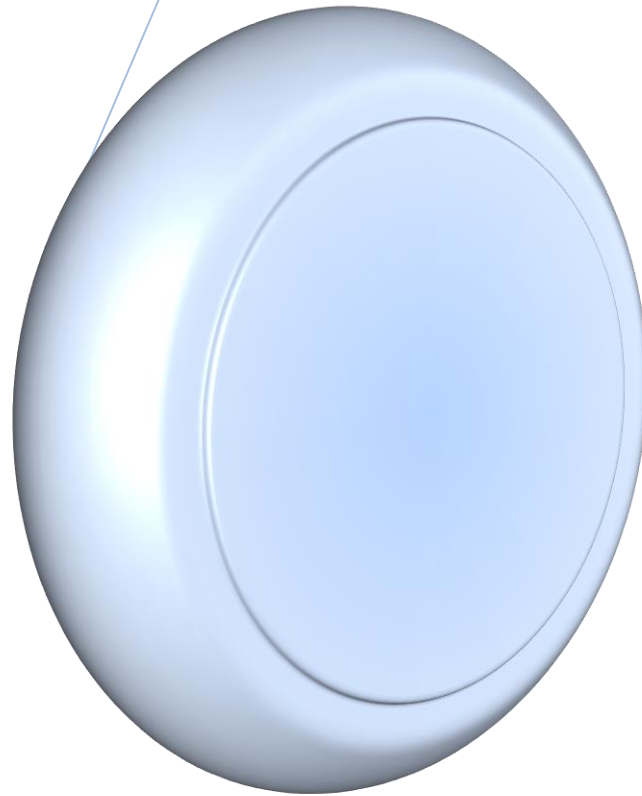


Siber Güvenlięe Giriş

Siber Güvenlięe giriş amaçlı düzenlenen PDF dökümü

Engin Arslan
25.08.2024



İçindekiler

EĞİTİM KAZANIMLARI	V
SİBER GÜVENLİK NEDİR?	1
Veri Nedir?.....	1
Kişisel Veriler Nelerdir?	1
Bilgi Güvenliği Nedir?	1
Siber Güvenlik Nedir?.....	2
HACKER TÜRLERİ	2
1. Siyah Şapkalı Hacker (Black Hat Hackers).....	2
2. Beyaz Şapkalı Hacker “Siber Güvenlik Uzmanları”	2
3. Gri Şapkalı Hacker (Gray Hat Hackers)	3
Sosyal Mühendisler (Social Engineers).....	3
Script Kiddies	3
Siber Güvenlik Uzmanı Çeşitleri (Red and Blue Team)	4
Siber Güvenlikte Bilinmesi Gereken Sistemler	4
SİBER GÜVENLİK KAVRAMLARI.....	4
ZARARLI YAZILIMLAR	7
1. Virüs.....	7
2. Worm (Solucanlar).....	7
3. Spyware (Casus Yazılım)	8
4. Adware (Reklam Yazılımı).....	8
5. Trojan (Truva Atı).....	9
6. Botnets (Zombi).....	9
7. Ransomware (Fidye Yazılımı).....	10
SALDIRI TÜRLERİ	10
Buffer Overflow	10
Croos-Site Request Forgery “CSRF”	10
Croos-Site Scripting (XSS)	11
Broken Access Control (Yetkisiz Erişim).....	11
Zero-Day Exploits (0 Days).....	11
Port Configuration Hataları (Port Ayarları Hatası).....	11
Rat (Remote Access Trojan) “Uzaktan Erişim Aracı”	11
Man-In-The-Middle (MITM) Saldırıları (Ortadaki Adam Saldırıları)	12

Denial-Of-Service (DOS) Saldırıları	12
SOSYAL MÜHENDİSLİK VE DALLARI	13
1. Phishing	13
2. Spear Phishing (Tek kişi veya gruba yönelik saldırı)	13
3. Shoulder Surfing (Omuz Sörfü).....	13
4. Dumpster Diving (Çöp Karıştırma).....	13
5. Role Playing (Rol Yapma).....	14
6. Pretexting (Bahane Uydurma).....	14
7. Baiting (Yemleme)	14
8. Tailgating (Kuyrukta Sürünme).....	14
9. Quid Pro Quo (Karşılık Bekleme)	14
10. Impersonation (Kimlik Taklidi).....	14
11. Farming (Çiftçilik).....	15
12. Vishing (Sesli Fishing).....	15
13. Water Holing.....	15
HACKER METODOLOJİSİ	16
SİBER GÜVENLİK ÖNERİLERİ	16
DONANIM ALTYAPISI GÜVENLİĞİ	17
Donanım Güvenliği	17
Altyapı Güvenliği.....	18
İşletim Sistemi Güvenliği	18
Uygulama Sunucusu Güvenliği	18
VERİ SIZINTISI (DATA BREACH)	19
A. İstem Dışı – Kazara Veri Sızıntısı	19
B. İstemli – Kasıtlı Veri Sızıntısı	19
Veri Sızıntısını Önleme.....	20
PAROLA/ŞİFRE NEDİR?.....	21
Parola ve Şifre Arasındaki Fark	21
Parola Güvenliği.....	21
Parola Saldırıları Nedir?	21
1. Brute Force Saldırısı:.....	22
2. Dictionary (Sözlük) Saldırısı:	22
3. Phishing Saldırısı:.....	22
4. Rainbow Table Saldırısı:.....	22

VERİTABANI GÜVENLİĞİ	23
Veri Tabanı Güvenliği Unsurları	23
KURUMSAL AĞ GÜVENLİĞİ (CORPORATE NETWORK)	24
KABLOSUZ AĞ GÜVENLİĞİ (WIRELESS NETWORK)	24
OWASP (WEB UYGULAMA GÜVENLİĞİ)	25
GÜVENLİK AMAÇLI KOD ANALİZLERİ	25
Güvenlik Amaçlı Kod	25
Statik Kod Analizi	25
Dinamik Kod Analizi	26
GÜVENLİ YAZILIM GELİŞTİRME (SSDLC)	26
SSDLC (Planlama) Ne İşe Yarar?	26
SİBER GÜVENLİK RİSK YÖNETİMİ	27
Siber Riskler	27
Siber Risk Yönetimi Tablosu	27
KVKK (Kişisel Verileri Koruma Kanunu) Nedir?	28
SİBER GÜVENLİK SERTİFİKALARI	29
OSCP (Offensive Security Certified Professional):	29
OSCE (Offensive Security Certified Expert):	29
OSWE (Offensive Security Web Expert):	29
OSWP (Offensive Security Wireless Professional):	29
CISSP (Certified Information Systems Security Professional)	29
CEH (Certified Ethical Hacker)	29
Comptia Security+	30
Ccna Cyberops (Cisco Certified Network Associate - Cyberops)	30
Certified Cloud Security Professional (CCSP)	30
SİBER GÜVENLİK ALANINDA POZİSYONLAR VE ÜNVANLAR	31
Bilgi Güvenliği Uzmanı (Information Security Specialist):	31
Ağ Güvenliği Mühendisi (Network Security Engineer):	31
Sızma Testi Uzmanı (Penetration Tester):	31
Güvenlik Analisti (Security Analyst):	31
Kimlik ve Erişim Yönetimi Uzmanı (Identity and Access Management Specialist):	31
Veri Güvenliği Analisti (Data Security Analyst):	31
Güvenlik Mimar (Security Architect):	31
! Olay Yanıtı Uzmanı (Incident Response Specialist):	31

Uygulama Güvenliği Uzmanı (Application Security Specialist):.....	32
Eğitim ve Farkındalık Uzmanı (Training and Awareness Specialist):	32
Yazılım Geliştirme Güvenliği Danışmanı (Secure Development Consultant):	32
Güvenlik Denetçisi (Security Auditor):	32
Mobil Uygulama Güvenliği Uzmanı (Mobile Application Security Specialist):	32
Güvenlik Ekip Lideri (Security Team Leader):	32
Veri Gizliliği Danışmanı (Data Privacy Consultant):	32
Endüstriyel Kontrol Sistemleri Güvenliği Uzmanı (Industrial Control Systems Security Specialist): .	32
Blockchain Güvenliği Uzmanı (Blockchain Security Specialist):.....	32
Dijital Tehdit Analisti (Digital Threat Analyst):	32
Yapay Zeka ve Makine Öğrenimi Güvenliği Uzmanı (AI and Machine Learning Security Specialist):	33
Uygulama Penetrasyon Testi Uzmanı (Application Penetration Testing Specialist):	33
Veri Analitiği ve Güvenlik Uzmanı (Data Analytics and Security Specialist):	33
Siber Hukuk Uzmanı (Cybersecurity Lawyer):	33
SOME VE SOC	34
Some (Siber Olaylarla Mücadele Ekibi) “Blue Team”	34
Some Ekibinde Çalışan Kişiler	35
Soc (Güvenlik Operasyon Merkezi)	36
Görevleri	36
İşleyişi	37
Önemi	37
Soc Örnekler	38
Soc Ekibinde Çalışan Kişiler.....	38
PROGRAM SERTİFİKASI.....	39

EĞİTİM KAZANIMLARI

Eğitimin sonunda;

- Siber güvenliği ve ilgili kavramları temel seviyede ifade edebilir,
- Siber güvenliğin alt alanlarının (sistem güvenliği, uygulama güvenliği, ağ güvenliği, veri tabanı güvenliği vb.) ne olduğunu ifade edebilir,
- Siber zafiyetlerin ne olduğunu ve kaynaklarını ifade edebilir,
- Siber tehdit, risk ve saldırı kavramlarını ayırt edebilir.

SİBER GÜVENLİK NEDİR?

Siber güvenlik dijital ortamda bilginin ve verinin güvenliği için yapılan tüm çalışmalardır.

Ağ yapısına bağlı ve bu sistemlerle ilişkili verileri yetkisiz kullanım veya zararlardan korumak için sarf edilen sonsuz bir çabadır.

Veri Nedir?

Veri, bilgisayarların işleyebileceği bir forma dönüştürülmüş gerçekler (sayılar, kelimeler, ölçümler, gözlemler, vb.) topluluğudur.

Kişisel Veriler Nelerdir?

