EDA ARSLAN

İçindekiler

[ARAŞTIRMA SORULARI 4](#_Toc172724981)

[SİBER GÜVENLİK 4](#_Toc172724982)

[BİLGİ GÜVENLİĞİ 4](#_Toc172724983)

[BİLGİ GÜVENLİĞİNİN TEMEL HEDEFLERİ 4](#_Toc172724984)

[Siber Saldırının Amacı Nedir? 5](#_Toc172724985)

[SİBER SALDIRI (CYBER ATTACK) 5](#_Toc172724986)

[SALDIRGAN(ATTACKER) 5](#_Toc172724987)

[SİYAH ŞAPKALI (black hat) HACKER 6](#_Toc172724988)

[BEYAZ ŞAPKALI (White hat) HACKER 6](#_Toc172724989)

[BAŞLICA SİBER TEHDİTLER 6](#_Toc172724990)

[1) Malware 7](#_Toc172724991)

[2) Phishing 7](#_Toc172724992)

[3) DoS ve DDoS 7](#_Toc172724993)

[4) Man in The Middle 7](#_Toc172724994)

[5) SQL Injection 7](#_Toc172724995)

[6) Cryptojacking 7](#_Toc172724996)

[7) Zero Day Exploit 8](#_Toc172724997)

[8) Passwords Attack 8](#_Toc172724998)

[9) Eavesdropping Attack 8](#_Toc172724999)

[10) Birthday Attack 8](#_Toc172725000)

[SİBER GÜVENLİK GEREKTİĞİ GİBİ SAĞLANAMAZ İSE OLUŞABİLECEK ZARARLAR 8](#_Toc172725001)

[SİBER TEHDİTLERİN ZARAR VERMESİNİ ENGELLEMEK VEYA AZALTAK İÇİN ALINACAK ÖNLEMLER 9](#_Toc172725002)

[Teknik Önlemler 9](#_Toc172725003)

[Organizasyonel Önlemler 9](#_Toc172725004)

[Bireysel Önlemler 10](#_Toc172725005)

[KRİPTOGRAFİ 10](#_Toc172725006)

[KÖTÜ AMAÇLI YAZILIM (MALWARE) LAR VE TÜRLERİ 11](#_Toc172725007)

[Türleri 11](#_Toc172725008)

[Kötü Amaçlı Yazılımlardan Korunma Yolları 12](#_Toc172725009)

[OLTALAMA (phishing) SALDIRISI 13](#_Toc172725010)

[Phishing Nedir? 13](#_Toc172725011)

[Oltalama Saldırısının Türleri 13](#_Toc172725012)

[Oltalama (Phishing) Saldırılarının Önemi 14](#_Toc172725013)

[SOSYAL MÜHENDİSLİK 15](#_Toc172725014)

[Sosyal Mühendislik Türleri 15](#_Toc172725015)

[Sosyal Mühendislikten Korunma Yolları 16](#_Toc172725016)

[SİBER SALDIRI ANALİZİ NEDİR? FAYDALARI NELERDİR? 16](#_Toc172725017)

[Aşamaları 16](#_Toc172725018)

[SİBER SALDIRIANALİZİ FAYDALARI 17](#_Toc172725019)

[GÜVENLİK AÇIĞI 19](#_Toc172725020)

[Güvenlik Açığı Türleri Nelerdir 19](#_Toc172725021)

[Sistemlerde güvenlik açıkları nasıl tespit edilir? 20](#_Toc172725022)

[Güvenlik açıkları nasıl kapatılır? 21](#_Toc172725023)

[WEB SALDIRILARI NEDİR? 21](#_Toc172725024)

[Web sitelerinde güvenlik açıkları nasıl tespit edilir? 21](#_Toc172725025)

[SOLUCAN(WORM) 25](#_Toc172725026)

[Solucanların Özellikleri ve Çalışma Prensibi 25](#_Toc172725027)

[Solucan Türleri ve Yayılma Yöntemleri 25](#_Toc172725028)

[Ünlü Solucan Örnekleri 26](#_Toc172725029)

[Solucanlardan Korunma Yöntemleri 26](#_Toc172725030)

[TRUVA ATI (TROJAN HORSE) 26](#_Toc172725031)

[Truva Atı'nın Özellikleri 26](#_Toc172725032)

[Truva Atı Türleri 27](#_Toc172725033)

[Truva Atı'nın Çalışma Prensibi 27](#_Toc172725034)

[Truva Atı'ndan Korunma Yolları 27](#_Toc172725035)

[CASUS YAZILIM (SPYWARE) 27](#_Toc172725036)

[Casus Yazılım Türleri 28](#_Toc172725037)

[Casus Yazılımın Çalışma Prensibi 28](#_Toc172725038)

[Casus Yazılımdan Korunma Yolları 29](#_Toc172725039)

[DDOS 29](#_Toc172725040)

[DDoS saldırısı nasıl işler? 29](#_Toc172725041)

[DDoS Saldırılarının Çeşitleri 30](#_Toc172725042)

[DDoS Saldırılarının Belirtileri 30](#_Toc172725043)

[DDoS Saldırılarından Korunma Yolları 30](#_Toc172725044)

[DDoS Saldırısına Karşı Hızlı Müdahale Adımları 31](#_Toc172725045)

[SON ZAMANLARDA GERÇEKLEŞEN ÖNEMLİ İNTERNET SALDIRILARI 31](#_Toc172725046)

[RANSOMWARE 32](#_Toc172725047)

[Fidye Yazılımının Türleri 32](#_Toc172725048)

[Kripto Fidye Yazılımı (Crypto Ransomware): 32](#_Toc172725049)

[Kilitleme Fidye Yazılımı (Locker Ransomware): 32](#_Toc172725050)

[Scareware: 32](#_Toc172725051)

[Doxware: 32](#_Toc172725052)

[Fidye Yazılımının Çalışma Prensibi 32](#_Toc172725053)

[Fidye Yazılımından Korunma Yolları 33](#_Toc172725054)

[Örnek Fidye Yazılım Saldırıları 33](#_Toc172725055)

[KAYNAKÇA 34](#_Toc172725056)

# ARAŞTIRMA SORULARI

## SİBER GÜVENLİK

İçinde yaşadığımız yüzyılın postmodern şartları içinde bulunduğumuz karışık ve bilinmezliklerle dolu dünyanın merkezinde kuşkusuz güvenlik kavramı yer almaktadır. Siber uzay olarak adlandırılan ve içinde bilgisayar sistemleri, online iletişim ağları ve kontrol sürecinin bulunduğu bilgi iletişim teknolojilerinin kurduğu bu devasa dünya, küresel ölçekte sosyal, ekonomik, politik ve kültürel bütünleşmenin bir parçası olarak hızla gelişmektedir. Günlük hayatta kullandığımız araç ve gereçlerin çoğu siber uzayın elemanıdır. Bu araçların ve bütün haliyle internet tabanının hayatı tehlikededir.

Siber güvenlik, dijital ortamda bilginin ve verinin güvenliği için yapılan bütün çalışmalardır. Ağ yapısına bağlı sistemleri ve bu sistemlerle ilişkili verileri yetkisiz kullanım veya zararlardan korumak için sarf edilen sonsuz bir çabadır.

## BİLGİ GÜVENLİĞİ

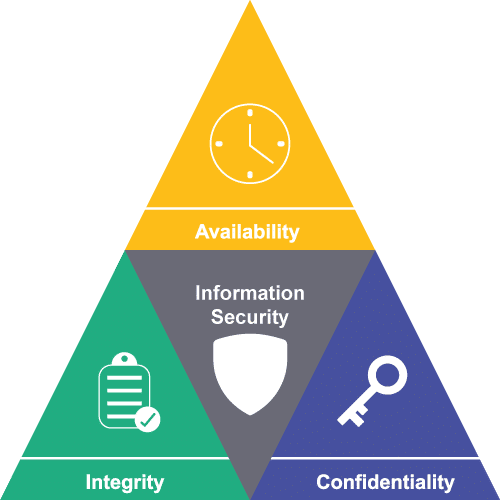
Bilgi güvenliği, bir organizasyonun veya bireyin hassas bilgilerini, verilerini ve bilgi kaynaklarını, yetkisiz erişim, değiştirme, ifşa veya zarar verme gibi tehditlere karşı koruma sürecidir.

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.

### BİLGİ GÜVENLİĞİNİN TEMEL HEDEFLERİ

1. GİZLİLİK: Hassas bilgilerin yetkisiz kişiler tarafından erişilmesini önlemek.
2. BÜTÜNLÜK : Bilgilerin değiştirilmesini veya bozulmasını engellemek.
3. ERİŞİLEBİLİRLİK: Yetkilendirilmiş kullanıcıların bilgilere güvenli bir şekilde erişimini sağlamak.
4. SÜREKLİLİK: Bilgilerin sürekli olarak kullanılabilir ve erişilebilir olmasını sağlamak.
5. İZLENEBİLİRLİK: Bilgiye kimin eriştiğini ve ne zaman eriştiğini izleyebilme yeteneği.

CIA CYBERSECURITY : CONFIDENTIALITY(gizlilik), INTEGRITY(bütünlük), AVAILABILITY(erişilebilirlik)



#### SİBER GÜVENLİK VE BİLGİ GÜVENLİĞİ

* Bilgi güvenliği, organizasyonların genel olarak bilgi varlıklarını korumak için aldıkları önlemleri kapsar.
* Siber güvenlik, bilgi sistemlerini ve ağlarını korumak için alınan spesifik önlemleri ifade eder. Siber güvenlik, bilgi güvenliğinin bir parçasıdır ve bilgi sistemlerinin çevrimiçi tehditlere karşı korunmasına odaklanır.
* Bilgi güvenliği ve siber güvenlik arasındaki ilişki karşılıklıdır. Siber güvenlik, organizasyonların bilgi güvenliğini sağlama çabalarının önemli bir bileşenidir. Bilgi güvenliği politika ve prosedürleri, siber güvenlik tedbirlerini içerirken, siber güvenlik önlemleri de bilgi güvenliğini destekler.

## Siber Saldırının Amacı Nedir?

Siber saldırıların en yaygın olarak bilinen amacı, mali kazanç elde etmek için kişisel verilerin (kimlik, kredi kartı ve adres bilgileri) toplanmasıdır. Ancak sistemler üzerinden politik ve rekabet amaçlı saldırılar da gerçekleşebilir.

İnternet üzerinden ticaret yapan e-ticaret sitelerinin düzgün çalışmasını engelleyebilen siber saldırılar, maddi anlamda ciddi kayıplara neden olabilir. Farklı politik grupların gerçekleştirdiği saldırılardaki ana amaç, bilgi korsanlığı ya da bilgi hırsızlığı olarak bilinir.

Sonuç olarak siber saldırıların genel amacı bilgi hırsızlığı ve mali kazanç elde etme arzusudur.

## SİBER SALDIRI (CYBER ATTACK)

Siber saldırı, odaklanılan bir sistemin açıklarını keşfederek, bilgilerin izinsiz bir şekilde alınmasıyla ya da değiştirilmesiyle gerçekleştirilen bilgi işlem sistemine saldırılması olarak tanımlanır. Siber saldırılar, kişiler, kurumlar ve devletler arası birçok farklı boyutta, yasa dışı şekilde gerçekleştirilir. Bilgi çalmak, değiştirmek ve hatta yok etmek amacıyla yapılan bilgisayar ve internet kaynaklı izinsiz erişim yöntemleri, toplu olarak “Siber Saldırı” adıyla anılır.

Amerika Birleşik Devletleri Ulusal Araştırma Konseyinde 2009 yılında yapılan bir çalışmada Siber Saldırılar; “Ağlar, bilgisayar sistemleri veya bilgiyi ve bunlarda yerleşik olan ya da bunları taşıyan programları bozmak, aldatmak, küçük düşürmek veya yok etmek için yapılan kasıtlı hareketler” olarak tanımlanmıştır (Singer ve Friedman, 2015).

## SALDIRGAN(ATTACKER)

Siber saldırı yapan kişilere genel olarak saldırgan(attacker) denir. Bu kişilerin aşağıdaki gibi hedefleri vardır:

1. Maddi kazanç elde etme
2. Şöhret elde etme ve bununla övünme,
3. Karşı tarafa maddi veya manevi zarar verme
4. Önemli bilgileri belli bir amaçla çalma(örn. casusluk)

## SİYAH ŞAPKALI (black hat) HACKER

Yasa dışı faaliyetler yürüterek kazanç sağlamayı amaçlayan hacker’lardır. Genellikle finansal kazanç, kişisel intikam veya politik nedenlerle sistemlere sızarlar.

