yazılımlara ve fidye yazılımlarına karşı savunmak için kullanılmıştır.
  - **Örnek şifreleme: Sezar Şifreleme**
  - 'selam' kelimesinin şifreli hali 'uğoçö' dir.

s + 3 = **u**	u - 3 = **s**
e + 3 = **ğ**	ğ - 3 = **e**
l + 3 = **o**	o - 3 = **l**
a + 3 = **ç**	ç - 3 = **a**
m + 3 = **ö**	ö - 3 = **m**



Bilgi Güvenliği İlkesi-Gizlilik

- **Erişim Denetimi**, bilgisayar sistemlerine ve bilgisayar ağlarına yetkisiz erişimi önlemek için çeşitli koruma mekanizmalarını tanımlar. Erişim kontrolü, kuruluş riskini en aza indiren temel bir güvenlik kavramıdır.

- **AAA (Authentication, Authorization and Accounting)** kavramı, kimlik doğrulama, yetkilendirme ve muhasebe gibi üç güvenlik hizmeti sunar.
- Kimlik doğrulama, yetkisiz erişimi önlemek için bilgisayar sistemine bir kimlik sağlamaktır. Sistem, kullanıcı adı-password kombinasyonunu kullanarak kullanıcıların kimliğini doğrulayabilir.
- Yetkilendirme, kullanıcıların hangi bilgisayar ve ağ kaynaklarına erişebileceğini ve kullanıcıların hangi işlemleri gerçekleştirebileceğini tanımlar.
- Muhasebe, kullanıcıların ne yaptıklarını, hangi kaynaklara eriştiklerini ve hangi değişiklikleri yaptıklarını izler.