1. Çevrimdışı Kimliğiniz
2. Çevrimiçi Kimliğiniz
3. Tıbbi Kayıtlar (Hasta Kayıtları)
 - Fiziksel, zihinsel ve diğer kişisel bilgiler
 - Reçeteler
4. Eğitim Kayıtları
 - Notlar, sınav puanları, alınan dersler, ödüller ve dereceler
 - Devamlılık
5. İstihdam ve Finansal Kayıtlar
 - Gelir ve giderler
 - Vergi kayıtları – maaş çekleri, kredi kartı özeti (ekstre) ve kredi notu
 - Geçmiş istihdam ve performans bilgileri

Bilgi Güvenliği Nedir?

Bilgi güvenliği, bir organizasyonun veya bireyin hassas bilgilerini, verilerini ve bilgi kaynaklarını, yetkisiz erişim, değiştirme, ifşa veya zarar verme gibi tehditlere karşı koruma sürecidir.

Bilgi güvenliği, bilgiyi gizli, bütünlüklü ve erişilebilir şekilde koruma amacını taşır. Bu kapsamda bilgi güvenliği, fiziksel güvenlik önlemlerini, teknik önlemleri ve insan kaynaklarına yönelik politikaları içerir.

Bilgi Güvenliğinin Temel Hedefleri: Gizlilik, Bütünlük, Erişilebilirlik, Süreklilik ve İzlenebilirlik

Siber Güvenlik Nedir?

Siber güvenlik özel bir alan: Bilgi sistemlerini ve ağıları korumak için alınan özel önlemleri ifade eder. Siber güvenlik, bilgi güvenliğinin bir parçasıdır ve bilgi sistemlerinin çevrimiçi tehditlere karşı korunmasına odaklanır.

HACKER TÜRLERİ

1. Siyah Şapkalı Hacker (Black Hat Hackers)



Amaçları kötüdür. Bilgisayar sistemlerine izinsiz erişmek, bilgileri çalmak veya zarar vermek gibi kötü niyetli eylemleri gerçekleştirirler

! Saldırganlar, kişisel kazanç veya zarar verme amaçlarıyla hareket edebilirler.

2. Beyaz Şapkalı Hacker “Siber Güvenlik Uzmanları”



Amaçları iyidir. Bilgisayar sistemlerinin güvenliğini test etmek veya zafiyetleri tespit etmek için izin almış güvenlik uzmanlarıdır. Sorunları tespit edip düzeltme konusunda organizasyonlara yardımcı olurlar.

3. Gri Şapkalı Hacker (Gray Hat Hackers)



Amaçları karmaşıktır ve genellikle belirsizdir

İzin almadan bilgisayar sistemlerini test edebilirler, ancak bu işlemi kötü niyetli amaçlarla yapmazlar.

Sistem zafiyetlerini tespit edip sahiplerine bildirirler, ancak izin almadan test yapma amaçlarla yapmazlar.

Genellikle devlette Gri şapkalı hackerlerin yeri yoktur. Ya Beyaz, Ya Siyah..

Sosyal Mühendisler (Social Engineers)

Teknik bilgisayar becerileri yerine insanları manipüle etmeye odaklanan saldırganlardır.

Kişisel verileri, kimlik bilgilerini veya giriş bilgilerini elde etmek için insanların güvenliğini kazanmaya çalışırlar.

Script Kiddies

Genellikle teknik bilgiye sahip olmayan veya sınırlı bilgiye sahip olan amatör saldırganlardır,

Hazır yazılımları veya saldırı araçlarını kullanarak basit saldırılar gerçekleştirirler,

Genellikle popüler olmayan hedeflere yönelirler.

Hacker Grupları (Hacktivist): Belirli bir sosyal veya politik amaç için siber saldırılar gerçekleştiren gruplardır.

Siber Güvenlik Uzmanı Çeşitleri (Red and Blue Team)

1. **Red Team:** İyi niyetli hack yapmayı amaçlarlar.
2. **Blue Team:** Başımıza gelebilecek saldırıları önceden öngörüp sistemi güçlendirirler.

Siber Güvenlikte Bilinmesi Gereken Sistemler



Siber Tehdit (Cyber Threat): Bilgisayar sistemlerine veya dijital ortama zarar verme veya hassas bilgilere erişme amacıyla gerçekleştirilen herhangi bir potansiyel zararlı aktiviteyi ifade eder.

Siber Saldırı (Cyber Attack): Bilgisayar sistemlerine veya dijital altyapılara yönelik saldırılar, siber tehdidin eylemleridir.

Firewall “Güvenlik Duvarı”: Ağ trafiğini izleyen ve izin trafiği geçiren, izin verilmeyen trafiği engelleyen bir güvenlik cihazdır.

Şifreleme (Encryption): Bilgilerin açık metin halinden, anlaşılması zor hale getirerek güvenli bir şekilde saklanması veya iletilmesini sağlayan bir güvenlik yöntemidir.

Kimlik Doğrulama (Authentication): Kullanıcıların veya sistemlerin kimliklerini doğrulama sürecidir. Parola, biyometrik veriler veya iki faktörlü kimlik doğrulama bu kavrama örnek olarak verilebilir. (Parmak izi, yüz okuma vs.)

Yetkilendirme (Authorization): Kimlik doğrulama sonrasında kullanıcılara veya sistemlere belirli kaynaklara erişim izni verilmesi sürecidir.

Güvenlik Güncellemeleri (Security Patch): Yazılım veya işletim sistemlerindeki güvenlik açıklarını kapatmak için yayınlanan düzeltmelerdir. Bu güncellemeler, bilgisayarların güvenliğini arttırmak için önemlidir.

Veri Sızıntısı (Data Breach): Hassas veya kişisel bilgilerin izinsiz bir şekilde sızdırılması veya çalınmasıdır. Bu, kullanıcıların gizliliğinin ihlal edilmesine neden olabilir.

Ağ Güvenliği (Network Security): Bilgisayar ağlarını, ağ trafiğini ve verileri koruma amacıyla alınan önlemleri ifade eder.

Güvenlik Politikası (Security Policy): Bir organizasyonun veya bireyin siber güvenlikle ilgili belirlediği kurallar, prosedürler ve yönergelerdir.

Güvenlik Bilinci (Security Awareness): Kullanıcıların siber güvenlik risklerini ve önlemlerini anlama ve bu konuda eğitilmiş olma durumunu ifade eder.

Ofansif Güvenlik (Hacking): Sistemlerin veya ağların güvenlik önlemlerini aşmayı amaçlayan siber saldırılar veya testler için kullanılan teknikler ve stratejiler.

Defansif Güvenlik (İyileştirme - Güçlendirme): Bilgisayar sistemlerini ev ağları koruma amacıyla güvenlik önlemlerini geliştirme ve iyileştirme süreçleridir.

Sızma Testi (Penetrasyon Testi / Penetration Test): Bilgisayar sistemlerinin veya ağların güvenlik açıklarını ve zafiyetlerini belirlemek için yapılan kontrollü saldırı ve testlerdir.

İç Ağ Sızma Testi (Internal Test): Bir organizasyonun iç ağındaki güvenlik açıklarını ve riskleri değerlendirmek için gerçekleştirilen sızma testleridir. (Sunucu, mobil uygulama vs. karşı yapılan testler)

Dış Ağ Sızma Testi (External Test): Bir organizasyonun dış ağındaki güvenlik açıklarını ve riskleri değerlendirmek için gerçekleştirilen sızma testleridir.

Uygulamaya Yönelik Sızma Testleri (+Mobil): Web uygulamaları veya mobil uygulamalar gibi yazılım uygulamalarının güvenlik açıklarını ve zafiyetlerini tespit etmek için yapılan testlerdir.

Bilgi Toplama Yöntemleri (Pasif / Aktif): Siber saldırganların veya güvenlik uzmanlarının hedef sistem veya organizasyon hakkında bilgi toplama işlemleri. Pasif bilgi toplama, kamu kaynaklarından veri toplamayı içerirken, aktif bilgi toplama, hedef sistemle doğrudan etkileşim gerektirebilir.

Sızma Testi Yöntemleri (Black Box – Gray Box – White Box): Sızma testi sırasında test edilen sistem veya uygulamanın bilgilendirilme düzeyine göre kullanılan yaklaşımlardır.

- **Siyah kutu (Black Box),** Önceden hiçbir bilgiye sahip olunmadan test edilirken, **Beyaz kutu (White Box)** tam bilgiye sahip olunurken test edilir. **Gri kutu (Gray Box)** ise kısmi bilgiye sahip olunarak yapılan bir yaklaşımı ifade eder.

Zafiyet Taraması (Vulnerability Assessment): Bilgisayar sistemlerinde ve ağlarda potansiyel güvenlik zafiyetlerini belirlemek ve sınıflandırmak için kullanılan bir süreçtir.

Exploit: Güvenlik açığı veya zafiyeti kullanarak bir sisteme veya uygulamaya sızmayı veya kontrol etmeyi amaçlayan yazılım veya kod parçasıdır.

Google Hacking (Google Dork): Google gibi arama motorları kullanarak hassas veya gizli bilgilere erişmeye çalışan siber saldırılar veya arama sorgularıdır



Siber terör, siber alanlarda yasa dışı veya tehlikeli eylemleri teşvik eden veya gerçekleştiren bir grup veya bireyler tarafından gerçekleştirilen eylemleri tanımlayan bir terimdir. Siber terör, geleneksel terörizmin dijital ortamda gerçekleşen bir uzantısıdır.

Siber Suç (Cyber Crime), bilgisayarlar, ağlar veya dijital teknoloji kullanarak yasa dışı faaliyetlerde bulunma eylemidir. Bu faaliyetler genellikle finansal kazanç, veri çalma veya zarar verme amaçları taşır.

ZARARLI YAZILIMLAR

Eskiden siber saldırılar sadece büyük kuruluş ve sistemlere yapıldı. Artık kötü niyetli saldırganlar, kişi veya kuruluş ayırt etmiyor. Zararlı yazılımlar, sistemleri parçalamaya, bilgi sızdırmaya, sistemi ele geçirmeye yönelik olabilir. Özünde her zararlı yazılım bir kod parçasıdır. Onları kendi içerisinde kategorize eden şey bulaştıkları sistemde nasıl davranışlar sergiledikleridir. Bu davranışlara göre zararlı yazılım bir Trojan, Worm, Ransomware veya virüs olarak anılabilirler.