Bu hacker’lar, zararlı yazılımlar ve kimlik avı gibi çeşitli tekniklerle güvenlik duvarlarını aşarlar. Sistem açıklarını bulup istismar eder, bilgi çalar veya sistemleri çökertirler.

Cracker’lar, internet üzerinden yazılım korsanlığı yapanlardan oyunların lisans anahtarlarını kıranlara kadar geniş bir yelpazede faaliyet gösterirler. Yazılım geliştiricileri ve güvenlik firmaları, cracker’ların zararlı eylemlerini engellemek için sürekli yeni korunma teknikleri geliştirmektedir.

Siber saldırıların %45’i siyah şapkalı hacker’lar tarafından gerçekleştirilir. Siyah şapkalı hackerların faaliyetleri, hem bireysel kullanıcılar için hem de büyük kurumsal yapıların güvenliği için ciddi tehditler oluşturur. Çeşitli zararlı yazılımlar (virüsler, trojanlar, ransomware) ve sosyal mühendislik teknikleriyle bilgi sızdırabilirler. Bu nedenle, sistem güvenliğini sağlamak için güçlü parolalar kullanmak, yazılımları güncel tutmak ve düzenli olarak güvenlik taramaları yapmak hayati önem taşımaktadır. Hackerlar her zaman yeni teknik yöntemler geliştirir, bu nedenle devamlı bir güvenlik stratejisi gereklidir.

## BEYAZ ŞAPKALI (White hat) HACKER

Bilgisayar sistemlerinin güvenliğini artırmak için çalışan etik hackerlardır. Amaçları, sistem açıklarını bulup bildirerek siber güvenliği sağlamaktır. Siyah şapkalı hacker’ların yaptığı işleri legal şekilde yapar.

* Sistem açıklıklarını belirler ve raporlar.
* Firma sistemlerini saldırılara karşı test eder.
* Siber güvenlik protokollerini geliştirir ve uygular.
* Kurum içi eğitimler düzenler.

Beyaz şapkalı hackerlar, sertifikasyon programları ile yetkinlik kazanır.

Bu tür hackerlar, şirketler ve devlet kurumları tarafından sıkça istihdam edilirler.

## BAŞLICA SİBER TEHDİTLER

Siber güvenliğin karşı karşıya olduğu tehditlerin üç katmanı vardır:

1. Siber suç finansal kazanç veya işlerin kesintiye uğraması için sistemleri hedefleyen tek aktörleri veya grupları içerir.
2. Siber saldırı genellikle politik nedenli bilgi toplamayı içerir.
3. Siber terör, elektronik sistemleri panik veya korkuya neden olacak şekilde baltalamak için tasarlanır.

Siber güvenliği tehdit etmek için kullanılan bazı yöntemler aşağıda verilmiştir.

* Kötü amaçlı yazılımlar (virüs, casus yazılım vb.),
* Oltalama (phishing),
* Hizmet engelleme (denial of service, DoS),
* Veri sızdırma,
* Yetki çalma,
* Aradaki adam (man in the middle) saldırıları

yaygın siber tehditlere örnek olarak verilebilir.

### 1) Malware

Malware kötü niyetli yazılımların kısaltmasıdır. Solucanlar, virüsler, truva atları bunlara örnek olarak verilebilir. Kişilerin izni olmadan bilgisayar sistemlerine sızdırılan kötü amaçlı yazılımlardır. Bilgisayarları veya ağları çalışamaz hale getirebilir, gizlenebilir, çoğalabilir veya saldırganlara erişim izni verip sistemi uzaktan kontrol edebilme şansı verebilirler.

### 2) Phishing

Kimlik avı saldırıları olarak adlandırılan bu yöntemde ise saldırganlar kişilere güvenilir kaynaklardan gelmiş gibi gösterilen e-postalar yollayarak kişilerin site bilgilerini, kredi kartı bilgilerini çalmaya çalışırlar. Genellikle e-posta yoluyla gönderdikleri linklere tıklayan mağdurlar, klonlanmış sitelere yönlendirilir ve girdikleri bilgileri saldırganlarla paylaşmış olurlar.

### 3) DoS ve DDoS

İngilizce açılımı Denial of Services ve Distributed Denial of Services olan bu yöntemler ise bazı çevrimiçi hizmetlerin düzgün çalışmasını engellemeye çalışmak için yapılan saldırılardır. Saldırganlar bir web sitesine veya bir veri tabanına çok fazla sayıda istek yollayıp sistemi meşgul ederler ve bu da sistemlerin çalışmasını durdurmasına yol açabilir. DDoS ise bu saldırıların birden fazla bilgisayardan yapılması ile olur.

### 4) Man in The Middle

Bu siber saldırı çeşidinde ise saldırganlar kurbanlar ile erişmek istedikleri web servisi arasında kendilerini gizleyerek, kurbanları kendi ağları üzerinden erişmek istedikleri servise yönlendirirler. Örneğin bir Wi-Fi ağını taklit ederler ve kurbanlar erişmek istedikleri Wi-Fi ağı yerine saldırganların Wi-Fi ağına girmiş olurlar. Bundan sonraki yaptıkları her işlemi saldırganlar görebilir ve kullanıcıların verilerini toplayabilirler.

### 5) SQL Injection

Günümüzde birçok veri tabanı SQL ile yazılmış komutlara uymak için tasarlanmıştır ve kullanıcılardan bilgi alan birçok web sitesi bu verileri SQL veri tabanlarına gönderir. Saldırganlar SQL güvenlik açıklarından faydalanarak kurbanların veri tabanlarını kontrol altına alırlar. Örneğin bir SQL enjeksiyon saldırısında bir bilgisayar korsanı, bazı SQL komutlarını ad ve adres bilgisi isteyen bir web formuna yazar; web sitesi ve veri tabanı doğru programlanmadıysa, veri tabanı bu komutları çalıştırmayı deneyebilir.

### 6) Cryptojacking

Cryptojacking, başkasının bilgisayarının sizin için cryptocurrency üretme işini yapmasını içeren özel bir saldırıdır. Saldırganlar gerekli hesaplamaları yapmak için kurbanın bilgisayarına kötü amaçlı yazılım yüklerler veya bazen kötü amaçla kullandıkları kodları kurbanın tarayıcısında çalışan JavaScript'te çalıştırırlar.

### 7) Zero Day Exploit

Adını bir yama yayınlandıktan sonra, kullanıcıların güvenlik güncellemelerini indirirken az sayıda bilgisayara ulaşmalarından alır. Yazılımdaki açıklar henüz daha düzeltilmemiştir ve bu da saldırganlara fırsat sağlar. Bu tür güvenlik açıklarından yararlanma teknikleri günümüzde Darkweb üzerinden yayınlanmakta veya satılmaktadır.

### 8) Passwords Attack

Şifreleme bir sisteme girerken kullandığımız en yaygın mekanizma olduğundan, parola saldırıları en yaygın saldırılar arasındadır. Brute Force olarak adlandırılan bir çeşidinde şifre tahmini için aralıksız olarak rastgele şifre deneyen bir kötü amaçlı teknik kullanılır. Bunu engellemenin en kolay yolu çok kez denenen parola girişiminin ardından kendini kilitleyen bir hesap kilitleme politikası uygulamaktır.

### 9) Eavesdropping Attack

Bu saldırı tipinde saldırganlar bir ağa sızarlar ve gizlice dinleme yaparak kullanıcıların o ağ üzerinden göndereceği kredi kartı bilgileri, şifreler ve konuşmalar gibi kişisel verileri dinlerler. Pasif olan yönteminde genellikle sadece dinleme yaparak bilgiler toplanır fakat aktif yönteminde ise saldırganlar kullanıcılara ağdaki dost bir birim gibi gözükerek sorular sorarak bilgi toplarlar.

### 10) Birthday Attack

Doğum günü saldırıları, bir mesajın, yazılımın veya dijital imzanın bütünlüğünü doğrulamak için kullanılan karma algoritmalara karşı yapılır. Bir karma işlevi tarafından işlenen bir mesaj, giriş mesajının uzunluğundan bağımsız olarak sabit uzunlukta bir mesaj özeti (MD) üretir. Bu MD, mesajı benzersiz bir şekilde karakterize eder. Doğum günü saldırısı, bir karma işlevi tarafından işlendiğinde aynı MD'yi üreten iki rastgele mesaj bulma olasılığını ifade eder. Bir saldırgan, kullanıcısı olduğu gibi mesajı için aynı MD'yi hesaplarsa, kullanıcının mesajını güvenle onunla değiştirebilir ve alıcı MD'leri karşılaştırsa bile değiştirmeyi tespit edemez.

## SİBER GÜVENLİK GEREKTİĞİ GİBİ SAĞLANAMAZ İSE OLUŞABİLECEK ZARARLAR

1. Veri İhlalleri ve Hırsızlığı: Hassas bilgiler (kişisel bilgiler, finansal veriler, sağlık kayıtları vb.) siber saldırılar sonucu çalınabilir. Bu, bireyler ve şirketler için ciddi maddi ve manevi kayıplara yol açabilir.
2. Finansal Kayıplar: Siber saldırılar, dolandırıcılık ve kimlik hırsızlığı gibi yöntemlerle bireylerin ve şirketlerin maddi kayıplar yaşamasına neden olabilir. Fidye yazılım saldırıları sonucu büyük meblağlar talep edilebilir.
3. Operasyonel Kesintiler: Siber saldırılar, şirketlerin ve kurumların operasyonlarını durma noktasına getirebilir. Hizmetlerin aksaması, üretimin durması veya kritik altyapıların zarar görmesi gibi durumlar büyük operasyonel kayıplara neden olabilir.
4. Reputasyon Zararları: Bir şirketin siber saldırıya uğraması, müşterilerinin ve iş ortaklarının güvenini kaybetmesine yol açabilir. Bu da uzun vadede müşteri kaybına ve gelir düşüşüne neden olabilir.
5. Yasal ve Düzenleyici Sorunlar: Veri ihlalleri, yasal yükümlülüklere uymayan şirketler için büyük cezalar ve davalarla sonuçlanabilir. GDPR gibi veri koruma yasaları ihlal edildiğinde ciddi yasal sonuçlar doğabilir.
6. Fidye Yazılım Saldırıları: Fidye yazılımlar, kullanıcıların dosyalarını şifreleyip erişimi engelleyerek fidye talep eder. Bu tür saldırılar, bireyleri ve şirketleri büyük maddi kayıplara uğratabilir.
7. Fikri Mülkiyet Hırsızlığı: Şirketlerin patentli teknolojileri, tasarımları ve diğer fikri mülkiyetleri çalınabilir, bu da rekabet avantajını kaybetmelerine neden olabilir.
8. Kritik Altyapıların Tehlikeye Girmesi: Enerji, su, ulaşım gibi kritik altyapılara yapılan saldırılar, toplumsal düzeni ciddi şekilde bozabilir ve geniş çaplı kesintilere yol açabilir.
9. İtibar Kayıpları: Siber saldırılara maruz kalan bireyler ve kurumlar, itibarlarını kaybedebilir. Bu da müşteri kaybına, ortaklıkların sona ermesine ve uzun vadede gelir düşüşüne yol açabilir.
10. Bireysel Güvenlik Tehditleri: Kişisel bilgilerinin çalınması bireylerin güvenliğini tehdit edebilir, kimlik hırsızlığına maruz kalmalarına ve maddi kayıplara neden olabilir.

## SİBER TEHDİTLERİN ZARAR VERMESİNİ ENGELLEMEK VEYA AZALTAK İÇİN ALINACAK ÖNLEMLER

İlk olarak alabileceğimiz bir dizi önlem vardır. Bunlar teknik, organizasyonel ve bireysel boyutta olabilir.

### Teknik Önlemler

* Güçlü Şifreleme: Verilerin şifrelenmesi, hem depolama hem de iletim sırasında hassas bilgilerin korunmasını sağlar.
* Güvenlik Duvarları ve Antivirüs Yazılımları: Güvenlik duvarları ve antivirüs yazılımları, kötü amaçlı yazılımların ve yetkisiz erişimlerin önlenmesine yardımcı olur.
* Düzenli Güncellemeler ve Yamalar: Yazılım ve sistemlerin düzenli olarak güncellenmesi, bilinen güvenlik açıklarının kapatılmasını sağlar.
* Çok Faktörlü Kimlik Doğrulama (MFA): MFA, kullanıcı kimlik doğrulama sürecine ek bir güvenlik katmanı ekler, böylece yalnızca şifreyle erişim sağlanamaz.
* Yedekleme ve Veri Kurtarma: Düzenli veri yedeklemeleri, veri kaybı durumunda verilerin geri yüklenebilmesini sağlar.
* Güvenlik Bilgi ve Olay Yönetimi (SIEM) Sistemleri: SIEM sistemleri, güvenlik olaylarını izler ve analiz eder, böylece potansiyel tehditler hızlı bir şekilde tespit edilebilir.

