BÖLÜM 1

GÜVENLİĞİN TEMEL UNSURLARI

ANAHTAR KAVRAMLAR

Bilgi Güvenliği, Gizlilik, Bütünlük, Kullanılabilirlik, Kimlik Doğrulama, Parola Güvenliği, Saldırı, Saldırgan

ÖĞRENME HEDEFLERİ

1. Güvenliğin temel unsurlarını açıklar
2. Güvenlikle ilgili temel terimlerin anlamını bilir
3. Güvenli ve güçlü parola oluşturur
4. Zararlı yazılımları açıklar
5. Türk spor politikasını açıklama
6. Yaygın kullanılan saldırı türlerini açıklar
7. Sosyal mühendislik saldırılarından korunma yöntemlerini uygular
8. Saldırganların kimler olduğunu açıklar

BİRİNCİ BÖLÜM

GİRİŞ

Günümüzde dijital dünya, hızla gelişen teknolojiyle birlikte hayatımızın vazgeçilmez bir parçası haline gelmiştir. İnternet, mobil cihazlar ve bilgisayarlar aracılığıyla saniyeler içinde dünyanın dört bir yanındaki bilgilere erişmemizi sağlar. Bu durum, bilgiye ulaşmanın kolaylaşmasıyla birlikte bilgi güvenliği konusunu da gündeme getirmiştir. Bilgi güvenliği, kişisel verilerin, finansal bilgilerin ve diğer hassas verilerin yetkisiz erişim, değişim, açıklama, engelleme veya imha edilmesine karşı korunmasını içerir. Bilgi güvenliği kavramı, sadece bireysel düzeyde değil, işletmeler, kuruluşlar ve devletler için de hayati öneme sahiptir.

Bilgi güvenliğinin neden öğrenilmesi gerektiğine dair en önemli sebeplerden biri, dijital tehditlerin giderek yaygınlaşması ve sofistike hale gelmesidir. Siber suçlar, kötü niyetli yazılımlar ve veri sızıntıları gibi tehditler, bireylerin ve organizasyonların güvenliğini ciddi şekilde tehlikeye atabilir. Bilgi güvenliği bilinci, kişisel ve kurumsal düzeyde riskleri anlama, önleme ve azaltma yeteneği sağlar. Ayrıca, bilgi güvenliği eğitimi, dijital dünyada güvenli davranışlar geliştirmemize yardımcı olur. Bu bilgi birikimi, hem bireysel gizliliğimizi korumak hem de toplumsal düzeyde daha güvenli bir dijital ortam oluşturmak için kritik öneme sahiptir. Bu nedenle, bilgi güvenliği konusunda bilinçli olmak ve bu alandaki bilgi ve becerilerimizi sürekli olarak güncellemek, dijital dünyada başarılı ve güvenli bir şekilde var olmamızı sağlamak için kaçınılmazdır.

1. TEMEL GÜVENLİK KAVRAMLARI

Bilgi güvenliği, dijital dünyada bireylerin ve organizasyonların güvenliğini sağlamak için temel taşlardan biridir. Bu güvenliği anlayabilmenin ve sağlayabilmenin ilk adımı, temel güvenlik kavramlarını bilmekten geçer. Güvenliğin temel kavramları, kişisel ve kurumsal verilerin korunması için zorunludur. Bu kavramlar, yetkisiz erişimden korunma, veri bütünlüğü, gizlilik, kimlik doğrulama ve şifreleme gibi unsurları içerir. Bu kavramlar, kullanıcıların dijital ortamlarda karşılaşabileceği tehditleri anlamalarını ve bu tehditlere karşı nasıl korunacaklarını bilerek güvenli davranışlar geliştirmelerine yardımcı olur. Aynı zamanda, organizasyonlar için bu kavramlar, müşteri güveni ve rekabet avantajı sağlamak açısından kritiktir. Temel güvenlik kavramlarını bilmek, siber tehditlere karşı savunma mekanizmalarını anlamak ve güvenliğin karmaşıklığını yönetmek için hayati öneme sahiptir. Bu bilgi, bireylerin ve kurumların dijital dünyada güvenli ve bilinçli bir şekilde hareket etmelerini sağlar.

Bu başlıkta temek güvenlikte kullanılan bazı yaygın kavramlar özetle ele alınacaktır. Bu kavramların doğru anlaşılması, ortak bir dil geliştirilmesine katkıda bulunduğu gibi, güvenlik tehdidin doğru anlaşılıp çözümlerin uygulanmasına da katkıda bulunacaktır.