1. Virüs

Virüs, bilgisayarlar ve diğer dijital cihazlar için zararlı yazılımlardan biridir. Bir virüs, genellikle zararlı bir program veya kod parçasıdır ve başka bir programın içine veya dosyasına yerleştirilmiştir. Bilgisayarınıza bulaştığında, zararlı kodlar çalışır ve cihazınıza zarar verebilir.

Nasıl Bulaşır?

Virüsler, çeşitli yollarla bulaşabilirler. Bunlar arasında e-posta ekleri, kötü amaçlı web siteleri, yazılım güncellemeleri veya zararlı programların yasadışı kopyaları bulunabilir. Genellikle kullanıcı hatası ile çalışır.

2. Worm (Solucanlar)

Worm (Solucan), bilgisayar ağlarında hızla yayılan ve çoğalan, zararlı bir yazılım türüdür. Bir Worm, bir bilgisayar ağı veya cihaz içindeki diğer cihazlara kendini kopyalayabilen bir zararlı yazılımdır. Worm'ler, kendilerini çoğaltarak hızla yayılır ve genellikle bilgisayar sistemlerine zarar verirler.

Nasıl Bulaşır?

Worm'ler, genellikle bilgisayar ağlarında veya internet üzerindeki güvenlik açıklarını kullanarak yayılırlar. Enfekte (bilgisayar programı) edilmiş bir cihazdan diğer cihazlara otomatik olarak kopyalanabilirler. E-posta eklentileri veya indirilebilir dosyalar gibi bulaştırma yöntemleri de kullanılabilir.

- # Worm'un virüse göre farkı ikisi de zararlı yazılım olmasına rağmen, Worm bir bilgisayara bulaştığı zaman izin istemeden diğer tüm ağ pc'lerine kendini kopyalar.

3. Spyware (Casus Yazılım)

Spyware, kullanıcının bilgisayarını veya diğer cihazlarını izlemek, bilgi toplamak ve genellikle izinsiz olarak kişisel bilgileri çalmak amacıyla tasarlanmış zararlı yazılımlardır.

Spyware, kullanıcının bilgisayar aktivitelerini izleyen ve toplayan bir yazılım türüdür. Bu yazılım, genellikle kullanıcının izni olmadan veya farkında olmadan kurulur.

Spyware, kullanıcının gezdiği web sitelerini, klavye girişlerini, e-posta adreslerini, parolaları ve diğer kişisel bilgileri kaydedebilir.

Nasıl Bulaşır?

Spyware, genellikle ücretsiz yazılımların veya uygulamaların içine gizlenmiş olarak gelir. Kullanıcılar bu yazılımları indirip kurduklarında spyware de sistemlerine bulaşır.

Bazı web siteleri, zararlı pop-up aracılığıyla da spyware bulaştırabilir.

- # Casus yazılıma (spyware) örnek olarak “keylogger *tuş kaydediciler*” örneğini vermek mümkündür.

4. Adware (Reklam Yazılımı)

Adware, ifadesinin kısaltmasıdır ve reklam destekli yazılım anlamına gelir. Temel amacı, kullanıcının internet tarayıcısına veya bilgisayarına istenmeyen reklamlar eklemek ve bu reklamlar aracılığıyla gelir elde etmektir.

Adware genellikle ücretsiz yazılımların veya uygulamaların bir parçası olarak bilgisayara bulaşır.

Nasıl Bulaşır?

Adware, genellikle ücretsiz yazılımların veya uygulamaların içine gizlenmiş olarak gelir. Kullanıcılar bu yazılımları indirip kurduğunda Adware de sisteme bulaşır.

Bazı web siteleri, zararlı pop-up reklamlar aracılığıyla da Adware bulaştırabilir.

5. Trojan (Truva Atı)

Trojan (Truva Atı), görünüşte zararsız veya yararlı bir program veya dosya gibi davranarak, kullanıcının bilgisayarına kötü amaçlı yazılım bulaştırmak için tasarlanmış bir tür zararlı yazılımdır.

Görünüşte zararsız bir program veya dosya gibi davranır, bu nedenle kullanıcılar tarafından kolayca kurulabilir.

Amaçları, bilgisayara kötü amaçlı yazılım, casus yazılım veya diğer zararlı işlevleri yüklemektir.

Nasıl Bulaşır?

Trojanlar, genellikle bilgisayar kullanıcılarına güvenilir ve çekici görünen e-posta ekleri, indirilebilir dosyalar veya uygulamalar aracılığıyla bulaştırılır.

Kullanıcılar, bu dosyaları veya uygulamaları indirip açtıklarında Trojan bilgisayarlarına bulaşır.

- # Genellikle JPG veya PDF dosyası olarak karşımıza çıkar, çift tıklanarak açılınca virüs bulaşmış olur.
- # Bu yazılım ile karşı tarafın kamerası, mikrofonu, dosyalarına görüntüleme gibi birçok içeriğine erişim sağlanabilir.

6. Botnets (Zombi)

Bot terimi robotun kısaltmasıdır. Amacı, bilgisayarınızı bir bot'a (zombi olarak da bilinir) çevirebilen kötü amaçlı yazılımları dağıtmaktır. Böyle bir durumda bilgisayarınızı, sizin haberiniz olmadan internet üzerinden otomatik görevleri gerçekleştirebilir.

Nasıl Bulaşır?

Botnetler, bilgisayarlara veya cihazlara bulaşmak için genellikle kötü amaçlı e-posta ekleri, bulaşmış web siteleri, güvensiz uygulamalar veya diğer kötü niyetli yazılımlar aracılığıyla yayılırlar. Kullanıcılar, bu bulaşmış dosyaları veya bağlantıları açtıklarında botnet bilgisayarlarına bulaşabilir.

7. Ransomware (Fidye Yazılımı)

Ransomware, kötü amaçlı bir yazılım türüdür ve adını rehine verileri fidye karşılığında serbest bırakma eyleminden alır.

Ransomware, dosyaları veya bilgisayarın tamamını şifreleyerek kullanıcının erişimini engeller.

Nasıl Bulaşır?

Ransomware, genellikle sahte e-posta ekleri, kötü amaçlı web siteleri, güvensiz indirme kaynakları veya açıkları kullanarak bilgisayarlara bulaşır.

Kullanıcılar, kötü amaçlı dosyaları veya bağlantıları açtıklarında ransomware bulaşabilir.

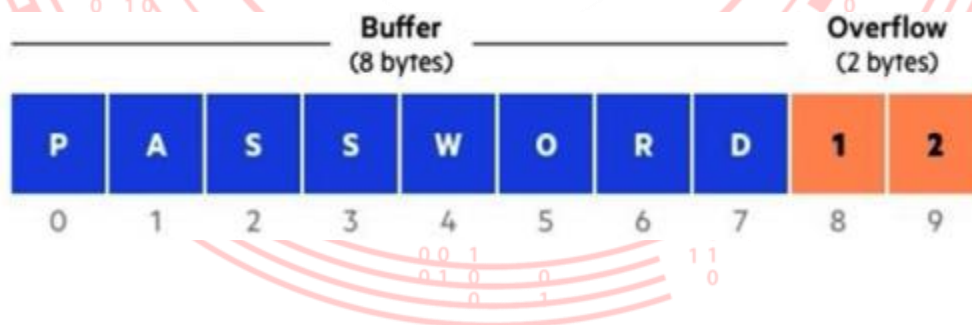
En büyük kötü amaçlı hack yöntemidir.

SALDIRI TÜRLERİ

Buffer Overflow

Bir programın bellek alanının sınırlarının dışına çıkılarak kötü amaçlı kodların çalıştırılmasına izin veren bir güvenlik açığıdır. Tamamen teknik bir saldırı türüdür.

Örnek: Morris Worm, buffer overflow açığı kullanılarak ilk büyük çaplı internet saldırısını gerçekleştirmiştir.



Cross-Site Request Forgery "CSRF"

Saldırganların kullanıcıların hesaplarını izinsiz olarak farklı bir web sitesi üzerinden işlem yapmaya zorladığı bir saldırı türüdür.

Örnek: Bir saldırgan, kullanıcının banka hesabından para transferi yapmasını isteyen sahte bir web sayfası oluşturabilir.

Croos-Site Scripting (XSS)

Saldırganların web sitelerine zararlı kodlar ekleyerek kullanıcıların tarayıcılarında çalışmasını sağladığı bir saldırı türüdür.

Örnek: Bir saldırgan, kullanıcılara zararlı bir JavaScript kodu içeren sahte bir e-posta gönderebilir.

Broken Access Control (Yetkisiz Erişim)

Kullanıcıların izin verilmeyen kaynaklara veya işlemlere erişim sağlamasına izin veren bir güvenlik açığıdır.

Örnek: Bir kullanıcının hesap ayarlarını değiştirmesi gereken bir işlevin, yetkisiz erişime açık olmasıdır.

Zero-Day Exploits (0 Days)

Yazılım veya sistem güvenlik açıklarının keşfedildiği henüz üretici tarafından ve düzeltilmediği durumlar.

Örnek: Saldırganlar, henüz açığı kapatılmamış bir yazılık veya işletim sistemi güvenlik açığından faydalanabilirler

- # Site veya uygulama sahibinin piyasaya sürdüğünden itibaren henüz keşfedilmeyen sistemdeki güvenlik açığıdır.

Port Configuration Hataları (Port Ayarları Hatası)

Ağ cihazlarının yanlış yapılandırılması sonucu ağ güvenliğinin tehlikeye girmesidir.

Örnek: Açık bir ağ bağlantısı, yetkisiz erişimlere yol açabilir.