### Organizasyonel Önlemler

* Güvenlik Politikaları ve Prosedürleri: Kurumlar, siber güvenlik için net ve ayrıntılı politikalar ve prosedürler oluşturmalıdır.
* Eğitim ve Farkındalık Programları: Çalışanların siber güvenlik konusunda eğitilmesi, insan hatasından kaynaklanan riskleri azaltır.
* Erişim Kontrolü: Erişim kontrolü, yalnızca yetkili kişilerin belirli verilere ve sistemlere erişebilmesini sağlar.
* Risk Değerlendirmesi ve Denetimler: Düzenli olarak risk değerlendirmeleri ve güvenlik denetimleri yapılmalıdır.
* Acil Durum Müdahale Planları: Olası bir siber saldırı durumunda hızlı ve etkili bir şekilde yanıt verebilmek için acil durum müdahale planları hazırlanmalıdır.

### Bireysel Önlemler

* Güçlü ve Benzersiz Şifreler: Her hesap için güçlü ve benzersiz şifreler kullanmak, hesapların ele geçirilmesini zorlaştırır.
* Güvenilir Kaynaklardan Yazılım İndirme: Yazılım ve uygulamalar yalnızca güvenilir kaynaklardan indirilmelidir.
* Phishing (Oltalama) Saldırılarına Karşı Dikkat: Şüpheli e-postalar ve bağlantılara tıklamaktan kaçınılmalı ve kişisel bilgiler paylaşılmamalıdır.
* Güvenli İnternet Kullanımı: Halka açık Wi-Fi ağlarında VPN kullanmak ve güvenli web sitelerine (https) erişmek önemlidir.
* Düzenli Yazılım ve Sistem Güncellemeleri: Kişisel cihazlar ve yazılımlar düzenli olarak güncellenmelidir.

## KRİPTOGRAFİ

Kriptografi, verilerin gizliliğini, bütünlüğünü ve doğruluğunu sağlamak amacıyla bilgi güvenliği teknikleri geliştiren ve uygulayan bilim dalıdır. Kriptografi, bilgiyi yetkisiz erişimden korumak için matematiksel algoritmalar ve anahtarlar kullanarak verileri şifrelemeyi ve çözmeyi içerir.

* Şifreleme (Encryption): Verilerin anlaşılabilir formattan (düz metin) şifreli formata (şifreli metin) dönüştürülmesi işlemidir. Bu, yetkisiz kişilerin veriyi okuyamamasını sağlar.

Simetrik Şifreleme: Aynı anahtar hem şifreleme hem de şifre çözme işlemi için kullanılır (örneğin, AES).

Asimetrik Şifreleme: İki farklı anahtar kullanılır; biri şifreleme (genel anahtar) ve diğeri şifre çözme (özel anahtar) için (örneğin, RSA).

* Şifre Çözme (Decryption): Şifreli metnin tekrar anlaşılabilir düz metne dönüştürülmesi işlemidir. Bu işlem, yalnızca yetkili kişilerin veriyi okuyabilmesini sağlar.
* Anahtar Yönetimi: Şifreleme ve şifre çözme işlemlerinde kullanılan anahtarların güvenli bir şekilde oluşturulması, saklanması, dağıtılması ve yok edilmesi sürecidir.
* Özet Fonksiyonları (Hash Functions): Verilerin sabit uzunlukta, benzersiz bir dijital parmak izine (hash) dönüştürülmesini sağlar. Özet fonksiyonları, veri bütünlüğünü ve kimlik doğrulamayı sağlamak için kullanılır (örneğin, SHA-256).

#### Kullanım Alanları

* Veri Gizliliği: Verilerin yetkisiz erişime karşı korunmasını sağlar. Örneğin, e-postaların veya dosyaların şifrelenmesi.
* Veri Bütünlüğü: Verilerin değiştirilmediğinden veya bozulmadığından emin olunmasını sağlar. Örneğin, dosya bütünlüğünü doğrulamak için hash fonksiyonları kullanılması.
* Kimlik Doğrulama: Kullanıcıların kimliklerinin doğrulanmasını sağlar. Örneğin, dijital imzalar ve sertifikalar.
* İmzalama ve Doğrulama: Verilerin ve iletilerin kaynağının doğrulanması ve değişmediğinin garantilenmesi için dijital imzalar kullanılır.

#### Örnek Algoritmalar

* AES (Advanced Encryption Standard): Simetrik şifreleme algoritmasıdır ve çok güvenli olarak kabul edilir.
* RSA: Asimetrik şifreleme algoritmasıdır ve özellikle anahtar değişimi ve dijital imzalar için kullanılır.
* SHA-256: Kriptografik özet fonksiyonu olup, genellikle veri bütünlüğü kontrolü ve kimlik doğrulama için kullanılır.

#### Kriptografinin Önemi

Kriptografi, dijital dünyanın güvenliğini sağlamak için kritik bir rol oynar. Özellikle internet üzerinden gerçekleştirilen iletişimlerde, finansal işlemlerde, elektronik oy kullanma sistemlerinde ve daha birçok alanda veri güvenliğini sağlamak için kullanılır. Güçlü kriptografik yöntemlerin kullanılması, bilgi güvenliği tehditlerine karşı önemli bir savunma hattıdır.

## KÖTÜ AMAÇLI YAZILIM (MALWARE) LAR VE TÜRLERİ

Kötü amaçlı yazılım (malware), bilgisayar sistemlerine, ağlara veya kullanıcı cihazlarına zarar vermek, bilgi çalmak veya kontrol ele geçirmek amacıyla tasarlanmış yazılım türlerini ifade eder. Malware, çeşitli biçimlerde olabilir ve her biri farklı zararlı amaçlara hizmet eder.

### Türleri

#### Virüsler

Açıklama: Kendisini başka programlara ekleyerek yayılabilen kötü amaçlı yazılımlardır. Kullanıcılar bu programları çalıştırdığında virüs aktif hale gelir ve çoğalır.

Etkileri: Dosyaları bozabilir, sistem performansını düşürebilir veya diğer kötü amaçlı yazılımları indirmek için kullanılabilir.

#### Solucanlar (Worms)

Açıklama: Solucanlar, ağlar üzerinden kendiliğinden yayılan bağımsız kötü amaçlı yazılımlardır. Kullanıcı müdahalesine ihtiyaç duymazlar.

Etkileri: Ağ trafiğini artırarak performansı düşürebilir, dosyaları bozabilir veya arka kapılar (backdoors) oluşturabilir.

#### Truva Atları (Trojans)

Açıklama: Yasal bir program veya dosya gibi görünen, ancak arka planda kötü amaçlı faaliyetler yürüten yazılımlardır.

Etkileri: Veri çalma, sistem kontrolü ele geçirme, diğer kötü amaçlı yazılımları indirme gibi faaliyetlerde bulunabilirler.

#### Casus Yazılımlar (Spyware)

Açıklama: Kullanıcının bilgisayar kullanımını izleyen ve bu bilgileri yetkisiz kişilere gönderen yazılımlardır.

Etkileri: Kişisel bilgilerin, şifrelerin ve finansal verilerin çalınmasına neden olabilir.

#### Reklam Yazılımları (Adware)

Açıklama: İstenmeyen reklamlar gösteren yazılımlardır. Genellikle ücretsiz programlarla birlikte gelirler.

Etkileri: Kullanıcı deneyimini olumsuz etkileyebilir, sistemi yavaşlatabilir ve daha ciddi kötü amaçlı yazılımlar için bir geçit oluşturabilir.

#### Fidye Yazılımları (Ransomware)

Açıklama: Kullanıcının dosyalarını şifreleyerek veya sisteme erişimini engelleyerek, kullanıcıdan fidye talep eden yazılımlardır.

Etkileri: Dosyaların kaybı, maddi zarar ve önemli veri kayıplarına yol açabilir.

#### Kök Kitler (Rootkits)

Açıklama: Sistemde derinlemesine gizlenerek varlıklarını gizleyen ve yetkisiz erişim sağlayan kötü amaçlı yazılımlardır.

Etkileri: Sistem güvenliğini tehlikeye atabilir, diğer kötü amaçlı yazılımların yüklenmesine olanak tanır.

#### Botnetler

Açıklama: Çok sayıda bilgisayarı zombi bilgisayarlar haline getirerek bir ağ oluşturur ve bu ağı kötü amaçlı faaliyetler için kullanır.

Etkileri: Dağıtılmış Hizmet Reddi (DDoS) saldırıları, spam gönderme, veri çalma gibi faaliyetlerde bulunabilir.

#### Keyloggerlar

Açıklama: Kullanıcının klavye vuruşlarını kaydeden ve bu bilgileri yetkisiz kişilere gönderen yazılımlardır.

Etkileri: Şifreler, kişisel bilgiler ve finansal veriler gibi hassas bilgilerin çalınmasına neden olabilir.

#### Açık Kapı Yazılımları (Backdoors)

Açıklama: Bir sisteme veya programa yetkisiz erişim sağlamak için kullanılan gizli yolları açan yazılımlardır.

Etkileri: Saldırganlar tarafından sistemin kontrol edilmesi ve diğer kötü amaçlı yazılımların yüklenmesi için kullanılabilir.

### Kötü Amaçlı Yazılımlardan Korunma Yolları

* Güçlü ve Güncel Antivirüs Yazılımları Kullanmak: Antivirüs programları, kötü amaçlı yazılımları tespit eder ve sistemden temizler.
* Düzenli Güncellemeler ve Yamalar: İşletim sistemleri ve yazılımlar için düzenli olarak güncellemeler yapılmalıdır.
* Güvenli İnternet Kullanımı: Güvenilir web sitelerini ziyaret etmek ve şüpheli e-postalardan kaçınmak önemlidir.
* Güçlü Parolalar ve Çok Faktörlü Kimlik Doğrulama: Hesaplar için güçlü parolalar kullanmak ve çok faktörlü kimlik doğrulama (MFA) uygulamak.
* Eğitim ve Farkındalık: Kullanıcıları siber güvenlik tehditleri konusunda eğitmek ve farkındalığı artırmak.

## OLTALAMA (phishing) SALDIRISI

Phishing, internet tarihinin en eski ve en etkili saldırı türlerinden biridir. Oltalama saldırıları olarak bilinen bu saldırı türünde genel olarak kurbanların e-posta hesaplarına; hediye, indirim, veya benzeri cezbedici sahte iletiler gönderilerek parola, kimlik bilgisi veyahut benzeri hassas verilerin çalınması amaçlanır.

İletilen e-posta mesajlarındaki zararlı bağlantılar tıklandığı zaman kurbanın av olması sağlanabildiği gibi e-postalar ile birlikte ek olarak gönderilen virüslü dosyaların çalıştırılması ile de kurbanların bilgisayarları saldırganlar tarafından ele geçirilebilir.

### Phishing Nedir?

* Phishing, genel olarak bir kişinin parolasını, bilgilerini öğrenmek banka hesabını veya amacıyla kullanılır.
* Saldırgan tarafından özel olarak hazırlanan phishing e-postası kredi kartı resmi bir kurumdan geliyormuş gibi ya da gerçek bir e-posta şeklinde görülür.
* Hazırlanan e-posta yardımıyla bilgisayar kullanıcıları sahte sitelere yönlendirilerek parolalarını vermeleri sağlanır. Diğer bir yandan bu epostalara eklenen dosyaların çalıştırılması ile kurbanların bilgisayarları ele geçirilerek saldırganın kontrolü altına girebilir.
* Phishing saldırılarında saldırgan kişi bir “yem” hazırlar ve bu yeme kurbanların takılmasını amaçlar.
* Yem genelde maaş zammı, hediye, ücretsiz tatil, para ödülü şeklinde cezbedici senaryolardan oluşturulur. Kurumlar için büyük riskler oluşturan bu saldırı türüne karşı büyük kayıplar yaşanmaması için çalışanlarının bilgilendirilmesi ve özel olarak eğitilmesi gereklidir.

### Oltalama Saldırısının Türleri

#### Klasik Oltalama (Phishing)

Açıklama: Saldırganlar, sahte e-postalar veya mesajlar göndererek kullanıcılardan hassas bilgiler talep eder. Bu mesajlar genellikle resmi kurum veya güvenilir şirketlerden geliyormuş gibi görünür.

Örnek: Bankanızdan geliyormuş gibi görünen bir e-posta, sizden hesap bilgilerinizi güncellemenizi ister ve sizi sahte bir web sitesine yönlendirir.