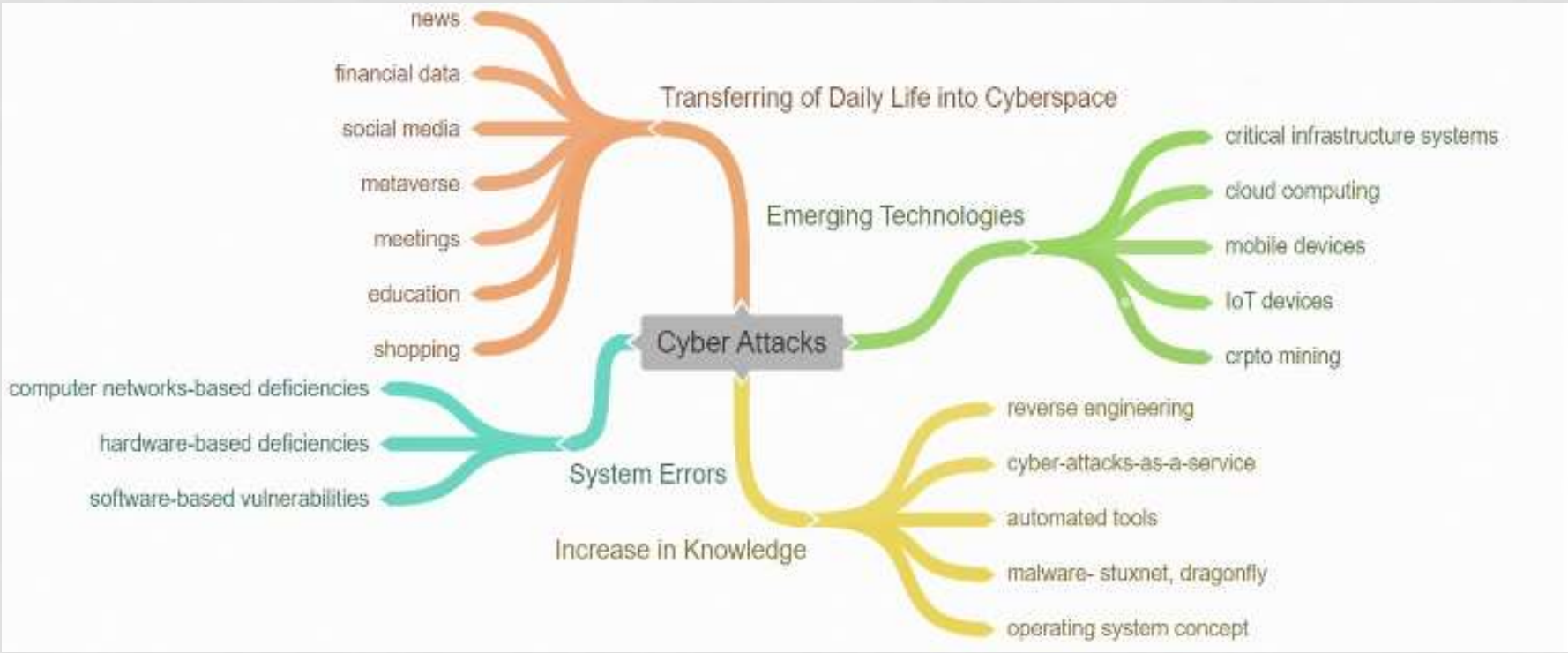
Bilgi Güvenliği İlkesi-Bütünlük

- **Bütünlük**, tüm yaşam döngüsü boyunca verilerin doğruluğu, kalitesi, tutarlılığı ve bütünlüğü ile ilgilidir. Bütünlüğü sağlamak için bilgiler yalnızca değiştirme hakkına sahip kullanıcılar tarafından değiştirilebilir. Veri bütünlüğü, çeşitli nedenlerle modern işletmeler için birinci önceliktir.
- Veri bütünlüğü geri kazanılabilirlik, izlenebilirlik ve bağlantı sağlar. Fiziksel cihaz uzlaşması, disk çökmesi, kötü amaçlı yazılım, hackleme, format boyunca tutarsızlıklar, cihazlar arasındaki veri aktarım hataları ve insan hatası nedeniyle veri bütünlüğü kaybedilebilir. Veri bütünlüğünü korumak için karma, veri tutarlılık kontrolleri ve veri doğrulama kontrolleri kullanılabilir.

Bilgi Güvenliği İlkesi-Kullanılabilirlik

- **Kullanılabilirlik** veri erişilebilirliği ile ilgilidir. Başka bir deyişle, veriler yetkili kullanıcı bunu talep ettiğinde veya kullandığında vardır.
- Sistem arızaları ve siber saldırılar bilgi sistemlerine ve hizmetlerine erişimi önleyebilir. DDOS saldırıları, meşru kullanıcılar sisteme erişmeye çalıştığında sistemin kullanılabilirliğini hedefleyen en yıkıcı siber saldırılardan biridir. DDOS saldırılarını tamamen durduran iyi bilinen bir sistem yoktur. Kullanılabilirliği sağlamak için sistem yedeklemeleri, sistem fazlalığı, sistem esnekliği, güncel işletim sistemi ve yazılım kullanılmalıdır. Buna ek olarak, sistem tek başarısızlık noktalarını ortadan kaldırabilir ve meydana geldiğinde arızaları tespit edebilir.

Siber Saldırılar Neden Artıyor?



Siber Saldırılar Neden Artıyor?

- Siber saldırıların başlıca nedenleri aşağıdaki gibi listelenebilir:
- 1. Mevcut sistem hatalarından kaynaklanan nedenler
- 2. Ortaya çıkan teknolojilerden kaynaklanan nedenler
- 3. Bilgi artışından kaynaklanan nedenler
- 4. Günlük yaşamın dijital ortama aktarılması
- 5. Saldırıların tespit edilmesini zorlaştıran coğrafi sınırlarının olmaması

Siber Saldırılar Neden Artıyor?

Mevcut sistem hatalarından kaynaklanan nedenler

- donanım eksikliklerinden kaynaklanan saldırılar,
- yazılım tabanlı buglardan kaynaklanan saldırılar
- bilgisayar ağlarındaki güvenlik açıklarından kaynaklanan saldırılar

olmak üzere üç gruba ayrılmaktadır.

1. Donanım eksikliklerinden kaynaklanan saldırılar: Donanım tabanlı eksiklikler ve hatalar kullanılarak başlatılan saldırıların önlenmesi daha zordur çünkü yazılım tabanlı geliştirilen araçlar donanım kaynaklı saldırıları tespit etmede ve önlemede yetersiz kalmaktadır. Truva atları, donanıma yönelik saldırıların temelinde yer alır. Bu kötü amaçlı yazılım varyantları, bilgisayar kaynaklarının aşırı kullanılmasına, performansın düşmesine ve aşırı güç kaynağı tüketimine neden olarak sistemin kapanmasına neden olur. Ayrıca, donanım parçalarının yasa dışı olarak kopyalanması ve güvenilmeyen bazı parçaların çevrimiçi olarak elde edilmesi, bilgisayar sisteminde arka kapılar oluşturur.

Siber Saldırılar Neden Artıyor?