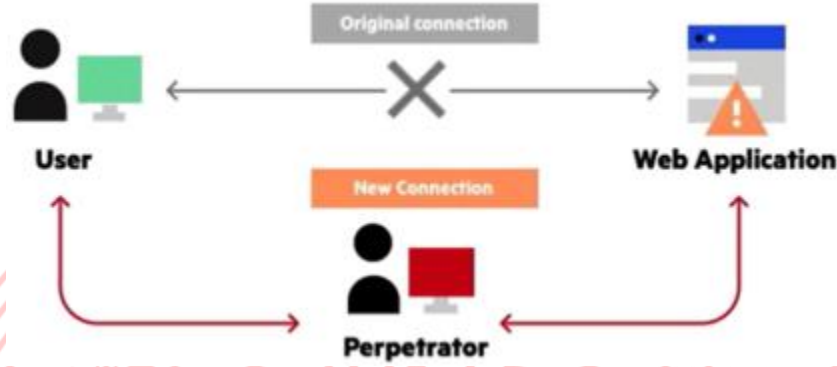
Rat (Remote Access Trojan) “Uzaktan Erişim Aracı”

Saldırganların bir bilgisayar sistemine uzaktan erişim sağlamak amacıyla kullanılan Truva atıdır.

Man-In-The-Middle (MITM) Saldırıları (Ortakdaki Adam Saldırıları)

Saldırganların iki iletişim tarafın arasına girerek iletileri izlemesine veya manipüle etmesine olana tanıyan saldırı türüdür.

Örnek: Bir kişi, halka açık bir Wi-Fi ağı üzerinden verileri izleyebilir veya değiştirebilir.

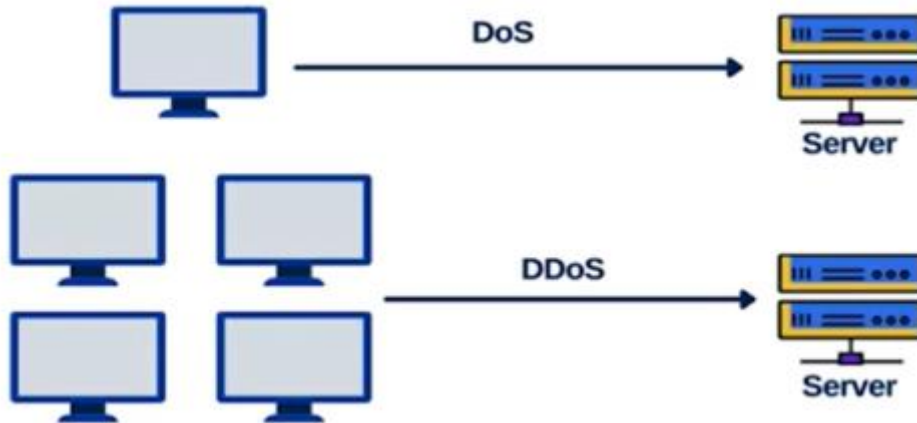


Bu saldırıyı yapmak kolaydır.

Denial-Of-Service (DOS) Saldırıları

Hedeflenen sistem veya ağı yoğun talep gönderilerek hizmetin kesilmesine neden olan saldırılardır.

Örnek: SYN Flood saldırısı, bir sunucunun hizmet veremeyecek kadar çok bağlantı isteği aldığı bir tür DOS saldırısıdır.



1 IP'den gelen devamlı istekleri Firewall (güvenlik duvarı) bunu göz ardı etmeye ve engellemeye çalışır fakat her zaman başarılı olmamaktadır.

SOSYAL MÜHENDİSLİK VE DALLARI

Sosyal Mühendislik, insanları manipüle ederek, insanların yapabileceği hataları göz önüne alarak bilgi edinme durumudur. (Bilgiyi çalma durumu)

1. Phishing

Saldırganlar, sahte e-postalar, web siteleri veya mesajlar kullanarak kullanıcıları kişisel bilgileri ifşa etmeye veya kötü amaçlı yazılımları indirmeye ikna etmeye çalışır.

Örnek: Kullanıcılara sahte bir banka e-postası göndererek, hesap paylaşımlarını isteyen bir phishing saldırısı.

2. Spear Phishing (Tek kişi veya gruba yönelik saldırı)

Phishing'in özelleştirilmiş bir türüdür; saldırganlar belirli kişileri hedef alarak daha inandırıcı mesajlar gönderir.

Örnek: CEO'yu taklit eden bir e-posta göndererek finans müdürünü para transferi yapmaya ikna etmeye çalışan bir spearphishing saldırısı.

3. Shoulder Surfing (Omuz Sörfü)

Saldırganlar, birisinin bilgisayar ekranını veya klavyesini izleyerek hassas bilgilere erişim sağlamaya çalışır. Birebir fiziksel olarak hassas bilgileri almaya denir.

Örnek: Halka açık bir Wi-Fi ağına bağlıyken, yan masada oturan kişinin şifresini izlemek.

4. Dumpster Diving (Çöp Karıştırma)

Saldırganlar, kurumların veya bireylerin çöplerini karıştırarak hassas bilgilere ulaşmaya çalışır.

Örnek: İşyerinin atıklarını karıştırarak, bilgisayarların atılan belgeleri üzerinden önemli bilgilere erişmeye çalışan bir saldırgan.

5. Role Playing (Rol Yapma)

Saldırganlar, güven kazanmak veya inandırıcılıklarını artırmak için sahte bir rol üstlenirler.

Örnek: Teknik destek uzmanı gibi davranarak, kullanıcılardan uzaktan bilgisayarlarına erişim izni talep eden bir role playing saldırısı.

6. Pretexting (Bahane Uydurma)

Saldırganlar, inandırıcı bir bahane uydurarak kişilerden bilgi veya yardım talep ederler.

Örnek: Sahte bir müşteri temsilcisi gibi davranarak, bir kişinin banka hesabı bilgilerini çalmaya çalışan bir pretexting saldırısı.

7. Baiting (Yemleme)

Saldırganlar, kullanıcıları kötü amaçlı yazılım içeren çekici dosyalar veya cihazlarla cezbetmeye çalışır.

Örnek: USB belleği park halindeki bir araçta bırakarak, bulan kişinin bilgisayarına kötü amaçlı yazılım bulaştırmaya çalışan bir baiting saldırısı.

8. Tailgating (Kuyrukta Sürünme)

Saldırganlar, birisinin yetkili bir alana girmesine izin vermesini bekleyerek güvenlik önlemlerini atlarlar.

Örnek: Bir işyerinin girişinde başkasının arkasından girerek içeri sızma girişimi.

9. Quid Pro Quo (Karşılık Bekleme)

Saldırganlar, kullanıcıları bir hizmet sunmaya veya yardım etmeye söz vererek bilgi elde etmeye çalışır.

Örnek: Sahte bir teknik destek uzmanı olarak arayan saldırgan, bilgisayarın şifresini öğrenmek için yardım isteyebilir.

10. Impersonation (Kimlik Taklidi)

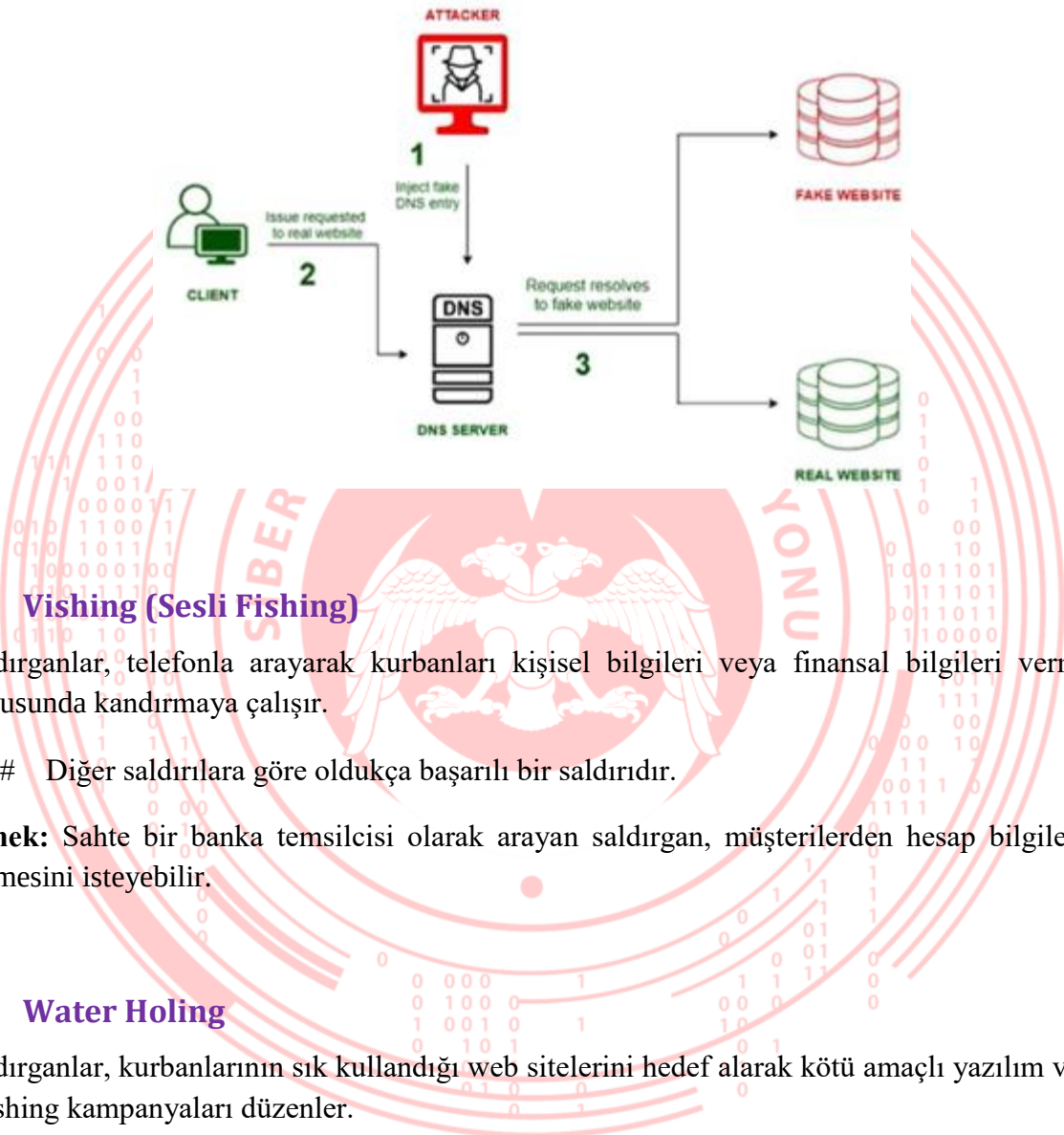
Saldırganlar, başkasının kimliğini taklit ederek güven kazanmaya çalışır.