#### Mızrak Oltalama (Spear Phishing)

Açıklama: Daha hedefli ve kişiselleştirilmiş bir oltalama saldırısıdır. Saldırganlar, belirli bir kişi veya kurum hakkında bilgi toplayarak daha inandırıcı mesajlar hazırlar.

Örnek: Bir şirketin finans departmanına, şirket CEO'sundan geliyormuş gibi görünen ve acil bir para transferi talep eden bir e-posta gönderilir.

#### Balina Avı (Whaling)

Açıklama: Üst düzey yöneticilere veya önemli kişilere yönelik yapılan, çok iyi planlanmış mızrak oltalama saldırısıdır.

Örnek: CEO'ya, hukuki bir sorunla ilgili acil bilgi isteyen sahte bir e-posta gönderilir.

#### Vishing (Voice Phishing)

Açıklama: Telefon yoluyla yapılan oltalama saldırılarıdır. Saldırganlar, kullanıcıları arayarak hassas bilgilerini vermelerini sağlar.

Örnek: Banka temsilcisi gibi davranan bir saldırgan, kullanıcının kart bilgilerini güncellemesi gerektiğini söyleyerek bilgi talep eder.

#### Smishing (SMS Phishing)

Açıklama: SMS mesajları aracılığıyla yapılan oltalama saldırılarıdır. Kullanıcılardan kişisel veya finansal bilgilerini paylaşmaları istenir.

Örnek: Bankanızdan geliyormuş gibi görünen bir SMS, hesabınızda şüpheli aktiviteler olduğunu ve bir bağlantıya tıklayarak doğrulama yapmanızı ister.

### Oltalama (Phishing) Saldırılarının Önemi

İnternet kullanımı yaygınlaştıkça, kurum çalışanları veya bireysel kullanıcılar daha fazla çevrimiçi olmak, ürün veya hizmetlere erişimde interneti kullanmayı talep etmektedir. Bu noktada internet kullanımının yaygınlaşması ile alışverişlerimiz, bankacılık işlemlerimiz, finansal işlemlerimiz, kurum içi iletişimlerimiz ve benzeri birçok kritik veri internet üzerinde yaygın olarak kullanılmaya başlanmıştır. Doğal olarak bu durum siber saldırganların bakış açısını değiştirerek hedefli saldırıların artırmasına sebep olmuştur.

Siber saldırganlar phishing yöntemleri ile bilinçsiz kullanıcıları hedefleyerek büyük zararlara sebep olmaktadır. Phising saldırıları hedefli olarak yapıldığı takdirde ise büyük bir başarı oranına sahiptir.

Doğal olarak siber saldırganlar internet tarihinin en eski ve en etkili yöntemlerinden biri olan phishing saldırılarını sıklıkla kullanmaktadır. Sosyal mühendislik saldırıları ile birlikte gerçekleştirilen spear phishing saldırıları ise maalesef ki siber saldırganların elinde korunması zor ve tehlikeli bir siber silah olarak kurumları tehdit etmektedir.

Phishing saldırıları hem sosyal mühendislik hem de teknik altyapı kullanılarak gerçekleştirilen bir suç olarak tanımlanır. Yaygın olarak e-posta aracılığıyla gerçekleştirilen bu saldırılar günümüz sosyal ağlarının popüler olması ile evrim geçirerek çok daha büyük kitlelere ulaştığını, virüs worm gibi zararlı kodların yayılmasında etkili rol oynadığı göstermiştir.

## SOSYAL MÜHENDİSLİK

Sosyal mühendislik; etkileme, zorlama, aldatıcı ilişkiler geliştirme, sorumluluğu, etik değerleri, dürüstlüğü ya da bağlılığı azaltma amacını güden yöntemler kullanarak kişileri gizli bilgi vermeleri veya erişim sağlamaları için aldatma sürecidir. Ayrıca sosyal mühendislik; “organizasyon güvenliğinin insanlarla etkileşime girilerek kırılmasıdır” şeklinde tanımlandığı gibi, “insanların ortak duygularındaki boşluklardan avantajlar elde etmek” şeklinde de tanımlanmaktadır. Karakteristik olarak hacking “teknik vasıtalarla yasaklanmış sistemlere girmeye çalışmayı” ifade eder. Hacking olayında hacker “güvenlik boşluklarından avantajlar elde etmeye çalışırken”, sosyal mühendis normal yollardan elde edemeyeceği bilgileri (örneğin şifreler, kripto anahtarları, kullanıcı ID’leri gibi) personeli manipüle ederek elde etmeye çalışır.1 Sonuçta, sosyal mühendislik teknik vasıtalar kullanarak ele geçirilmesi son derece zor olan bilgileri elde etmek için kullanılan bir yöntemdir. Sosyal mühendislik tekniklerinin çoğu insanlardaki psikolojik özelliklerin istismar edilmesine dayanmaktadır.2 Özetle sosyal mühendislik, iletişim (kişiler arası, kişiyle kurum arası, kurumlar arası) açıklıklarından ya da insan davranışlarındaki istismara açık alanlardan faydalanarak güvenlik süreçlerini etkisiz hale getirme yöntemlerine dayanan yasadışı müdahale süreçleridir.

### Sosyal Mühendislik Türleri

#### Phishing (Oltalama)

Açıklama: Kullanıcılardan kişisel ve finansal bilgilerini almak için sahte e-postalar veya mesajlar gönderme yöntemi.

Örnek: Bankanızdan geliyormuş gibi görünen bir e-posta, sizden hesap bilgilerinizi doğrulamanızı ister.

#### Spear Phishing (Mızrak Oltalama)

Açıklama: Daha hedefli ve kişiselleştirilmiş oltalama saldırısı. Belirli bir kişi veya kurumu hedef alır.

Örnek: Bir çalışanı hedef alarak, şirketin IT departmanından geliyormuş gibi görünen bir e-posta ile kullanıcı adı ve şifre bilgilerini istemek.

#### Pretexting (Ön Metin)

Açıklama: Saldırganın, belirli bir senaryo veya kimlik altında bilgi talep ettiği yöntem.

Örnek: Bir banka temsilcisi kılığına girerek, kullanıcının kimliğini doğrulamak için kişisel bilgilerini istemek.

#### Baiting (Yemleme)

Açıklama: Kullanıcıları zararlı yazılımlar içeren dosyaları indirmeye veya kötü amaçlı bağlantılara tıklamaya teşvik eden yöntem.

Örnek: Ücretsiz müzik veya film indirme vaadiyle kullanıcının kötü amaçlı bir dosyayı indirmesi.

#### Quid Pro Quo (Karşılıklı Çıkar)

Açıklama: Kullanıcıya bir hizmet veya fayda sunma karşılığında bilgi talep etme yöntemi.

Örnek: Teknik destek hizmeti sunuyormuş gibi davranarak, kullanıcının bilgisayarına erişim bilgilerini istemek.

#### Tailgating (Arkasına Takılma)

Açıklama: Yetkisiz bir kişinin, yetkili bir kişiyle birlikte güvenli bir alana girmesi yöntemi.

Örnek: Bir çalışan kapıyı açarken, saldırganın bu fırsatı değerlendirip bina içine girmesi.

#### Dumpster Diving (Çöp Karıştırma)

Açıklama: Önemli bilgilerin yer aldığı belgeleri, eski bilgisayar parçalarını veya diğer materyalleri aramak için çöpleri karıştırma yöntemi.

Örnek: Çöpte bulunan eski belgelerden veya elektronik cihazlardan kullanıcı adı, şifre ve diğer hassas bilgileri toplama.

### Sosyal Mühendislikten Korunma Yolları

* Eğitim ve Farkındalık: Çalışanları ve kullanıcıları sosyal mühendislik saldırıları konusunda eğitmek ve farkındalık yaratmak.
* Güçlü Kimlik Doğrulama: Çok faktörlü kimlik doğrulama (MFA) ve güçlü parolalar kullanmak.
* Şüpheli Talepleri Doğrulama: Bilgi talep eden kişilerin kimliğini doğrulamak için ek kontroller yapmak.
* Bilgi Paylaşımını Sınırlama: Hassas bilgileri yalnızca yetkili kişilere vermek ve bu bilgileri paylaşmadan önce dikkatli olmak.
* Güvenli Erişim Prosedürleri: Fiziksel ve dijital erişim kontrol önlemlerini uygulamak.
* Bilgisayar Güvenliği: Antivirüs yazılımları ve güvenlik duvarları kullanarak kötü amaçlı yazılımlara karşı korunmak.
* Düzenli Güvenlik İncelemeleri: Güvenlik politikalarını ve uygulamalarını düzenli olarak gözden geçirmek ve güncellemek.

## SİBER SALDIRI ANALİZİ NEDİR? FAYDALARI NELERDİR?

Siber saldırı analizi, bir siber saldırının nasıl gerçekleştiğini, saldırganların hangi yöntemleri ve araçları kullandığını, saldırının sistemlere ve verilere olan etkisini ve saldırıya karşı alınan önlemlerin etkinliğini belirlemek için yapılan detaylı inceleme sürecidir. Bu analiz, hem saldırının kaynağını tespit etmek hem de gelecekte benzer saldırılara karşı daha iyi koruma sağlamak amacıyla yapılır.

### Aşamaları

#### Saldırı Tespiti ve İzleme

Log Analizi: Sistem logları incelenir ve anormal aktiviteler belirlenir.

Güvenlik Bilgi ve Olay Yönetimi (SIEM) Sistemleri: Bu sistemler, güvenlik olaylarını gerçek zamanlı olarak izler ve analiz eder.

#### İlk Yanıt

Olay Müdahale Ekibi: Olayın türünü ve kapsamını belirlemek için acil müdahale ekibi devreye girer.

İzolasyon: Etkilenen sistemlerin daha fazla zarar görmesini önlemek için izolasyonu sağlanır.

#### Derinlemesine Analiz

Kök Neden Analizi (Root Cause Analysis): Saldırının temel nedenlerini ve nasıl gerçekleştirildiğini belirlemek.

Malware Analizi: Kötü amaçlı yazılımların analiz edilmesi ve bunların çalışma prensiplerinin anlaşılması.

Adli Bilişim (Digital Forensics): Etkilenen sistemlerdeki dijital delillerin toplanması ve incelenmesi.

#### Zarar Değerlendirmesi

Veri Kaybı ve Etkisi: Hangi verilerin çalındığı veya zarar gördüğü değerlendirilir.

Sistem Hasarı: Sistemlerin ve ağın ne derece zarar gördüğü belirlenir.

İyileştirme ve Düzeltici ÖnlemlerYamaların Uygulanması: Güvenlik açıklarını kapatmak için gerekli yazılım yamaları uygulanır.

Güvenlik Politikalarının Güncellenmesi: Mevcut güvenlik politikaları gözden geçirilir ve güncellenir.

Kullanıcı Eğitimi: Kullanıcılara güvenlik farkındalığı eğitimleri verilir.

#### Raporlama

Detaylı Rapor Hazırlama: Saldırının nasıl gerçekleştiği, alınan önlemler ve gelecekteki öneriler hakkında detaylı bir rapor hazırlanır.

Paydaşlarla Paylaşım: Rapor ilgili paydaşlarla, yönetimle ve gerekli durumlarda hukuki mercilerle paylaşılır.

#### Gelişmiş Savunma Stratejileri

Güvenlik Duvarlarının ve IDS/IPS Sistemlerinin Güncellenmesi: Saldırıyı tespit eden ve engelleyen sistemler güncellenir.

Ağ Segmentasyonu: Ağ trafiğini sınırlamak ve saldırıların yayılmasını önlemek için ağ segmentasyonu uygulanır.

Sürekli İzleme ve Tehdit İstihbaratı: Yeni tehditlere karşı sürekli izleme yapılır ve güncel tehdit istihbaratı kullanılır.

### SİBER SALDIRIANALİZİ FAYDALARI

#### Gelecekteki Saldırıları Önleme

Zayıf Noktaların Belirlenmesi: Sistemlerin ve ağların zayıf noktalarını tespit ederek bu açıkları kapatmak için gerekli önlemleri almayı sağlar.

Savunma Stratejilerinin İyileştirilmesi: Daha güçlü savunma mekanizmaları geliştirmek ve gelecekteki saldırılara karşı hazırlıklı olmak için bilgi sağlar.

#### Hızlı ve Etkili Müdahale

Erken Tespit ve Yanıt: Saldırıların erken tespiti ve hızlı müdahale ile zararların minimize edilmesini sağlar.

Olay Müdahale Planlarının Geliştirilmesi: Kurumların olay müdahale planlarını ve protokollerini geliştirmelerine yardımcı olur.

#### Veri ve Varlıkların Korunması

Veri Güvenliği: Hassas verilerin ve kritik varlıkların korunmasını sağlar.