Mevcut sistem hatalarından kaynaklanan nedenler

2.Yazılım tabanlı hatalardan kaynaklanan saldırılar: Siber saldırıların büyük bir çoğunluğu hala uygulama yazılımlarındaki hatalar, güvenlik açıkları ve eksikliklerden kaynaklanmaktadır. Bu güvenlik açıkları ve hatalar her geçen gün artmaktadır. Yazılım kaynaklı zafiyet ve hataların başlıca nedenleri şu şekilde sıralanabilir:

- giriş doğrulama hataları
- kullanıcı erişim kontrolü ile ilgili sorunlar
- eksik veya yanlış kimlik doğrulama
- taşıma dizini sorunu
- tampon taşması
- yapılandırılmış sorgu dilinin (SQL) neden olduğu sorunlar
- siteler arası komut dosyası çalıştırma (XSS)
- bilinen güvenlik açıklarına sahip bileşenleri kullanma
- web hizmetleri ve API'lerle ilgili sorunlar
- uygunsuz yazılım güvenlik testi

Siber Saldırılar Neden Artıyor?

Mevcut sistem hatalarından kaynaklanan nedenler

3. Bilgisayar ağlarındaki güvenlik açıklarından kaynaklanan saldırılar: İnternet üzerinden veriler aktarılırken bilgisayar korsanları verilere erişebilir, değiştirebilir veya tamamen değiştirebilir. Bu tür tehditlerin ortaya çıkmasının temel nedeni, önceden oluşturulmuş bilgisayar ağ protokollerinin ve ağ cihazlarının herhangi bir güvenlik kaygısı olmadan oluşturulması ve yapılandırılmasıdır. Bilgisayar ağlarına yönelik saldırıların büyük çoğunluğu, ağ protokollerindeki güvenlik açıklarından kaynaklanmaktadır. Bu protokoller, iletim kontrol protokolü (TCP), İnternet protokolü (IP), adres çözümleme protokolü (ARP), dinamik ana bilgisayar yapılandırma protokolü (DHCP) ve alan adı sistemi (DNS) olarak sıralanabilir. Örneğin, IP kullanılarak ağ üzerinden paketler taşınırken, bu paketlerin doğruluğunu ve gizliliğini kontrol edecek bir yapı bulunmadığından, taşıma sırasında paketlerdeki bilgiler açığa çıkabilir ve değiştirilebilir.

Siber Saldırılar Neden Artıyor?

Ortaya çıkan teknolojilerden kaynaklanan nedenler

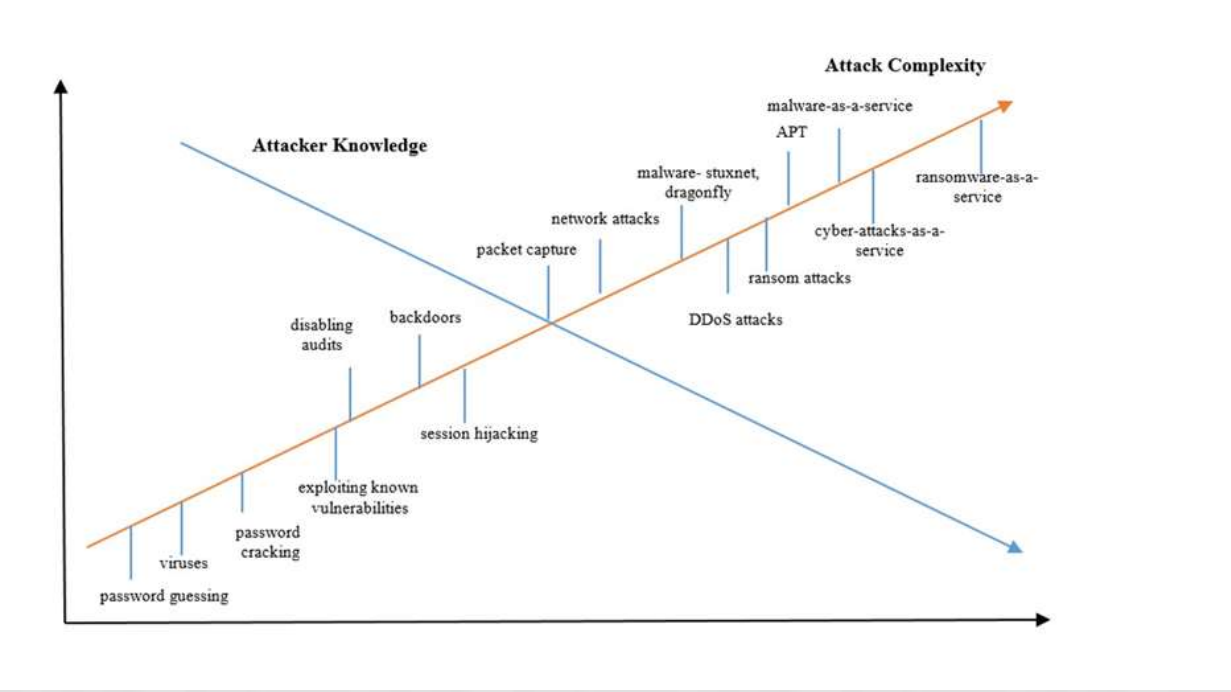
Teknolojinin hızlı gelişimi ile birlikte internet ortamına her geçen gün yeni cihazlar ve yazılımlar eklenmektedir.Çok sayıda uygulama programının kısa sürede üretilmesi, akıllı telefon ve IoT cihazları gibi yeni cihazların bilgisayar ağlarına eklenmesi siber saldırıların sayısını artırıyor. Ayrıca farklı şirketlere ait bilgilerin bulut ortamında aynı fiziksel yapı üzerinde saklanması ve bu ortamların 3. kişiler tarafından yönetilmesi ve bakımının yapılması da güvenlik kaygılarını artırmaktadır. Yeni gelişen teknolojilerden kaynaklanan nedenler ise şu şekilde sıralanabilir:

1. Artan akıllı telefon sayısı
2. Artan IoT cihazlarının sayısı
3. Bulut bilişimin kullanımının artması
4. Kritik altyapı sistemlerinin sayısındaki artış

Siber Saldırılar Neden Artıyor?

Bilgi artışından kaynaklanan nedenler

1990'larda ve 2000'lerin başında bilgisayar sistemlerine saldırılar başlatmak çok zordu. Sadece bilgisayar sistemlerinde geniş bilgi ve deneyime sahip uzmanlar bilgisayar sistemlerine saldırabilir. Son birkaç yılda, saldırı araçlarının yaygın kullanımı, bilginin hızla yayılması ve bilgisayar yazılımı ve ağ protokollerinde güvenlik açıklarının kolay tespiti sonucunda siber saldırıları başlatmak daha kolay hale geldi.



Siber Saldırılar Neden Artıyor?

Günlük yaşamın dijital ortama aktarılması

- Sosyal yaşamın yıllar önce sanal çevreye geçmeye başlaması
- Sosyal medya ortamlarının kullanıcıların önemli kişisel bilgilerini depolaması
- Büyük kurum ve kuruluşların %50'sinden fazlasının, çalışanlarının sosyal medyada aşırı bilgi paylaşımı
- Banka kartlarının ve kredi kartlarının yayılması
- Sanal paranın yaygınlaşması

Siber Saldırılar Neden Artıyor?

Saldırıların tespit edilmesini zorlaştıran coğrafi sınırlarının olmaması

Siber saldırılar, coğrafi sınırlar olmadan dünyanın herhangi bir yerinden 7/24 meydana gelebilir. Saldırı sırasında yakalanmamak için saldırganlar, yerlerini gizlemek için belirli teknikler kullanırlar. Buna ek olarak, farklı ülkeler arasında siber saldırılarla ilgili caydırıcı yasaların olmaması, saldırı noktasında siber suçluları teşvik etmektedir. İnternete saldırmanın kolay olması, coğrafi sınırların olmaması ve siber suçluların ülkeler arasında teslim edilmesi noktasında mevzuat eksikliği, siber saldırılardaki artışın nedenleri arasında gösterilebilir.

Özet

- Bu bölümde, siber saldırıların zamanla gelişiminden bahsedilmiştir.
- Saldırılarda artışa neden olan teknik ve teknik olmayan nedenler listelenmiştir.
- Siber saldırılar dinamiktir ve saldırı formatını ve hedef kitleyi zaman zaman değiştirerek tüm bilgisayar tabanlı sistemleri ve internet ortamını etkiler.
- Sosyal yaşamın internet ortamına aktarılması siber saldırıları ve yıkıcı etkilerini arttırır.
- Oluşturulan yazılımdaki hatalar ve güvenlik açıkları, ağ protokollerinin yetersizliği, ağa eklenen cihaz sayısındaki artış ve kritik sistemlerin karmaşıklığı siber güvenlik risklerini artırır.
- Buna ek olarak, sosyal yaşamın sanallaştırılması, sosyal ağların aşırı kullanımı, saldırganların artan bilgileri ve kullanıcıların internette dikkatsiz kullanımı da dijital dünyada güvenlik risklerini artırmaktadır.