Örnek: Birinin telefon numarasını taklit ederek, sahte bir kimlikle banka işlemi yapmaya çalışan bir impersonation saldırısı.

11. Farming (Çiftçilik)

Saldırganlar, kullanıcıları sahte web sitelerine yönlendirerek kişisel bilgilerini toplamaya çalışır.

Örnek: Kullanıcıları sahte bir banka web sitesine yönlendiren ve giriş bilgilerini çalmaya çalışan bir pharming saldırısı.



12. Vishing (Sesli Fishing)

Saldırganlar, telefonla arayarak kurbanları kişisel bilgileri veya finansal bilgileri vermek konusunda kandırmaya çalışır.

Diğer saldırılara göre oldukça başarılı bir saldırıdır.

Örnek: Sahte bir banka temsilcisi olarak arayan saldırgan, müşterilerden hesap bilgilerini vermesini isteyebilir.

13. Water Holing

Saldırganlar, kurbanlarının sık kullandığı web sitelerini hedef alarak kötü amaçlı yazılım veya phishing kampanyaları düzenler.

Örnek: Bir sektörün ilgi çekici bir web sitesini hackleyen ve ziyaretçilerini kötü amaçlı yazılım ile enfekte¹ etmeye çalışan bir water holing saldırısı.

¹ Bilgisayar virüsü

HACKER METODOLOJİSİ



! Siber güvenlik uzmanı (Beyaz şapkalı hacker) bir bireyin iş akışı yukardaki gibi olmalıdır.

SİBER GÜVENLİK ÖNERİLERİ

- Çift Faktörlü Kimlik Doğrulama Kullanın
- Şifre Yöneticisi Kullanın
- Güçlü ve Benzersiz Şifreler Kullanın
- Kişisel Bilgilerinizi Paylaşmaktan Kaçın
- Bilinmeyen E-postalara ve Bağlantılara Dikkat Edin
- Yazılım Güncellemelerini İhmal Etmeyin
- Sosyal Mühendislik Saldırılarına Karşı Bilinçli Olun
- Bilinmeyen USB Cihazlarından Kaçının (!Keylogger!)
- Ağ Güvenliği İçin Firewall Kullanın
- Bilgilerinizi Düzenli Olarak Yedekleyin
- Önemli Evraklarınızı İmha Etmeden Çöpe Atmayın



DONANIM ALTYAPISI GÜVENLİĞİ

Donanım güvenliği, bilgisayar sistemlerinin ve cihazlarının donanım bileşenlerinin, yazılım saldırılarına veya fiziksel tehditlere karşı korunmasını sağlayan bir bilgi güvenliği dalıdır. Temel amaç, donanımın gizlilik, bütünlük ve erişilebilirlik açısından güvende olmasını sağlamaktır.

Donanım Güvenliği

Güvenlik Açıkları		
Donanım	Yazılım	Veri
Kasıtsız Zarar - Yiyecek-İçecek - Hayvanlar - Toz - Yıldırım - Kaba kullanım	Silinme - Kasıtlı - Kasıtsız	Gizliliğin ihlali - Dinlenme (dinleyiciler, alıcılar) - Bilgi Sızdırma(insanlar yoluyla) - Engelleme - Silme - Ulaşılamaz, ya da kullanılamaz hale getirme - Bütünlüğün bozulması - Veri değişikliği - Sahte Veri
Kasıtlı Zarar - Hırsızlık - Fiziksel Zararlar (Kırma, Bozma, Parçalama)	Değiştirilme - Truva Atları - Virüsler - Arka kapılar - Bilgi sızdırma	
	Hırsızlık - Lisansız kullanım - İzinsiz kopyalama	

Altyapı Güvenliği

Alt yapı güvenliği, bir organizasyonun bilgisayar ağlarının, sunucularının, yönlendiricilerinin ve diğer altyapı bileşenlerinin güvende olduğundan emin olma sürecini ifade eder. Bu, ağ erişiminin sınırlanması, güçlü kimlik doğrulama ve veri iletişiminin şifrelenmesi gibi önlemleri içerir.

Örnek: Bir şirketin ağının güvenliği için güvenlik duvarı (firewall) kullanmak, yetkilendirilmemiş erişimi engellemek için ağ anahtarlarını ve yönlendiricilerini yapılandırmak.

İşletim Sistemi Güvenliği

	windows	android	MacOS/ iOS	linux	pardus
Logo					
Geliştirici	Microsoft	Google	Apple	Linux Vakfı	Tübitak
Lisans Durumu	Ücretli Lisanslı	Ücretsiz Lisanslı	Ücretli Lisanslı	Ücretsiz, Genel Kому Lisansı	Ücretsiz
Kullanılan Cihazlar	Bilgisayarda Windows, Telefon ve Tabletlerde Windows Phone	Tablet ve Telefonlarda	Mac bilgisayarlarında MacOS, Iphone ve Ipad lerde iOS	Bilgisayarda	Bilgisayarda
Kaynak Kodu	Kapalı Kaynak	Açık Kaynak	Kapalı Kaynak	Açık Kaynak	Açık Kaynak
Güvenlik Düzeyi	Orta	Orta	Yüksek	Yüksek	Yüksek

İşletim sistemi güvenliği, bilgisayar veya sunucu üzerinde çalışan işletim sistemlerinin güvende olduğundan emin olma sürecini ifade eder. Bu, güncellemelerin düzenli olarak uygulanması, gereksiz hizmetlerin kapatılması ve güçlü parola politikalarının uygulanması gibi önlemleri içerir.

Uygulama Sunucusu Güvenliği

Uygulama sunucusu güvenliği, web sunucuları, veritabanı sunucuları veya diğer uygulama sunucularının güvende olduğundan emin olma sürecini ifade eder. Bu, güvenlik yamalarının uygulanması, gereksiz hizmetlerin kapatılması ve sıkı erişim kontrolünün sağlanması gibi önlemleri içerir.

VERİ SIZINTISI (DATA BREACH)

Veri sızıntısı, hassas veya kişisel bilgilerin yetkisiz erişim veya ifşa sonucu sızdırıldığı bir olaydır. Veri sızıntıları, organizasyonların veya bireylerin güvenliğini ve gizliliğini tehlikeye atabilir.

- ! Veri sızıntılarının büyüklüğü önemli değildir. Veri tabanından bir uygulamanın sadece kullanıcıların e-postalarının bile alınması çok büyük sonuçlar doğuracaktır.

Bu tür bir sızıntı, kişisel bilgilerin, finansal bilgilerin, sağlık kayıtlarının veya diğer hassas verilerin yetkisiz kişilerin eline geçmesi durumunda meydana gelir.

- a. İstem Dışı - Kazara Veri Sızıntısı
- b. İstemli - Kasıtlı Veri Sızıntısı

A. İstem Dışı - Kazara Veri Sızıntısı

Kazara veri sızıntısı, verinin yetkisiz bir şekilde ifşa edilmesine veya kaybedilmesine neden olan istem dışı olayları ifade eder.

- # Bu tür sızıntılar genellikle insan hataları, teknik arızalar veya kötü niyetli olmayan ihlaller sonucu meydana gelir

B. İstemli - Kasıtlı Veri Sızıntısı

İstem dışı kasıtlı veri sızıntısı, verinin kötü niyetli bir eylem sonucu ifşa edilmesine neden olan bir durumu ifade eder. Bu tür sızıntılar, bilinçli bir şekilde veri çalmayı veya ifşa etmeyi amaçlayan kişiler veya gruplar tarafından gerçekleştirilir. Saldırganlar, hassas verilere erişmek veya bu verileri kötü amaçlı olarak kullanmak için çeşitli yöntemler kullanabilirler.

- # Bir şirket çalışanının çalıştığı şirketteki gizli bilgileri dışarıya yansıtması örneğini verebiliriz.

Veri Sızıntısını Önleme

Veri sızıntısını önleme, hassas veya kişisel bilgilerin yetkisiz erişim veya ifşa sonucu sızdırılmasını engellemeyi amaçlar. Bu, organizasyonların veya bireylerin gizliliğini ve verilerinin güvenliğini korumak için alınan önlemleri içerir.

Veri Sızıntısını Önlemenin Temel Prensipleri ve Önerileri:

- Eğitim ve Farkındalık
- Güçlü Kimlik Doğrulama
- Veri Şifreleme
- Güncel Yazılımlar ve Yama Yüklemleri
- Siber Güvenlik Yazılımı Kullanımı
- Veri Erişim Kontrolleri
- Veri Yedeklemeleri
- Ağ Güvenliği



Şirketler, Darkweb'de verilerinin gizliliğinin ihlal edilmesine nasıl tepki veriyor?

Kaspersky 258 şirketi, çalınmış kimlik bilgileri, veri sızıntısı, ilk erişim izni gibi verilerinin Darkweb'de kullanımıyla ilgili bilgilendirildi





PAROLA/ŞİFRE NEDİR?

Parola bir kullanıcının belirli bir hesaba veya sistemde kimliğini doğrulamak için kullandığı gizli karakter dizisidir.

Parolalar, kullanıcı adı ile birlikte kullanılarak hesaba erişim sağlar. Genellikle harf, rakam ve sembollerin kombinasyonlarından² oluşurlar ve gizliliklerinin korunması önemlidir.

Örnek: "P@sswOrd123" veya "MySecretCode2023!"

Parola ve Şifre Arasındaki Fark

Parola ve şifre her ne kadar da aynı terimlermiş gibi görünse de aslında siber güvenlik uzmanı olarak bir kariyer düşüncemiz var ise temel farkı öğrenmemiz gerekmektedir. Herhangi bir uygulama veya web sitesine giriş için e-postadan sonra girilen bilgiye **“Parola”** bu parolanın da veri tabanında tutulmasına **“Şifre”** denir. Parolalar veri tabanında direk yazmaz, her harf veya karaktere denk gelen sayı/semboller vardır. Örneğin; bir kullanıcının parolası “Siber{_gynlk” ise bu parolaya denk gelen “45+*/shnv=^>” şifresi yazar. Her veri tabanı şifrelemesi şirkete özgü olduğundan bunun mantığını anlamak oldukça zordur.