Finansal Kayıpların Azaltılması: Saldırılardan kaynaklanan maddi zararları azaltarak finansal kayıpları en aza indirir.

#### Yasal Uyum ve Raporlama

Yasal Yükümlülüklerin Karşılanması: Yasal düzenlemelere ve endüstri standartlarına uyumu sağlar.

Hukuki Delil Sağlama: Hukuki süreçler için gerekli delillerin toplanmasını ve korunmasını sağlar.

#### İtibarın Korunması

Müşteri Güveninin Sağlanması: Hızlı ve etkili bir müdahale, müşterilerin güvenini korur ve işletmenin itibarını sürdürür.

İtibarın Güçlendirilmesi: Güçlü bir güvenlik duruşu, kurumun itibarını artırır ve rekabet avantajı sağlar.

#### Sürekli İyileştirme

Güvenlik Politikalarının Güncellenmesi: Mevcut güvenlik politikalarının ve prosedürlerinin güncellenmesini ve iyileştirilmesini sağlar.

Sürekli İzleme ve Gelişim: Sürekli izleme ve gelişim süreçlerinin bir parçası olarak güvenlik duruşunun sürekli iyileştirilmesine katkıda bulunur.

#### Eğitim ve Farkındalık

Kullanıcı Farkındalığını Artırma: Çalışanların ve kullanıcıların siber güvenlik tehditleri konusunda bilinçlenmesini sağlar.

Eğitim Programlarının Geliştirilmesi: Eğitim ve farkındalık programlarının geliştirilmesine yardımcı olur.

#### Organizasyonel Dayanıklılık

Risk Yönetimi: Organizasyonel risklerin daha iyi yönetilmesini sağlar ve kurumsal dayanıklılığı artırır.

İş Sürekliliği: İş süreçlerinin kesintisiz devam etmesini sağlar ve iş sürekliliği planlarının etkinliğini artırır.

## GÜVENLİK AÇIĞI

Güvenlik açığı, bir sistemin veya uygulamanın koruma mekanizmalarının zayıf veya eksik olduğu durumu ifade eder. Bu tür bir açık, kötü niyetli kişilerin sisteme izinsiz erişim sağlamasına veya hizmetin istenmeyen şekilde kullanılmasına neden olabilir.

Güvenlik açıkları, birçok farklı faktörden kaynaklanabilir. Yazılım hataları, tasarım hataları, zayıf şifreleme yöntemleri, kötü yapılandırma, güncelleme ve yama eksiklikleri, kullanıcı hataları veya kötü amaçlı yazılımların sistemlere sızması gibi faktörler, güvenlik açıklarının ortaya çıkmasına katkıda bulunabilir.

Güvenlik açıkları, bilgisayar sistemlerinde, ağlarda, web uygulamalarında, mobil uygulamalarda ve diğer bilgi teknolojilerinde bulunabilir. Bu açıklar, yetkisiz erişim, veri sızıntısı, kimlik avı (phishing), veri bozulması veya hizmet kesintisi gibi güvenlik ihlallerine yol açabilir.

Güvenlik açıklarının tespit edilmesi ve düzeltilmesi önemlidir. Bu genellikle siber güvenlik uzmanları, güvenlik testleri ve izleme süreçleri kullanılarak gerçekleştirilir. Güvenlik açıklarıyla mücadele etmek için, iyi bir güvenlik politikası oluşturulması, yazılım ve sistemlerin düzenli olarak güncellenmesi ve kullanıcıların bilinçlendirilmesi gibi önlemler alınabilir.

### Güvenlik Açığı Türleri Nelerdir

1- Zayıf Şifreler

Zayıf veya tahmin edilebilir şifreler, kötü niyetli kişilerin hesaplara yetkisiz erişim sağlamalarına olanak tanır.

2- Yazılım Hataları

Yazılım programlarında bulunan hatalar, siber saldırganların sisteme girmek veya yetkisiz işlemler gerçekleştirmek için kullanabilecekleri güvenlik açıklarına yol açabilir.

3- Güncelleme Eksikliği

İşletim sistemleri ve yazılımlar düzenli olarak güncellenmelidir. Eksik güncellemeler, bilinen güvenlik açıklarının saldırganlar tarafından istismar edilmesine olanak sağlayabilir.

4- Ağ Güvenliği Zafiyetleri

Ağ altyapısında veya ağa bağlı cihazlarda güvenlik açıkları olabilir. Bu açıklar, ağ trafiğinin izlenmesi, izinsiz erişim veya veri hırsızlığı gibi saldırılara yol açabilir.

5- Kimlik Doğrulama Zafiyetleri

Kötü niyetli kişilerin kimlik doğrulama mekanizmalarını aşmalarına veya yanıltmalarına olanak tanıyan güvenlik açıkları.

6- XSS (Cross-Site Scripting)

XSS güvenlik açığı, web uygulamalarında bulunabilir. Kötü niyetli kullanıcılar, kullanıcıların tarayıcılarında zararlı kodların çalışmasını sağlayarak kullanıcıları manipüle edebilir veya gizli bilgileri çalabilir.

7- SQL Enjeksiyonu

Bu açık, web uygulamalarına yapılan SQL sorgularının güvenli bir şekilde işlenmemesi sonucunda ortaya çıkar. Saldırganlar, SQL enjeksiyonu kullanarak veritabanına yetkisiz erişim sağlayabilir veya veri çalabilir.

8- Sosyal Mühendislik

Sosyal mühendislik, insanların güvenini kötüye kullanarak saldırılara girmek veya hassas bilgilere erişmek için manipülatif taktikler kullanma yöntemidir.

### Sistemlerde güvenlik açıkları nasıl tespit edilir?

1- Zafiyet Taramaları

Otomatik araçlar kullanarak bir sistem veya ağdaki bilinen güvenlik açıklarını tespit etmeyi amaçlar. Bu taramalar, açık portlar, güncelleme eksiklikleri, zayıf şifreler ve yaygın olarak bilinen zafiyetler gibi potansiyel riskleri belirlemek için kullanılabilir.

2- Penetrasyon Testleri

Bir sistem veya ağın güvenlik zaaflarını gerçek bir saldırgan gibi değerlendirmek amacıyla sızma testleri yapılır. Deneyimli güvenlik uzmanları, sistemdeki güvenlik açıklarını manuel olarak keşfetmeye çalışır ve saldırı senaryolarını simüle eder. Bu testler, gerçek dünya saldırılarını taklit ederek sistemin güvenlik düzeyini değerlendirmeye yardımcı olur.

3- Kaynak Kod İncelemesi

Yazılım güvenliğini değerlendirmek için kaynak kod incelemesi yapılabilir. Uzmanlar, yazılımın kaynak kodunu analiz ederek potansiyel hataları, zayıf noktaları veya kötü tasarımları tespit edebilir. Bu yöntem, özellikle özel veya kritik uygulamalar için kullanışlıdır.

4- Log İncelemesi

Sistem ve ağ logları, olası güvenlik açıklarının tespit edilmesinde önemli bir kaynaktır. Loglar, şüpheli faaliyetleri, giriş denemelerini veya anormal davranışları belirleyebilir ve potansiyel güvenlik sorunlarını gösterebilir.

5- Sosyal Mühendislik Testleri

Sosyal mühendislik testleri, kullanıcıların güvenlik bilincini ve tepkilerini değerlendirmek için kullanılır. Bu testler, telefonla arama, sahte e-posta gönderme veya fiziksel erişim denemeleri gibi yöntemleri içerebilir.

6- Güvenlik İncelemeleri ve Denetimleri

Sistemlerin güvenlik politikaları, yapılandırmaları ve uygulamaları periyodik olarak gözden geçirilmelidir. Bu incelemeler, güvenlik standartlarına uyumu değerlendirebilir, gerektiğinde düzeltici eylemler belirleyebilir ve sürekli güvenlik iyileştirmeleri sağlayabilir.

### Güvenlik açıkları nasıl kapatılır?

* Yazılım sistemlerinin ve bileşenlerinin güncel olması çok önemlidir. Yazılım sağlayıcılarının yayınladığı güncellemeler düzenli olarak kontrol edilmeli ve sistemi en son güvenlik yamalarıyla güncellemek gerekir.
* Son kullanıcılar güçlü şifreler kullanmalı ve gerekirse şifre politikaları uygulanmalıdır. İki faktörlü kimlik doğrulama gibi ek güvenlik önlemleri kullanarak güvenliğin arttırılması gerekir.
* Kullanılmayan veya gereksiz hizmetler kapatılmalıdır. Çok sayıda ve gereksiz çalışan hizmetler saldırganların hedef olarak kullanabileceği potansiyel açıkları fazlalaştırır.
* Bir güvenlik duvarı kullanarak ağ trafiği izlenmeli ve istenmeyen/zararlı aktiviteler engellenmelidir. Ayrıca, saldırı tespit ve olay yönetimi (IDS/IPS) sistemleri ile ağdaki anormal aktiviteleri izlemek mevcut güvenlik açıklarını kapatmaya yardımcı olacaktır.
* Sistemleri düzenli olarak güvenlik açısından incelemek ve zayıf noktaları tespit etmek proaktif bir yaklaşım ile güvenlik açıklarını herhangi bir saldırıya maruz kalmadan kapatmak için önemli bir silahtır. Kod incelemeleri, penetrasyon testleri veya siber güvenlik danışmanlığı gibi yöntemler ile sistemlerde güvenlik maksimum düzeyde sağlanabilir.
* Olayları izlemek ve hızlı yanıt vermek için bir olay izleme ve yanıt planı oluşturmak, siber tehdit ile karşılaşıldığında ne yapılacağını planlı olarak ve hızlıca gerçekleştirebilmenizi sağlar. Güvenlik ihlalleri durumunda, etkin bir şekilde müdahale edebilmek için doğru prosedürleri belirleyip bunları uygulamak önemlidir.

## WEB SALDIRILARI NEDİR?

Web site saldırısı nedir? Siber suçlular, bilgisayar korsanları ve hackerlar tarafından; bilişim araç ve teknolojilerini (bilgisayar, telefon, tablet, internet, ağ, yazılım vb) farklı teknikler kullanılarak, belli bir amaca hizmet için yapılan saldırılarına denir. Web site saldırılarının çoğu maddi çıkar elde etmek için yapılmaktadır. Genellikle bu saldırıları gerçekleştiren kişiler web yazılımı, sunucu ve güvenlik odaklı açıklardan faydalanıp bu saldırıları yaparlar.

### Web sitelerinde güvenlik açıkları nasıl tespit edilir?

* Web sitesiyle ilişkili ağ trafiğini izlemek, saldırı girişimlerini veya anormal etkinlikleri tespit etmek için kullanılabilir. Ağ analizi araçları, veri paketlerini izlemek ve analiz etmek için kullanılır. Bu, saldırı girişimlerini veya güvensiz iletişimleri tespit etmek ve web sitesinin güvenlik açıklarını belirlemek için yardımcı olur.
* Web sunucusunun günlüklerini incelemek, saldırı girişimlerini veya anormal etkinlikleri belirlemeye yardımcı olur. Web günlükleri, potansiyel saldırılar veya güvenlik açıklarının izlerini taşıyabilir. Bu nedenle, günlükleri düzenli olarak incelemek, güvenlik açıklarını tespit etmek ve saldırılara karşı tepki vermek için önemlidir.
* Web sitesinin kod tabanını inceleyerek potansiyel güvenlik açıklarını bulmak için kod incelemesi yapılabilir. Geliştiriciler veya güvenlik uzmanları tarafından yapılabilir ve kötü niyetli aktörlerin potansiyel olarak istismar edebileceği güvenlik açıklarını tespit etmeye yardımcı olur. Web sitesindeki zafiyetler belirlendikten sonra önlemler alınarak iyileştirmelerin yapılması gerekmektedir.
* Sızma (penetrasyon) testi, güvenlik uzmanlarının web sitesini saldırgan bir bakış açısıyla test ettiği bir yöntemdir. Bu testler, güvenlik açıklarını manuel olarak tespit etmek ve saldırılara karşı direnci
* değerlendirmek için gerçekleştirilir. Sızma testi, daha sofistike ve hedefe yönelik saldırı senaryolarını içerir ve daha kapsamlı sonuçlar sağlar.
* Otomatik zafiyet tarama araçları, web sitelerinin güvenlik açıklarını tespit etmek için kullanılır. Bu araçlar, yaygın zafiyetlerin (örneğin SQL enjeksiyonu, XSS, güvenlik duvarı bypass gibi) bulunduğu noktaları taramak ve raporlamak için kullanılır. Açık kaynak veya ücretli/ücretsiz araçlarla zafiyet taramaları gerçekleştirilebilir.