Parola Güvenliği

Parola güvenliği, kullanıcıların parolalarını güvende tutma ve kötü niyetli kişilerin hesaplara yetkisiz erişimini engelleme pratiğini ifade eder.

Güçlü parola güvenliği, zorlukla tahmin edilebilecek karmaşık parolaların kullanılmasını içerir.

Ayrıca, parolaların düzenli değiştirilmesi ve güvende tutulması da önemlidir.

Güçlü bir parola, büyük harf, küçük harf, rakam ve sembollerin karışımını içerir ve kişisel bilgilere dayanmaz.

Parola Saldırıları Nedir?

Parola saldırıları, kötü niyetli kişilerin veya yazılımın bir hesaba veya sistemdeki parolayı tahmin etmeye veya kırarak yetkisiz erişim elde etmeye çalıştığı siber saldırı türleridir.

Aşağıda bazı parola saldırısı türleri ve örnekleri verilmiştir:

² Birleşim

1. Brute Force Saldırısı:

Örnek: "aaaaa", "aaaab", "aaaac", ... # Parolaların tek tek denenmesi

2. Dictionary (Sözlük) Saldırısı:

Örnek: "password", "admin", "123456"

Bize özel oluşturulan bilgilerin şifre olarak denenmesi (Ad, Anne Adı, Doğum Tarihi..)

3. Phishing Saldırısı:

Örnek: Kullanıcıların banka hesap bilgilerini girmelerini isteyen sahte bir banka web sitesi.

4. Rainbow Table Saldırısı:

Örnek: Önceden hesaplanmış MD5 veya SHA-1 karma değerlerini içeren bir veri tabanı.



HER UYGULAMA VEYA WEB SİTESİNİN ŞİFRESİ BİRBİRİNDEN FARKLI OLMALIDIR!

KURUMSAL AĞ GÜVENLİĞİ (CORPORATE NETWORK)

Kurumsal ağ, bir organizasyonun veya işletmenin içindeki bilgisayarların ve diğer cihazların birbiriyle iletişim kurduğu, bilgi ve veri paylaştığı özel bir iletişim altyapısını ifade eder.

Kurumsal, ağlar, çalışanların işbirliği yapması, veri ve dosya paylaşımı, e-posta iletişimi gibi günlük iş süreçlerini desteklemek için kullanılır.

Kurumsal ağ güvenliği, bir organizasyonun iç ağına yönelik tehditlere karşı koruma sağlama pratiğini ifade eder.

Bu, ağa yetkisiz erişimden, veri sızıntısından veya diğer siber saldırılardan korunmayı içerir. Ayrıca, çalışanların ve organizasyonun veri güvenliği politikalarına uygun davranmalarını teşvik etmek de önemlidir.

KABLOSUZ AĞ GÜVENLİĞİ (WIRELESS NETWORK)

Kablosuz ağ, bilgisayarlar, telefonlar, tabletler ve diğer cihazların kablosuz iletişim teknolojileri aracılığıyla birbirleriyle veya internetle iletişim kurmasını sağlayan bir ağ türüdür. Bu iletişim Wi-Fi, Bluetooth veya diğer kablosuz iletişim protokollerini kullanarak gerçekleşir.

Kablosuz ağlar, kablolu ağlara göre daha esneklik ve mobilite⁴ sağlar.

Kablosuz ağ güvenliği, kablosuz ağları yetkisiz erişim ve siber saldırılardan koruma pratiğini ifade eder.

Kablosuz ağlar, yaygın olarak kullanıldıkları için güvenlikleri önemlidir çünkü kötü niyetli kişiler veya cihazlar bu ağlara kolayca erişebilirler.

Kablosuz ağ güvenliği, ağın gizliliğini, bütünlüğünü ve erişilebilirliğini korumayı amaçlar.

⁴ Bir yerden başka bir yere olan hareketi ya da bir durumdan başka bir duruma geçişi



OWASP (WEB UYGULAMA GÜVENLİĞİ)

OWASP, "Open Web Application Security Project" kelimelerinin baş harflerinden oluşan bir kısaltmadır ve açık kaynaklı bir topluluk tarafından yönetilen bir projeyi ifade eder.

OWASP, yazılım ve web uygulamalarının güvenliğini artırmayı amaçlayan bir dizi kaynak ve rehber sunar. OWASP, web uygulama güvenliği alanında dünya genelinde tanınan bir otoritedir.

- # Her 3 yılda bir yaptığı anketlerle web sitelerinin en çok hacklenmesinin 10 sebebini açıklıyor ve bu sebeplerin önüne geçmek için eğitimler yayınlar.

OWASP, geliştiricilere, güvenlik profesyonellerine ve organizasyonlara aşağıdaki konularda yardımcı olur:

- Güvenli Uygulama Geliştirme
- Siber Tehditlere Karşı Koyma
- Eğitim ve Bilinçlendirme

GÜVENLİK AMAÇLI KOD ANALİZLERİ

Güvenlik Amaçlı Kod

Güvenlik amaçlı kod, yazılım geliştirme sürecinde güvenlik açıklarını tespit etmek ve önlemek amacıyla eklenen programlama kodlarını ifade eder. Bu kodlar, yazılımın siber saldırılara ve güvenlik ihlallerine karşı daha dayanıklı olmasını sağlar.

Güvenlik amaçlı kodlama uygulamaları, yazılımın zayıf noktalarını tespit eder ve düzeltilmesine yardımcı olur.

Statik Kod Analizi: Bu, yazılımın kaynak kodunun incelemesiyle gerçekleştirilen bir güvenlik testidir. Yazılımın piyasaya sürülmeden önce kodlara bakılarak yapıldığı testtir.

Bu analiz, kodun yazılım geliştirme aşamasında yapıldığı için daha erken tespit ve düzeltme imkânı sağlar.

- # Otomatik analiz araçları kullanılarak kod üzerinde potansiyel güvenlik açıkları ve hatalar tespit edilir.

Dinamik Kod Analizi: Bu, yazılımın çalışma zamanında test edilmesini içerir.

Bu analiz, uygulamanın gerçek dünya koşullarında nasıl davrandığını değerlendirmeye yardımcı olur.

Uygulama çalışırken güvenlik açıkları ve zayıf noktalar test edilir.

GÜVENLİ YAZILIM GELİŞTİRME (SSDLC)

Güvenli Yazılım Geliştirme Yaşam Döngüsü (Software Security Development Life Cycle - SSDLC), yazılım geliştirme sürecinin her aşamasında güvenlik önlemlerinin ve uygulamalarının bütünleşmesini sağlayan bir yöntem veya süreçtir.

SSDLC, yazılımın tasarımından başlayarak kodlama, test, yayınlama ve bakım aşamalarını içerir ve güvenlik açıklarının erken tespiti ve düzeltilmesini hedefler.



Şekil 1 Güvenli Yazılım Geliştirme Yaşam Döngüsü

SSDLC (Planlama) Ne İşe Yarar?

Güvenlik açıklarının erken tespiti: Yazılım geliştirme sürecinin her aşamasında güvenlik değerlendirmeleri yaparak potansiyel tehditleri erken tespit eder.

Yazılım güvenliği kültürünü teşvik eder: Geliştiricilerin ve diğer ekip üyelerinin yazılım güvenliği konusunda bilinçlenmelerine ve eğitilmelerine yardımcı olur.

SİBER GÜVENLİK RİSK YÖNETİMİ

Siber Riskler

Siber riskler, bilgi teknolojileri ve internetin kullanımıyla ilişkilendirilen potansiyel tehlikeleri ifade eder.

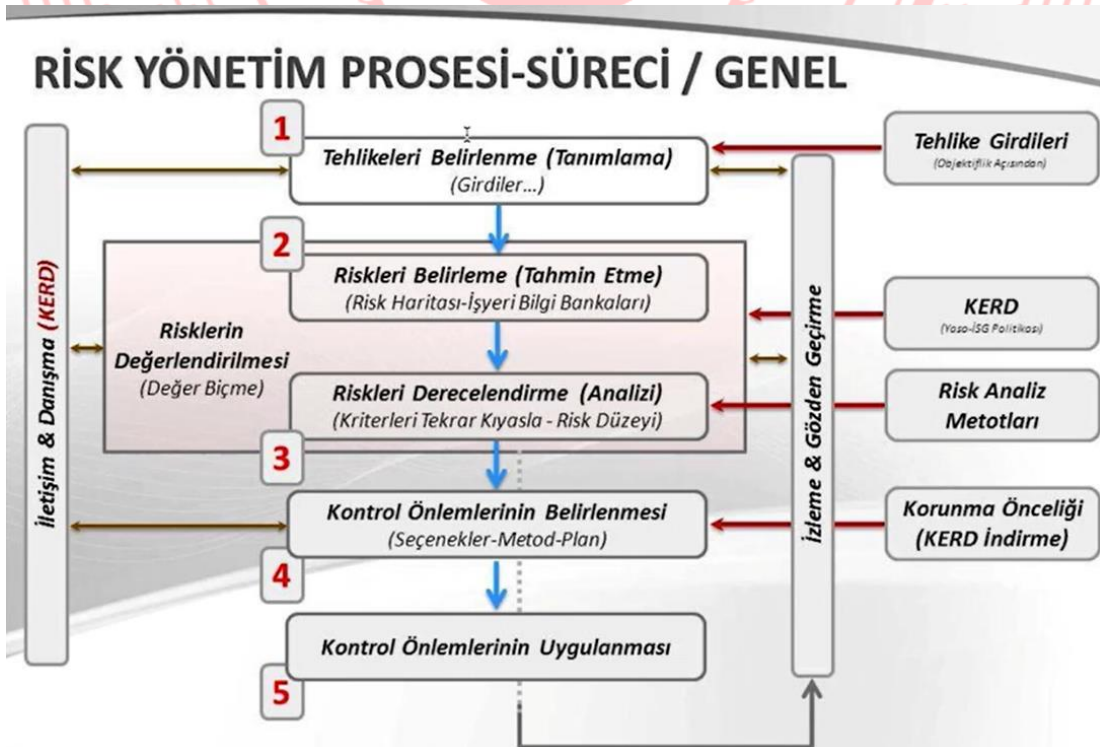
İşte siber risklerin bazıları:

1. **Veri Sızıntısı** Örnek: Bir kuruluşun müşteri bilgilerinin sızdırılması.
2. **Malware (Kötü Amaçlı Yazılım)** Örnek: Bir ransomware saldırısı.
3. **Phishing** Örnek: Bir çalışanın sahte bir e-postaya tıklaması.
4. **DDOS Saldırısı** Örnek: Bir e-ticaret sitesinin saldırıya uğraması ve erişilemez hale gelmesi.
5. **İç Tehditler** Örnek: İçeriden bir saldırganın gizli bilgilere erişimi.

Risk yönetimi, organizasyonların karşılaştığı riskleri tanımlama, analiz etme, değerlendirme, azaltma veya kabul etme sürecini ifade eder.

Siber risk yönetimi, organizasyonların siber tehditleri ve riskleri belirlemesine, bu riskleri azaltmasına veya kabul etmesine ve uygun güvenlik önlemlerini uygulamasına yardımcı olur.

Siber Risk Yönetimi Tablosu



Siber risk yönetimi, tüm organizasyonlar için önemlidir, özellikle büyük kuruluşlar, finans kurumları ve sağlık sektörü gibi hassas verilere sahip olanlar için daha kritiktir.

Bilgi güvenliği profesyonelleri, risk yöneticileri ve üst düzey yöneticiler siber risk yönetimi süreçlerini uygular.

KVKK (Kişisel Verileri Koruma Kanunu) Nedir?



Türkiye'de kişisel verilerin korunmasını düzenleyen bu kanun, siber güvenlikle de ilgilidir.

Organizasyonlar, kişisel verilerin güvenliğini sağlamak için çeşitli siber güvenlik önlemleri almak zorundadır.



Şekil 2 KVKK Bilgi Güvenliği

SİBER GÜVENLİK SERTİFİKALARI

Offensive Security, siber güvenlik alanında eğitim ve sertifikasyon programları sunan bir şirkettir. Offensive Security'nin sunduğu bazı önemli sertifikalar şunlardır:

OSCP (Offensive Security Certified Professional): OSCP, Offensive Security'nin en popüler ve tanınmış sertifikasıdır.

Kali Linux'da buna dâhildir

Alması en zor sertifikadır

OSCE (Offensive Security Certified Expert): OSCE, bilgisayar güvenliği uzmanlarının bilgisayar sistemlerine sızma testleri yapma yeteneklerini daha derinlemesine göstermelerine olanak tanır.

OSWE (Offensive Security Web Expert): OSWE sertifikası, web uygulamalarının güvenliğini test etme ve web uygulama sızma testleri yapma yeteneklerini ölçer.

OSWP (Offensive Security Wireless Professional): OSWP sertifikası, kablosuz ağ güvenliği ile ilgilenen kişilere yöneliktir.

CISSP (Certified Information Systems Security Professional)

CISSP, bilgi sistemleri güvenliği profesyonelleri için dünya genelinde tanınmış bir sertifikadır.

Bilgi güvenliği yönetimi, risk yönetimi, güvenlik mimarisi ve diğer konularda uzmanlaşmış profesyonellere yöneliktir.



Certified Information
Systems Security Professional



CEH (Certified Ethical Hacker)

CEH sertifikası, etik hackerlar için tasarlanmıştır. Bu sertifika, ağları güvenlik açıklarını tespit etmek ve kapatmak için yetenekli hale getirmek isteyen profesyoneller için geçerlidir. Test soruları çözülerek alınır.

Comptia Security+



CompTIA Security+, temel siber güvenlik kavramlarını ve uygulamalarını kapsayan bir sertifikadır.

Bu sertifika, siber güvenlik kariyerine yeni başlayanlar veya temel bilgiye sahip olanlar için uygundur.

- ! Sertifikaları almak için oturup bir sistemi hacklemek gerekmektedir. Eğer hacklenemezse sertifika alınamamaktadır.
- ! Sertifikaları almak ücret açısından baya maliyetlidir

Ccna Cyberops (Cisco Certified Network Associate - Cyberops)



CCNA CyberOps, ağ güvenliği ve siber güvenlik alanlarında uzmanlaşmak isteyen ağ profesyonelleri için Cisco tarafından sunulan bir sertifikadır.

Certified Cloud Security Professional (CCSP)



CCSP, bulut bilişim güvenliği uzmanları için tasarlanmış bir sertifikadır.

Bulut ortamında güvenliği sağlamak için gereken bilgi ve becerileri ölçer.

SİBER GÜVENLİK ALANINDA POZİSYONLAR VE ÜNVANLAR

Bilgi Güvenliği Uzmanı (Information Security Specialist):

Güvenlik duvarlarını yapılandırır, güvenlik yazılımını güncellerler.

Ağ Güvenliği Mühendisi (Network Security Engineer):

Ağ içi iletişimin güvenli bir şekilde gerçekleştiğinden emin olurlar.

DOS saldırılarına karşı savunma önlemleri geliştirirler.

Sızma Testi Uzmanı (Penetration Tester):

Örneğin, organizasyonun web uygulamasında açıklar bularak güvenlik zafiyetlerini ortaya çıkarırlar.

Güvenlik Analisti (Security Analyst):

Örneğin, bir kullanıcının hesabının ele geçirilmesini tespit edip bu olayı incelerler.

Kimlik ve Erişim Yönetimi Uzmanı (Identity and Access Management Specialist):

Örneğin, bir işletme için tek oturum açma (Single Sign-On) sistemini uygularlar.

Veri Güvenliği Analisti (Data Security Analyst):

Bir sağlık kurumu için hastaların tıbbi kayıtlarının güvenliğini sağlarlar.

Güvenlik Mimar (Security Architect):

Bulut tabanlı bir hizmetin güvenliğini sağlamak için mimari planlar hazırlarlar.

! Olay Yanıtı Uzmanı (Incident Response Specialist):

Bir fidye yazılım saldırısına karşı hızlı bir kurtarma planı oluştururlar.

Uygulama Güvenliği Uzmanı (Application Security Specialist):

Bir e-ticaret sitesinin web uygulamasının güvenliğini denetlerler.

Eğitim ve Farkındalık Uzmanı (Training and Awareness Specialist):

Sahte e-posta kampanyaları düzenleyerek çalışanların dikkatini çekerler.

Yazılım Geliştirme Güvenliği Danışmanı (Secure Development Consultant):

Yazılım geliştiricilere güvenlik açıklarını düzeltme konusunda rehberlik ederler.

Güvenlik Denetçisi (Security Auditor):

Bir finans kuruluşunun güvenlik prosedürlerini denetlerler.

Mobil Uygulama Güvenliği Uzmanı (Mobile Application Security Specialist):

Bir bankanın mobil bankacılık uygulamasının güvenliğini test ederler.

Güvenlik Ekip Lideri (Security Team Leader):

Bir büyük organizasyonun güvenlik ekibinin liderliğini yaparlar.

Veri Gizliliği Danışmanı (Data Privacy Consultant):

GDPR gibi düzenlemelere uyum sağlamak için bir şirkete danışmanlık yaparlar.

Endüstriyel Kontrol Sistemleri Güvenliği Uzmanı (Industrial Control Systems Security Specialist):

Bir enerji santralinin ICS güvenliğini sağlarlar.

Blockchain Güvenliği Uzmanı (Blockchain Security Specialist):

Bir kripto borsasının güvenliğini sağlarlar.

Dijital Tehdit Analisti (Digital Threat Analyst):

Bir siber casusluk saldırısını inceleyerek kimin arkasında olduğunu belirlerler.

Yapay Zeka ve Makine Öğrenimi Güvenliği Uzmanı (AI and Machine Learning Security Specialist):

Bir sağlık kuruluşu için hastaların sağlık verilerini korurken yapay zeka kullanırlar.

Uygulama Penetrasyon Testi Uzmanı (Application Penetration Testing Specialist):

Bir e-ticaret uygulamasının güvenliğini test ederler.

Veri Analitiği ve Güvenlik Uzmanı (Data Analytics and Security Specialist):

Veri madenciliği teknikleriyle güvenlik olaylarını önceden tahmin ederler.

Siber Hukuk Uzmanı (Cybersecurity Lawyer):

Bir şirketin bir veri ihlali sonucu maruz kaldığı yasal sorunları ele alırlar.

İşe yeni başlayanlara “Analist” denir.

SOME VE SOC

Some (Siber Olaylarla Mücadele Ekibi) “Blue Team”

SOME (Siber Olaylara Müdahale Ekibi), bir organizasyonun veya kurumun siber güvenliği ile ilgili olayları izlemek, tespit etmek, analiz etmek, yanıtlamak ve çözmek için kurulan bir ekiptir. Bu ekip, siber tehditlere karşı savunma sağlamak, olayları hızla çözmek ve potansiyel olarak zararlı etkileri en aza indirmek amacıyla çalışır.

SOME ekibi genellikle aşağıdaki görevleri yerine getirir:

Olay Tespiti: SOME ekibi, ağlarını ve sistemlerini sürekli olarak izler ve potansiyel siber tehditleri tespit etmek için güvenlik olaylarını analiz eder.

Olay Analizi: Ekip, tespit edilen olayları ayrıntılı bir şekilde analiz eder.

Olay Yanıtı: SOME ekibi, bir siber olay tespit edildiğinde hızla yanıt verir.

Olayın Düzgün Kayıt Altına Alınması: Ekip, tüm olayları ve müdahale süreçlerini ayrıntılı bir şekilde kayıt altına alır.

SOME ekibi, organizasyonların siber güvenliğini artırmak ve siber saldırılara karşı direnç olmalarını sağlamak için çok önemlidir.

Önemli nedenler şunlar olabilir:

Siber Tehditlere Hızlı Yanıt: SOME ekipleri, siber saldırıları hızla tespit edebilir ve yanıtlayabilir, bu da organizasyonların potansiyel olarak büyük zararları en aza indirmelerine yardımcı olur.