En yaygın saldırılar aşağıda verilmiştir.

#### 1) Yansıtılmış XSS ​​(Kalıcı olmayan) saldırıları

Yansıtılmış (Reflected) XSS saldırıları, saldırıyı yapan tarafından, web sayfasına kötü amaçlı kodun enjekte edilmesi ve ardından sunucuda depolanmadan hemen kullanıcıya geri yansıtılması sonucu oluşur. Yansıtılan XSS saldırıyla, hedef kişilere e-posta mesajı, başka bir web sitesinden bağlantı gibi farklı yollarla link, form gibi bağlantılar iletilir. Bu kullanıcılar, kötü amaçlı bu bağlantılara tıklaması, form göndermesi veya yalnızca kötü amaçlı hazırlanmış bir siteye göz atması için farklı teşvik teknikleri kullanması sonucu; siteye enjekte edilen kod, saldırıyı kullanıcının tarayıcısına geri yansıtan savunmasız web sitesine gitmesini sağlar. Bu sayede, web tarayıcı kötü amaçlı kodu, güvenilir bir sunucudan geldiği için yürütür. Javascript dili kullanılan sitelerde, bu açığa çok rastlanmaktadır.

#### 2) Kalıcı XSS ​​saldırıları

Kalıcı (Depolanmış – Stored) XSS saldırısı; Saldırı yapan bilgisayar korsanı tarafından, kötü amaçlı kodu sayfaya enjekte etmesinin ardından sayfaya her erişim olduğunda ve yürütüleceği sunucuda depolandığında ortaya çıkar. Kod enjekte edilmiş bir form sayesinde, kullanıcının girmiş olduğu tüm bilgiler, saldırıyı yapanın yönlendirdiği sunucuya – veri tabanına kaydolur. bu saldırı türü ciddi olumsuz sonuçlar doğurabilir. çok tehlikelidir.

#### 3) DOM XSS Saldırıları

DOM (Document Object Model – Belge Nesne Modeli) XSS saldırısı; saldırıyı yapan bilgisayar korsanı, istemci komut dosyasının çalıştığı internet sitesinin tarayıcısında DOM değiştirerek yük enjekte eder. Web sayfası değişmez, fakat sayfada bulunan istemci tarafı kodu, kötü amaçlı kod değişiklikleriyle çalışır. Bu XSS saldırı türü de çok tehlikelidir.

##### XSS Saldırılarına Karşı Alınak Önlemler

* Web uygulaması güvenlik duvarı (WAF) kullanmak.
* Giriş, form vb için doğrulamak kullanmak. Sunucu tarafından işlenmeden önce, kötü amaçlı kod için kullanıcı verisinin kontrol edilmesi anlamına gelir.
* Özel karakterleri HTML varlık eşdeğerlerine dönüştüren çıktı kodlamasını kullanmak.
* Arama kutu girdisi, uygun kodlama kontrolünü içerecek şekilde sterilize etmek.
* Web site sunucusu geçersiz istekleri yönlendirecek şekilde ayarlamak.
* Web site sunucusu, eşzamanlı birden çok girişi tespit edebilir. Ve bu giriş oturumlarını sonlandırabilir şekilde ayarlamak.
* Web site sunucusu iki veya daha fazla farklı IP adresinden, eşzamanlı girişi tespit edebilir. Ve oturumları sonlandırabilir.
* Web sitesi daha önce kullanılan kredi kartı numarası, TC numarası gibi önemli bilgilerin sadece birkaç hanesini gösterebilir şekilde ayarlamak.
* Web sitesi kullanıcıların kayıt bilgilerini değiştirmeden önce, tekrar eski parolalarını girmelerini sağlamak .
* Web sitesinde İçerik Güvenlik Politikası‘nın pek çok farklı yönünü kullanmak ve sağlamak.
* Çerez HttpOnly bayrağı ile işaretlenerek JavaScript’in çereze erişimi engellemek.

#### 4) SQL Enjeksiyonu

SQL (Structured Query Language – Yapılandırılmış Sorgu Dili) web site kullanıcılarının veri tabanlarıyla bağlantı ve etkileşim kurmasını sağlayan bir sorgu dilidir. Oturum açma, form, sepetler vs genellikle bir SQL veri tabanına bağlanır. Örneğin; kullanıcılar, yöneticiler, editörler ad, şifre gibi bilgileri girerek bir web sitesinin korumalı bu alanlarında oturum açabilir. SQL bu almış olduğu ve veri tabanına kayıt edilen bu tür oturum açma, giriş bilgilerini bir sonraki oturum açma, giriş vs için işler. SQL enjeksiyonu çok ciddi bir güvenlik sorunu olmasının yanı sıra SQL veritabanı kullanan web sitesine, uygulamasına saldırmak için kullanılıyor.

SQL enjeksiyonu ise; arka planda (back-end) veri tabanına dayalı web siteleri ve uygulamalarına saldırmak için kullanılan bir saldırı türüdür. Bu saldırı için, web yazılım güvenlik açığından ve SQL dili özelliklerinden faydalanarak kod yerleştirme ve yürütme tekniğidir. Saldırgan SQL kodlarını silebilir, değiştirebilir, veri tabanını ele geçirebilir. Bu tür web site saldırısı – SQL enjeksiyonu saldırıları önlemek zordur. ancak veritabanınızı korumaya yardımcı olmak için atabileceğiniz birkaç adım vardır. En yaygın SQL enjeksiyonu web site saldırı türleri;

* In-Band SQL (Klasik SQL Saldırıları)
* Error-Based SQL (Hata tabanlı SQL Saldırıları)
* Union-Based SQL Saldırıları
* Inferential SQL Saldırıları
* Content-Based Blind SQL (İçerik tabanlı SQL Saldırıları)
* Time-Based Blind SQL (Zamana dayalı SQL Saldırıları)
* Out-of-Band SQL

#### 5) DDoS Web Site Saldırısı (Distrubuted Denial of Service Attack)

Dağıtılmış hizmet engelleme saldırısı olarak türkçeye çevrilen DDOS saldırısı; web sitesine sahte trafik sağlayıp, sürekli istek göndermesi sonucu internet sitesini kullanılmaz hale getirilmek için amaçlanan yıkıcı bir siber saldırıdır. Ağa bağlı web sitesinin alt yapısının bağlı olduğu hostun kapasite sınırlarında faydalanarak gerçekleştirilir. internet sitesine çok fazla sahte kullanıcı trafik isteği yapılması, web sunucunun kapasitesini ve çalışmasını engeller. Web hosting kullanıcı trafik limitini doldurmak için, birden fazla bilgisayara ihtiyaçları yoktur. Tek bilgisayardan, birden fazla istek gönderebilirler. Bazı DDoS web site saldırı türleri şu şekildedir.

* Volume Based DDoS Attack (Hacim Odaklı DDoS Saldırılar)
* Protocol Based DDoS Attack (Protokol Odaklı DDoS Saldırılar)
* Application Layer DDoS Attack (Uygulama Katmanlı DDoS Saldırılar)
* SYN Flood DDoS Saldırıları
* UDP Flood DDoS Saldırıları
* Ping of Death (PoD) Saldırıları
* Ping Flood Saldırıları

DDoS Web Site Saldırılarına Karşı Alınacak Önlemler

DDoS saldırılarını önlemek zor olabilir. Fakat bu saldırıları karşı önlem almak mümkün. Ama kesin çözüm değildir.

* Web sunucusunun saldırı esnasında, sahte trafiği bertaraf edecek DDoS koruması kullanabilirsiniz. Bu hizmeti, günümüzde hosting- sunucu hizmeti sağlayan şirketler sağlamaktadır.
* CDN (içerik dağıtım ağı) kullanılması tavsiye edilir. İnternet üzerindeki birden çok veri merkezinde bulunan dağınık ve geniş bir sunucu sistemi olduğu için web sitesi sunucuna yapılan saldırılardan, büyük çoğunlukta zarar görmeyecektir.
* Ağ sunucu altyapısının iyi tasarlanmış bir sisteme sahip olması önemlidir.
* Rate limiting ile aynı IP adresinden gelen, belirli bir süre içindeki maksimum istek sayısı belirlenir, bu sayede maksimum trafik değerini aşan IP engellenir.
* Sunucu sistem güncellemeleri aksatılmamalı ve tam yapılmalı.
* Anti virüs programları kullanılmalıdır.
* Güvenlik duvarının aktif hale getirilmesi ve kullanılması.
* E-posta filtrelerin kullanılması ve spam trafiğinin engellenmesi için ilgili ayarların yapılması.

#### 4) Parola Saldırıları (Password Spraying Attack)

Web site kullanıcılarının şifrelerinin, varsayılan veya çok kullanılan akılda kalıcı şifrelerden oluşturulmuş olmasından faydalanan bilgisayar korsanları tarafından yapılan siber saldırı türüdür. Kaba kuvvet saldırıları, parola püskürtme saldırıları olarakta bilinmektedir. En çok kullanılan parola saldırıları;

* Kaba Kuvvet Saldırıları
* Sözlük Saldırıları
* Sosyal Mühendislik Saldırıları

Parola Saldırılarına Karşı Alınacak Önlemler

* Tüm web tabanlı hesaplar için güçlü, benzersiz parolalar oluşturmak gerekir.
* Düzenli olarak parolaları yinelemek gerekir. Eski parolayı anımsatmamalı ve benzerlik olmaması gerekir.
* Google Şifre Yöneticisi gibi parola yöneticisi kullanılması tavsiye edilir. Şifre yöneticisi sayesinde, güvenli parola oluşturma, yönetme ve saklama aracı olmasından dolayı, parola püskürtme siber saldırılarını durdurmanın en etkili ve en kolay yollarından biridir.
* iki faktörlü kimlik doğrulama giriş yöntemini kullanarak, bir hesaba şifreli girişin yanında kod, desen gibi sizin yönetiminizde olan cihazların fiziksel temas özelliklerini kullanarak giriş yapılabilir.

parola saldırılarına karşı alınabilecek bu önlemlere ek birçok yöntem vardır.

#### 5) Kimlik Avı Saldırıları

Kimlik avı saldırısı, web sitesi kullanıcı oturum açma bilgileri, bankacılık sistemine giriş bilgileri, içerik yönetim sistemi yönetici bilgileri gibi önemli bilgileri çalmak, kaydetmek, aktarmak için yapılan bir siber saldırıdır.

Kimlik avı saldırılarında kullanılan yöntemler benzerlik gösterir. Örneğin, güvenilir bir kurumdan gelen maillere benzer e-postalar gönderilmesi ve ardından mağdurun bu maili dikkate almasını sağlamak. En çok kullanılan yöntemler arasında yer alıyor. Kişi bu mail içeriğindeki bir bağlantı linki ile gitmiş olduğu sahte web sayfasındaki giriş bölümlerini tamamlaması sonrasındaki süreç ile saldırganın tüm bilgiye ulaşması sağlanmış olunur.

Kimlik Avı Saldırılarına Karşı Alınacak Önlemler

* Size gelen yönlendirici içeriği hassasiyetle inceleyin.
* Link/URL yapısını kontrol edin.
* E-posta uzantısını araştırın, uzantının karşılığı bir dijital veya kurumsal içerik var mı? yok mu? Bu önemli.
* Eğer yönlendirilen site içeriği uygun görünüyor olsa bile URL’de https güvenlik protokolü var mı diye kontrol edin.
* Web tabanlı tarama yapan, anti virüs yazılımları kullanın.
* Yazılı içeriklerinde kullanılan dil yapısı, kurallarına da dikkat ederseniz. Hatalar yakalamanız mümkün.

## SOLUCAN(WORM)

Solucan (worm), bilgisayar ağları üzerinden kendini çoğaltabilen ve yayılabilen, kötü amaçlı bir yazılım türüdür. Solucanlar, bir sisteme girdikten sonra kullanıcı müdahalesi gerektirmeden kendini çoğaltır ve diğer sistemlere yayılır. Bu tür yazılımlar, genellikle bilgisayar ağlarına zarar vermek, ağ trafiğini artırmak, sistem kaynaklarını tüketmek veya daha ciddi saldırılara zemin hazırlamak amacıyla kullanılır.

### Solucanların Özellikleri ve Çalışma Prensibi

* Bağımsız Çalışma: Solucanlar, bir virüsün aksine, başka bir dosyaya veya programa ihtiyaç duymadan kendi başlarına çalışabilirler.
* Ağ Üzerinden Yayılma: Solucanlar, ağ bağlantılarını kullanarak kendilerini diğer sistemlere yayarlar. Bu yayılma genellikle e-posta, ağ paylaşımı, veya güvenlik açıklarından yararlanarak gerçekleşir.
* Kendi Kendine Çoğalma: Solucanlar, bir sisteme bulaştıktan sonra otomatik olarak kendilerini kopyalayarak diğer sistemlere bulaşırlar.
* Sistem Kaynaklarını Tüketme: Solucanlar, sistem belleğini, CPU gücünü ve ağ bant genişliğini tüketerek sistem performansını ciddi şekilde düşürebilirler.
* Kötü Amaçlı Yükler: Bazı solucanlar, sadece yayılmakla kalmayıp aynı zamanda arka kapılar (backdoors) açabilir, casus yazılımlar yükleyebilir veya veri çalabilir.

### Solucan Türleri ve Yayılma Yöntemleri

* E-posta Solucanları: Bu solucanlar, kendilerini e-posta ekleri olarak gönderirler. Bir kullanıcı bu eki açtığında solucan aktif hale gelir ve kendini kullanıcıdaki e-posta adreslerine gönderir.
* Ağ Solucanları: Bu solucanlar, ağ bağlantıları ve güvenlik açıkları aracılığıyla yayılır. Genellikle işletim sistemi veya ağ hizmetlerindeki zayıf noktaları hedef alır.
* Dosya Paylaşım Solucanları: Bu solucanlar, paylaşılan dosya ve klasörlerde kendilerini kopyalayarak yayılırlar.
* Mesajlaşma Solucanları: Anlık mesajlaşma servisleri üzerinden yayılırlar. Kullanıcılar, zararlı bağlantılara tıkladığında veya dosyaları indirdiğinde solucan aktif hale gelir.

### Ünlü Solucan Örnekleri

* Morris Solucanı (1988): İnternet üzerindeki ilk büyük solucan saldırısı olarak bilinir. Bir üniversite öğrencisi tarafından yazılmış olup, internetin %10'una yakınını etkileyerek büyük bir hasar yaratmıştır.
* ILOVEYOU Solucanı (2000): E-posta yoluyla yayılan ve dünya çapında milyonlarca bilgisayara bulaşan bir solucandır. Büyük maddi zararlar yaratmıştır.
* Conficker Solucanı (2008): Microsoft Windows işletim sistemlerindeki bir güvenlik açığından yararlanarak yayılan bu solucan, dünya genelinde milyonlarca bilgisayarı etkiledi.
* Stuxnet Solucanı (2010): İran’ın nükleer programını hedef alarak santrifüjleri bozmak amacıyla geliştirilmiş karmaşık bir solucandır. Sanayi kontrol sistemlerine odaklanan ilk kötü amaçlı yazılım olarak bilinir.

### Solucanlardan Korunma Yöntemleri

* Güncellemeler ve Yamalar: İşletim sistemi ve yazılımlarınızın güncel olduğundan emin olun. Güvenlik açıklarını kapatan yamaları düzenli olarak uygulayın.
* Antivirüs ve Antimalware Yazılımları: Güvenilir antivirüs ve antimalware yazılımları kullanarak sisteminizi koruyun. Bu yazılımların güncel olduğundan emin olun.
* Güvenlik Duvarları: Güvenlik duvarları kullanarak ağ trafiğinizi kontrol edin ve izinsiz erişimleri engelleyin.
* E-posta ve Mesajlaşma Güvenliği: E-posta eklerine ve mesajlaşma uygulamalarında paylaşılan bağlantılara dikkat edin. Şüpheli e-postaları ve mesajları açmaktan kaçının.
* Eğitim ve Farkındalık: Çalışanları ve kullanıcıları siber güvenlik tehditleri ve korunma yolları konusunda eğitin.
* Ağ İzleme ve Analiz: Ağ trafiğinizi izleyerek anormal aktiviteleri tespit edin ve gerekli önlemleri alın.

## TRUVA ATI (TROJAN HORSE)

Truva Atı (Trojan Horse), adını Antik Yunan mitolojisindeki Truva Savaşı'ndan alan, zararlı yazılımların bir türüdür. Kullanıcının farkında olmadan bir bilgisayara veya ağa zararlı yazılım yüklemesine neden olan, genellikle meşru veya yararlı bir yazılım gibi görünen bir programdır. Truva Atı, doğrudan kendini kopyalayamaz veya yayamaz, ancak kötü amaçlı işlevlerini gizlice yerine getirmek için kullanılır.

### Truva Atı'nın Özellikleri

* Gizlilik: Truva Atları, genellikle meşru yazılımlar veya dosyalar gibi görünerek kullanıcının güvenini kazanır.
* Kötü Amaçlı İşlevler: Sistemlere arka kapılar açmak, hassas bilgileri çalmak, diğer kötü amaçlı yazılımları indirmek veya sistemleri uzaktan kontrol etmek gibi işlevlere sahiptir.
* Çoğalmama: Virüslerin ve solucanların aksine, Truva Atları kendi kendini çoğaltmaz. Ancak, bir kez sisteme girdiklerinde, saldırganların başka zararlı yazılımlar yüklemesine olanak tanır.

### Truva Atı Türleri

* Arka Kapı (Backdoor) Truva Atı: Sisteme gizlice giriş yaparak saldırganların bilgisayara uzaktan erişim ve kontrol sağlamasına olanak tanır.
* Bankacılık Truva Atı: Finansal bilgileri hedef alarak kullanıcıların banka hesap bilgilerini çalar.
* İndirme Truva Atı (Downloader): Diğer kötü amaçlı yazılımları bilgisayara indirip kuran Truva Atı türüdür.
* Casus Yazılım (Spyware): Kullanıcının etkinliklerini izleyerek gizli bilgileri toplar.
* Kötü Amaçlı Reklam Yazılımı (Adware): İstenmeyen reklamlar göstererek kullanıcıları rahatsız eder ve bazen daha fazla zararlı yazılım indirir.
* Kilitli Ekran (Ransomware) Truva Atı: Kullanıcının bilgisayarını veya dosyalarını kilitleyerek, erişim sağlamak için fidye talep eder.

### Truva Atı'nın Çalışma Prensibi

* Sosyal Mühendislik: Kullanıcıların Truva Atını indirmesi veya çalıştırması için kandırma teknikleri kullanılır. Örneğin, çekici e-postalar, sahte web siteleri veya pop-up reklamlar kullanılarak kullanıcılar tuzağa düşürülür.
* Gizli Yükleme: Truva Atı, genellikle bir yazılımın veya dosyanın parçası olarak gizlenir ve kullanıcı tarafından çalıştırıldığında etkin hale gelir.
* Sistemi Tehlikeye Atma: Truva Atı, kötü amaçlı işlevlerini yerine getirmek için sisteme arka kapılar açar, bilgileri çalar veya başka zararlı yazılımları indirir.
* Uzaktan Kontrol: Saldırganlar, Truva Atı aracılığıyla bilgisayarı uzaktan kontrol edebilir, dosyaları yönetebilir ve diğer kötü amaçlı faaliyetleri gerçekleştirebilir.

### Truva Atı'ndan Korunma Yolları

* Güvenilir Yazılım ve Kaynaklar Kullanma: Yazılımları ve dosyaları yalnızca güvenilir ve resmi kaynaklardan indirin.
* Antivirüs ve Güvenlik Yazılımları: Güncel antivirüs ve güvenlik yazılımları kullanarak Truva Atlarını tespit edin ve kaldırın.
* Güncellemeler ve Yamalar: İşletim sistemi ve yazılımların güncel olduğundan emin olun. Güvenlik yamalarını düzenli olarak uygulayın.
* Eğitim ve Farkındalık: Çalışanları ve kullanıcıları sosyal mühendislik saldırıları ve Truva Atları hakkında bilinçlendirin.
* E-posta ve İnternet Güvenliği: Şüpheli e-postaları açmaktan ve bilinmeyen bağlantılara tıklamaktan kaçının. İnternette gezinirken dikkatli olun.
* Güvenlik Duvarları: Güvenlik duvarları kullanarak ağ trafiğini kontrol edin ve izinsiz erişimleri engelleyin.

## CASUS YAZILIM (SPYWARE)

Casus yazılım (spyware), kullanıcıların bilgisayarlarını izlemek, bilgilerini toplamak ve bu bilgileri saldırganlara göndermek amacıyla kullanılan kötü amaçlı bir yazılım türüdür. Casus yazılım genellikle kullanıcıların bilgisi ve izni olmadan sistemlere sızar ve gizlice çalışır. Bu tür yazılımlar, özellikle kişisel verilerin ve gizliliğin ihlali açısından büyük tehditler oluşturur.

### Casus Yazılım Türleri

#### Anahtar Kaydediciler (Keyloggers)

Tanım: Kullanıcının klavye tuş vuruşlarını kaydederek şifreler, kredi kartı numaraları ve diğer hassas bilgileri toplar.

Kullanım Amacı: Genellikle finansal bilgiler ve oturum açma bilgilerini çalmak için kullanılır.

#### Tarayıcı Casus Yazılımları (Browser Hijackers)

Tanım: Web tarayıcılarının ayarlarını değiştirerek, varsayılan ana sayfa, arama motoru ve yeni sekme sayfalarını değiştiren yazılımlardır.

Kullanım Amacı: Kullanıcıyı istenmeyen veya zararlı web sitelerine yönlendirerek reklam geliri elde etmek veya zararlı yazılımlar indirmek.

#### Adware

Tanım: İstenmeyen reklamlar göstererek kullanıcıları rahatsız eder ve bazen daha fazla zararlı yazılım indirir.

Kullanım Amacı: Reklam gelirleri elde etmek ve kullanıcı davranışlarını izlemek.

#### Sistem İzleyiciler

Tanım: Kullanıcının sistem faaliyetlerini izleyerek ekran görüntüleri alır, uygulama kullanımı ve diğer aktiviteleri kaydeder.

Kullanım Amacı: Genellikle kurumsal casusluk veya kişisel bilgi toplama için kullanılır.

#### İzleme Çerezleri (Tracking Cookies)

Tanım: Kullanıcının internet üzerindeki gezinti alışkanlıklarını izleyen küçük veri dosyalarıdır.

Kullanım Amacı: Genellikle pazarlama ve reklamcılık amacıyla kullanıcı profilleri oluşturmak için kullanılır.

### Casus Yazılımın Çalışma Prensibi

* Gizli Kurulum: Casus yazılımlar, genellikle kullanıcı fark etmeden bilgisayara yüklenir. Bu, ücretsiz yazılımlar, e-posta ekleri veya sahte yazılım güncellemeleri yoluyla gerçekleşebilir.
* Bilgi Toplama: Yüklendikten sonra, casus yazılım sistem üzerinde çeşitli bilgileri toplar. Bu bilgiler kullanıcı etkinlikleri, tuş vuruşları, ziyaret edilen web siteleri ve kişisel veriler olabilir.
* Veri Gönderme: Toplanan bilgiler, saldırganın kontrol ettiği uzak bir sunucuya gönderilir.
* Sürekli İzleme: Casus yazılım, kullanıcının faaliyetlerini sürekli olarak izler ve yeni bilgiler toplar. Bu, yazılımın kaldırılmadığı sürece devam eder.

### Casus Yazılımdan Korunma Yolları

#### Güvenlik Yazılımları Kullanma

Antivirüs ve Antispyware: Güvenilir antivirüs ve antispyware yazılımları kullanarak sistemi düzenli olarak tarayın.

Güncellemeler: Antivirüs yazılımınızı ve diğer güvenlik yazılımlarınızı güncel tutun.

#### Dikkatli İnternet Kullanımı

Şüpheli Bağlantılardan Kaçınma: Bilinmeyen veya güvenilmeyen e-posta eklerini ve bağlantıları açmaktan kaçının.

Güvenilir Kaynaklardan İndirme: Yazılımları yalnızca resmi ve güvenilir kaynaklardan indirin.

#### Tarayıcı Güvenliği

Eklentiler ve Eklenti Yönetimi: Tarayıcınıza yalnızca güvenilir eklentileri yükleyin ve düzenli olarak eklenti yönetimi yapın.

Güvenlik Ayarları: Tarayıcınızın güvenlik ayarlarını yüksek seviyede tutun.

#### Güncellemeler ve Yamalar

İşletim Sistemi ve Yazılımlar: İşletim sistemi ve diğer yazılımlarınızı güncel tutun. Güvenlik açıklarını kapatan yamaları düzenli olarak uygulayın.

#### Kullanıcı Eğitimi ve Farkındalık

Eğitim Programları: Çalışanlarınızı ve kullanıcılarınızı casus yazılım ve diğer siber tehditler hakkında eğitin.

Güvenlik Farkındalığı: Kullanıcıların güvenlik farkındalığını artırarak, sosyal mühendislik saldırılarına karşı dikkatli olmalarını sağlayın.