Veri ve Varlık Koruması: SOME ekipleri, organizasyonların hassas verilerini ve diğer varlıklarını koruma görevini üstlenir. Bu, veri sızıntıları ve kayıplarının önlendiği anlamına gelir.

Siber Güvenlik Farkındalığı: SOME ekibi, organizasyonun siber güvenlik farkındalığını artırır ve güvenlik politikalarını uygulamak için en iyi uygulamaları teşvik eder.

Uzun Vadeli Öğrenme: SOME ekipleri, saldırılar hakkında bilgi toplar ve bu bilgiler gelecekteki olaylara karşı hazırlık olarak kullanır. Bu, organizasyonun siber güvenlik savunmasını sürekli olarak güçlendirmeye yardımcı olur.

Some Ekibinde Çalışan Kişiler

Siber Güvenlik Analisti: Olayları izler ve analiz eder, yanıt planlarını uygular.

Siber Tehdit Avcısı: Gelişmiş tehditleri tespit eder ve izler.

Kriz Yöneticisi: Büyük olayların kriz yönetimini sağlar.

Siber Güvenlik Eğitmeni: Çalışanları güvenlik konusunda eğitir ve farkındalık programları düzenler.

Temel Yetenek	Eğitimler
Açıklık Analizi	- Temel Güvenlik Denetim Eğitimi - Sistem Güvenlik Denetim Eğitimi - Sızma Testleri Eğitimi - Saldırı Teknikleri Eğitimi
Kayıt Yönetimi	- Saldırı Tespit Sistemi Eğitimi - Kayıt Yönetimi Eğitimi - Merkezi Güvenlik İzleme ve Olay Yönetimi Eğitimi
Siber Olay Müdahale	- Siber Olaylara Müdahale Ekibi Kurulumu ve Yönetimi Eğitimi - Bilgi Sistemleri Adli Analizi Eğitimi - Bilgisayar Adli Analizi – Derinlemesine Windows Eğitimi - Karşı Adli Bilişim Eğitimi - İleri Bilgisayar Adli Analizi ve Olay Müdahale Eğitimi - Ağ Adli Analizi Eğitimi - Zararlı Yazılım Analiz Yöntemleri Eğitimi - DDoS Saldırıları ve Korunma Yolları Eğitimi - Bilişim Hukuku
Bilgi Güvenliği Yönetimi	- ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Uygulama Eğitimi - ISO 22301 İş Sürekliliği / Felaket Kurtarım Planlaması Eğitimi

Temel Yetenek	Eğitimler	Eğitimden Beklenen Faydalar
Zafiyet Analizi	- Güvenli Yapılandırma Denetimi Eğitimi - Sızma Testleri Eğitimi - Saldırı Teknikleri Eğitimi	Kurumsal SOME personelinin bir siber olay gerçekleşmeden önce sistemlerdeki önemli zafiyetleri tespit etmesi ve karşı önlem uygulamasını koordine etmesi için gerekli yetenekleri kazanması
Kayıt Yönetimi	- Saldırı Tespit ve Kayıt Yönetimi Eğitimi - Merkezi Güvenlik İzleme ve Olay Yönetimi Eğitimi	Kurumsal SOME personelinin sistemdeki kayıtları takip edebilmesi, sistemler ve tehditler ile ilgili farkındalık kazanabilmesi
Siber Olay Müdahale	- Siber Olaylara Müdahale Ekibi Kurulumu ve Yönetimi Eğitimi - Bilişim sistemleri Adli Analizi Eğitimi - Bilgisayar Adli Analizi - Derinlemesine Windows Eğitimi - Ağ Adli Analizi Eğitimi - Zararlı Yazılım Analiz Yöntemleri Eğitimi - DDoS Saldırıları ve Korunma Yolları Eğitimi - Bilişim Hukuku Eğitimi	Bir siber olay gerçekleşmesi durumunda gerekli olacak olay yönetimi ve koordinasyonu yeteneklerinin kazanılması, dijital delillerin geçerliliğinin bozulmaması için alınacak tedbirlerin öğrenilmesi. Adli analiz esasen kolluk makamının görevi olmakla birlikte, kurumların “sistem izleme” ve “kayıt yönetimi” kapsamında giriş seviyesinde adli analiz bilgisine sahip olması gerekmesi.
Bilgi Güvenliği Yönetimi	- ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Uygulama Eğitimi	Bilgi güvenliği/siber güvenlik sürecinin kavratılması ve Bilgi Güvenliği Yönetim Sistemi ile ilgili farkındalık oluşması.

Soc (Güvenlik Operasyon Merkezi)

SOC (Güvenlik Operasyon Merkezi), bir organizasyonun veya kurumun siber güvenliği ile ilgili sürekli izleme, tehdit tespiti, yanıt verme ve güvenlik olaylarını yönetme **amacıyla** kurulan bir merkezdir. SOC, siber tehditlere karşı savunma sağlamak ve siber güvenliği artırmak için tasarlanmış bir operasyonel birimdir.

Görevleri

Siber Tehdit İzleme: SOC, organizasyonun bilgisayar ağları ve sistemlerini sürekli olarak izler ve siber tehditlerin erken tespitini sağlar.

Tehdit Analizi: SOC, tespit edilen tehditleri analiz eder ve bunların ne kadar ciddi olduğunu ve organizasyona ne tür zararlar verebileceğini belirlemeye çalışır.

Olay Yanıtı: SOC, siber güvenlik olaylarını hızla yanıtlar. Tehditlerin etkisini sınırlamak ve organizasyonun sistemlerini korumak için gerekli aksiyonları alır.

Olay Kayıt ve Raporlama: SOC, tüm güvenlik olaylarını ayrıntılı bir şekilde kayıt altına alır ve bu kayıtları organizasyonun yasal gereksinimlerine ve raporlama ihtiyaçlarına uygun olarak saklar.

İşleyişi

SOC, genellikle birkaç ana bileşenden oluşur:

Monitörleme ve Algılama Sistemleri: Bilgisayar ağları ve sistemlerini sürekli olarak izlemek ve tehditleri tespit etmek için kullanılan güvenlik araçları ve yazılımları içerir.

Analiz ve Yanıt Ekibi: Tehditleri analiz eden ve olaylara yanıt veren siber güvenlik uzmanlarından oluşur.

Olay Kayıt ve Yönetim: Olayların kaydedildiği ve raporlandığı bir veritabanını içerir.

İletişim ve İşbirliği: İlgili paydaşlarla iletişim kurma ve işbirliği yapma yeteneklerini içerir. Bu, diğer organizasyon birimleri, üçüncü taraf güvenlik hizmet sağlayıcıları ve yetkilendirilmiş makamlarla iletişimi içerebilir.

Önemi

Siber Tehditlere Hızlı Yanıt: SOC, organizasyonların siber tehditlere hızlı bir şekilde yanıt vermesini sağlar, bu da potansiyel hasarın en aza indirilmesine yardımcı olur.

Veri ve Varlık Koruması: SOC, organizasyonların hassas verilerini ve diğer varlıklarını koruma görevini üstlenir, böylece veri sızıntıları ve kayıpları önlenir.

Siber Güvenlik Bilinci: SOC, organizasyon içinde siber güvenlik farkındalığını artırır ve güvenlik politikalarının uygulanmasına yardımcı olur.

Sürekli İyileştirme: SOC, güvenlik olaylarından öğrenir ve organizasyonun siber güvenlik savunmasını sürekli olarak güçlendirmeye yardımcı olur.



Soc Örnekler

Sosyal Mühendislik Saldırısı Tespiti: Bir çalışan, sahte bir e-posta aldığını bildirir. SOC, bu e-postayı analiz eder, sahte olduğunu teyit eder ve diğer çalışanları uyarır.

Siber Tehdit İstihbaratı Kullanımı: SOC, karanlık web ve siber tehdit istihbarat kaynaklarından gelen bilgileri izler, tehditleri belirler ve buna karşı önlemler alır.

Güvenlik Olaylarının İzlenmesi: SOC, organizasyonun ağlarını ve sistemlerini sürekli olarak izler. Örneğin, bir saldırganın sisteme yetkisiz erişim sağlama girişimini tespit edebilir.

Soc Ekibinde Çalışan Kişiler

Siber Güvenlik Analisti: Olayları izler, analiz eder ve yanıt planlarını uygular.

Siber Tehdit İstihbarat Analisti: Tehdit istihbaratını izler ve analiz eder.

Günlük İzleme Analisti: Günlük kayıtları inceler ve potansiyel güvenlik olaylarını tespit eder.

Kriz Yöneticisi: Büyük olayların kriz yönetimini sağlar.

USİBM
ULUSAL SİBER OLAYLARA MÜDAHALE MERKEZİ

FAALİYET AMACI

- ULUSAL SİBER GÜVENLİK ANLAYIŞINI GELİŞTİRMEK
- SİBER TEHDİTLERİ ÖNLEMEK AMACIYLA ALARM, UYARI VE DUYURU
- KRİTİK DURUMLARDA YERİNDE MÜDAHALE EKİPLERİYLE KONTROL SAĞLAMAK
- SİBER OLAYLARA MÜDAHALEDE ULUSAL KOORDINASYON

ULUSLARARASI TELEKOMÜNİKASYON BİRLİĞİ GLOBAL SİBER GÜVENLİK ENDEKSİ SIRALAMASI

TÜRKİYE

- DÜNYA'DA 11.
- AVRUPA'DA 6.

PROJELERDEN BAZILARI

- AVCI**
Zararlı yazılım bulaşmış sistemlerin ve komuta kontrol merkezlerinin tespiti
- KASIRGA**
Ülkenin internete açık kaynaklarına ilişkin zafiyet taraması ve hizmet sürekliliğinin sağlanması
- AZAD**
Makine öğrenmesi ve yapay zeka ile "botnet"lere dahil olan köle bilgisayarların belirlenmesi
- ATMACA**
Zafiyete ait risklerin proaktif şekilde engellenmesi
- KULE**
Tespit edilen siber güvenlik eksikliklerine ilişkin bilgilerin ilgili taraflara iletilmesi

PROGRAM SERTİFİKASI