## DDOS

Dağıtılmış Ağ Saldırıları, genellikle Dağıtılmış Hizmet Reddi (DDoS) saldırıları adıyla bilinir. Bu tür saldırılar, bir şirketin web sitesini sağlayan altyapı gibi, herhangi bir ağ kaynağı için geçerli olan belirli kapasite sınırlarından faydalanır. DDoS saldırısı, saldırıya uğrayan web kaynağına birden çok istek göndererek web sitesinin çok sayıda isteği işleme kapasitesini aşmayı ve doğru şekilde çalışmasını engellemeyi amaçlar.

DDoS saldırılarının tipik hedefleri arasında şunlar bulunur:

* İnternet alışveriş siteleri
* Online kumarhaneler
* Online hizmetler sağlamaya dayanan tüm işletme veya kuruluşlar

### DDoS saldırısı nasıl işler?

Web sunucuları gibi ağ kaynaklarının eş zamanlı olarak hizmet verebileceği isteklerin sayısı sınırlıdır. Sunucunun kapasite sınırına ek olarak sunucuyu internete bağlayan kanal da sınırlı bir bant genişliğine/kapasiteye sahiptir. İstek sayısı altyapıdaki herhangi bir bileşenin kapasite sınırını her aştığında hizmet düzeyi büyük olasılıkla aşağıdaki sorunlardan biriyle karşılaşır:

* İsteklere verilen yanıtlar normalden çok daha yavaş olur.
* Bazı (veya tüm) kullanıcı istekleri tamamen yoksayılabilir.

Genellikle saldırganın başlıca amacı web kaynağının normal çalışmasını tamamen engellemek, yani tam "hizmet reddi" sağlamaktır. Saldırgan, saldırıyı durdurması karşılığında para da isteyebilir. Bazı durumlarda DDoS saldırısı rakip bir firmanın itibarını zedeleme ya da işine zarar verme girişimi niteliğinde de olabilir.

### DDoS Saldırılarının Çeşitleri

* Hacim Temelli Saldırılar (Volume-Based Attacks)

Örnekler: ICMP (Ping) Flood, UDP Flood

Amaç: Aşırı trafikle bant genişliğini doldurmak.

* Protokol Saldırıları (Protocol Attacks)

Örnekler: SYN Flood, Ping of Death

Amaç: Hedef sistemin kaynaklarını (örneğin, bellek, CPU) tüketmek.

* Uygulama Katmanı Saldırıları (Application Layer Attacks)

Örnekler: HTTP Flood, Slowloris

Amaç: Uygulama veya web sunucusunu hedef alarak hizmetlerin yanıt verme yeteneğini bozmak.

### DDoS Saldırılarının Belirtileri

* Ağ Hızı Düşüşü: İnternet bağlantısında yavaşlama.
* Web Sitesi Erişim Sorunları: Web sitesine veya belirli sayfalara erişimde zorluk.
* Hizmet Kesintileri: Sunucuların veya hizmetlerin tamamen kullanılamaz hale gelmesi.
* Anormal Trafik Artışı: Sistem veya ağ trafiğinde beklenmedik ve aşırı artış.

### DDoS Saldırılarından Korunma Yolları

#### Ağ İzleme ve Trafik Analizi

Gerçek Zamanlı İzleme: Ağ trafiğini gerçek zamanlı izleyerek anormal aktiviteleri tespit edin.

Trafik Analizi: Olağandışı trafik desenlerini tanımlayabilen analiz araçları kullanın.

#### Yük Dengeleme (Load Balancing)

Trafik Yönlendirme: Yük dengeleme cihazları ve teknikleri kullanarak trafiği birden fazla sunucuya yönlendirin.

Anycast Yönlendirme: Trafiği coğrafi olarak dağıtarak yükü hafifletin.

#### Saldırı Tespit ve Önleme Sistemleri (IDS/IPS)

İzinsiz Giriş Tespit ve Önleme: IDS/IPS sistemleri kullanarak DDoS saldırılarını tespit edin ve önleyin.

Güvenlik Duvarı Kuralları: Güvenlik duvarı kurallarını güncelleyerek kötü amaçlı trafiği engelleyin.

#### Bulut Tabanlı DDoS Koruma Hizmetleri

DDoS Koruma Sağlayıcıları: Cloudflare, Akamai gibi DDoS koruma hizmetleri sunan sağlayıcılardan yararlanın.

Trafik Temizleme: Trafiği bulut tabanlı temizleme merkezlerine yönlendirerek kötü amaçlı trafiği filtreleyin.

#### Ağ Donanımı ve Yapılandırma

Yedekli Altyapı: Yedekli ağ ve sunucu altyapısı oluşturarak saldırı sırasında hizmet sürekliliğini sağlayın.

Router ve Switch Ayarları: Router ve switch’lerde trafik limitleri ve filtreleme kuralları uygulayın.

#### Uygulama ve Yazılım Güvenliği

Web Uygulama Güvenlik Duvarı (WAF): Web uygulama güvenlik duvarları kullanarak uygulama katmanı saldırılarını engelleyin.

Güncellemeler ve Yamalar: Yazılımlarınızı ve uygulamalarınızı düzenli olarak güncelleyerek bilinen güvenlik açıklarını kapatın.

#### Acil Durum Planları ve Tatbikatlar

Olay Müdahale Planları: DDoS saldırılarına karşı acil durum müdahale planları oluşturun.

Tatbikatlar ve Eğitim: Çalışanlarınızı ve IT ekibinizi düzenli tatbikatlarla eğiterek hazırlıklı olmalarını sağlayın.

### DDoS Saldırısına Karşı Hızlı Müdahale Adımları

* Durumu Değerlendirme: Saldırının türünü ve etkisini hızlı bir şekilde değerlendirin.
* Trafik Filtreleme: Mümkünse saldırı trafiğini filtrelemek veya azaltmak için anında önlemler alın.
* Servis Sağlayıcıları ile İletişim: İnternet servis sağlayıcıları veya bulut DDoS koruma hizmetleriyle hemen iletişime geçin.
* Kayıt ve Raporlama: Olayı kaydedin ve saldırının detaylarını belgeleyerek gelecekteki analiz ve iyileştirme çalışmaları için raporlayın.

## SON ZAMANLARDA GERÇEKLEŞEN ÖNEMLİ İNTERNET SALDIRILARI

* Fransız Devlet DDoS Saldırısı: Mart 2024'te, Fransız devlet hizmetleri büyük bir DDoS saldırısına maruz kaldı. Bu saldırı, 300'den fazla web alanı ve 177.000 IP adresini etkiledi. Başbakan Gabriel Attal’ın ofisi bu saldırıyı “benzeri görülmemiş bir yoğunlukta” olarak tanımladı. Hacker grubu Anonymous Sudan bu saldırının sorumluluğunu üstlendi​.
* Change Healthcare Fidye Yazılımı Saldırısı: Şubat 2024'te, ABD'deki en büyük sağlık ödeme işleyici olan Change Healthcare büyük bir fidye yazılımı saldırısına uğradı. Bu saldırı, sağlık hizmeti sağlayıcılarının hastalardan ödeme almasını haftalarca engelledi ve günlük yaklaşık 100 milyon dolar kayba yol açtı. ALPHV/BlackCat adlı ransomware grubu bu saldırının sorumluluğunu üstlendi​.
* İngiltere Savunma Bakanlığı Maaş Sistemine Saldırı: Mayıs 2024'te, İngiltere Savunma Bakanlığı'nın maaş sistemi hacklendi. Bu saldırı, 270.000 mevcut ve eski personelin kişisel verilerini açığa çıkardı. Hükümet, saldırının Çin tarafından gerçekleştirildiğinden şüpheleniyor​.
* NHS Scotland Fidye Yazılımı Saldırısı: Mart 2024'te, İskoçya'nın NHS Dumfries and Galloway sağlık hizmeti, Inc Ransomware Group tarafından saldırıya uğradı. Saldırganlar, hastalar ve personel hakkında 3 terabaytlık hassas veriyi çaldı ve bu verileri yayınladı​.
* Mother of All Breaches (MOAB): 2024'ün başında gerçekleşen bu olay, 26 milyar kaydı içeren 12 terabaytlık devasa bir veri sızıntısını içeriyordu. Bu veri sızıntısı, LinkedIn, Twitter, Weibo ve Dropbox gibi büyük platformlardan toplanan verileri içeriyordu​.

## RANSOMWARE

Kullanıcıların veya organizasyonların bilgisayar sistemlerine sızarak dosyalarını şifreleyen ve ardından bu dosyaların yeniden erişilebilir hale gelmesi için fidye talep eden bir tür kötü amaçlı yazılımdır. Fidye yazılımı, genellikle zararlı e-posta ekleri, kötü niyetli web siteleri veya sahte yazılım güncellemeleri aracılığıyla yayılır.

### Fidye Yazılımının Türleri

### Kripto Fidye Yazılımı (Crypto Ransomware):

Özellikleri: Dosyaları şifreler ve kullanıcıların bu dosyalara erişimini engeller.

Örnekler: CryptoLocker, WannaCry.

### Kilitleme Fidye Yazılımı (Locker Ransomware):

Özellikleri: Kullanıcının cihazının ekranını veya belirli işlevlerini kilitler.

Örnekler: Police Locker, Winlocker.

### Scareware:

Özellikleri: Sahte güvenlik yazılımları veya uyarılar göstererek kullanıcıyı korkutur ve fidye ödemesini talep eder.

Örnekler: FakeAV.

### Doxware:

Özellikleri: Kullanıcıların hassas verilerini çalar ve bu verileri ifşa etme tehdidinde bulunur.

Örnekler: RansomWeb.

### Fidye Yazılımının Çalışma Prensibi

* Sistemlere Sızma: Fidye yazılımı, genellikle kullanıcıların e-posta ekleri veya kötü amaçlı yazılım içeren bağlantılar yoluyla cihazlarına bulaşır.
* Şifreleme: Fidye yazılımı, cihazdaki dosyaları veya sistemin tamamını şifreler.
* Fidye Talebi: Kullanıcıya bir mesaj gösterilir ve bu mesajda dosyaların geri alınabilmesi için belirli bir miktar fidye ödenmesi istenir. Ödeme genellikle Bitcoin gibi izlenmesi zor dijital para birimleri ile yapılır.
* Ödeme ve Şifre Çözme: Kullanıcı fidye öderse, saldırganlar genellikle bir şifre çözme anahtarı sağlar, ancak bu her zaman gerçekleşmez.

### Fidye Yazılımından Korunma Yolları

#### Güncellemeler ve Yamalar:

Yazılımlarınızı ve işletim sisteminizi düzenli olarak güncelleyin ve güvenlik yamalarını uygulayın.

#### Güvenilir Antivirüs Yazılımları:

Güvenilir antivirüs ve antimalware yazılımları kullanarak düzenli taramalar yapın.

#### Yedekleme:

Verilerinizi düzenli olarak yedekleyin ve bu yedekleri çevrimdışı ve güvenli bir yerde saklayın.

#### Eğitim ve Farkındalık:

Çalışanlarınızı ve kullanıcılarınızı şüpheli e-postalar ve bağlantılar konusunda eğitin.

#### E-posta ve Web Filtreleme:

E-posta ve web trafiğini filtreleyerek kötü amaçlı içerikleri engelleyin.

#### Güvenlik Duvarı ve IDS/IPS:

Güvenlik duvarı ve izinsiz giriş tespit/önleme sistemleri kullanarak ağ trafiğini izleyin ve şüpheli aktiviteleri engelleyin.

### Örnek Fidye Yazılım Saldırıları

* WannaCry: 2017'de dünya genelinde birçok kuruluşu etkileyen büyük bir fidye yazılım saldırısıdır. Hızla yayılarak birçok önemli sistemi etkiledi.
* NotPetya: 2017'de Ukrayna'da başlayıp küresel ölçekte yayılmış bir fidye yazılımıdır. Finansal ve lojistik sektörlerde ciddi hasarlara yol açmıştır.

# KAYNAKÇA

<https://dergipark.org.tr/tr/pub/dpuiibf/issue/68606/1076685>

<https://turk.net/blog/siber-saldiri-nedir/>

<https://dergipark.org.tr/tr/download/article-file/505144#:~:text=Bilgisayar%20ve%20internet%20konusunda%20profesyonel,(Milliyet%20Gazetesi%2C%2020>

<https://tubitak.gov.tr/sites/default/files/25506/siber_guvenlik_lise.pdf>

<https://dergipark.org.tr/en/download/article-file/209001>

<https://techmonitor.ai/technology/cybersecurity/biggest-cyberattacks-of-2024>

<https://www.techopedia.com/biggest-data-breaches-and-cyber-hacks>