Siber Güvenlik : Siber güvenlik, bilgisayar sistemlerini, ağları ve diğer dijital altyapıları, siber saldırılardan, veri sızıntılarından, yetkisiz erişimlerden ve diğer tehditlerden koruma amacı taşıyan bir disiplindir (Diakun-Thibault, 2014). Siber güvenlik, bilgi teknolojileri alanında bilgi güvenliği, ağ güvenliği, bilgisayar güvenliği ve internet güvenliği gibi alt alanları içerir. Bu alandaki uzmanlar, siber tehditleri tespit etmek, önlemek, yanıtlamak ve bu tehditlere karşı korunma stratejileri geliştirmekle görevlidir.

Risk: Bilgi güvenliğinde "risk", bir organizasyonun veya bireyin dijital varlıklarını tehdit eden olası bir olayın gerçekleşme olasılığı ve bu olayın organizasyon veya birey için oluşturabileceği olumsuz etkilerin derecesi olarak tanımlanır. Yani, siber güvenlik riski, bir saldırının veya veri sızıntısının olasılığı ve bu olayın sonucunda meydana gelebilecek zararın büyüklüğüdür. Diğer bir ifade ile risk, organizasyonların stratejik amaçlarına ulaşmak için gerçekleştirdiği eylemlerinin etkinliğindeki sapma potansiyeli olarak tanımlanabilir (Mustafa Hakan & Seval, 2019).

Tehdit (threat): Siber güvenlikte "tehdit", bilgisayar sistemlerine, ağlara, cihazlara veya dijital verilere yönelik zarar verebilecek veya bu varlıkları tehlikeye atabilecek potansiyel tehlikeleri ifade eder. Daha formal bir ifade ile tehdit, "*bir bilgi sistemi aracılığıyla, yetkisiz erişim, yok etme, ifşa etme, bilgiyi değiştirme ve/veya hizmet sunumunu engelleme yoluyla, görevlere, görevlendirmelere, imajlara, ulusal siber varlıklara veya personele darbe vurma yeteneğine sahip olan herhangi bir olay*" (Li & Liu, 2021)olarak tanımlanabilir.

Güvenlik açığı *(vulnerability)*: Bir bilgisayar sistemi, yazılım, ağ veya uygulamada var olan ve istenmeyen saldırıların gerçekleştirilmesine olanak tanıyan zayıf bir noktadır. Bu zayıf nokta, saldırganların sisteme yetkisiz olarak erişmelerine, veri çalmalarına, sistemi kontrol etmelerine veya başka zararlı faaliyetlerde bulunmalarına imkan verebilir.

Güvenlik açıkları, hatalı yazılım kodlaması, eksik güvenlik önlemleri, kötü konfigürasyonlar veya güvenlik politikalarının ihlali gibi nedenlerle ortaya çıkabilir. Bu açıklar, sistemin savunmasız olmasına ve saldırılara karşı hassas hale gelmesine yol açar.

Saldırı (attack): Bilgisayar sistemlerine, ağlara veya dijital varlıklara yönelik kötü niyetli ve zarar verici faaliyetleri ifade eder (Humayun ve diğerleri, 2020). Siber ataklar, siber saldırganlar veya kötü amaçlı yazılımlar (*malware*) tarafından

gerçekleştirilen, bilgi sızıntısı, hizmet kesintisi, veri manipülasyonu ve diğer olumsuz sonuçlara yol açabilen girişimlerdir.

Sömürü (exploit): Bilgisayar sistemlerinde veya yazılımlarda var olan güvenlik açıklarını veya zayıflıkları hedefleyen ve bu açıkları kullanarak yetkisiz erişim, veri sızdırma, hizmet kesintisi gibi zararlı faaliyetler gerçekleştiren bir yazılım veya kod parçasıdır. Bu tür yazılımlar, bilgisayar korsanları veya siber saldırganlar tarafından, hedeflenen sistemin veya yazılımın zayıf noktalarını sömürmek amacıyla kullanılır. Exploitler, belirli bir güvenlik açığına özgü olarak tasarlanabilir ve bu açığı etkilemiş olan sistemler veya yazılımlar için geçerli olabilir. Bu açıkları kullanarak, saldırganlar sisteme yetkisiz olarak erişebilir, zararlı kodları yükleyebilir, veri çalabilir veya diğer zararlı faaliyetleri gerçekleştirebilir.

Arka kapı (backdoor): Normalde yetkili olmayan kişilere veya yazılımlara, sistemde gizlice erişim sağlama yeteneği veren bir yazılım veya yöntemdir. Genellikle ağ güvenliği veya uygulama güvenliği zafiyetlerinden kaynaklanır. Bu güvenlik açıkları, yazılım hataları, zayıf parolalar, eksik güvenlik güncellemeleri gibi nedenlerle oluşabilir.

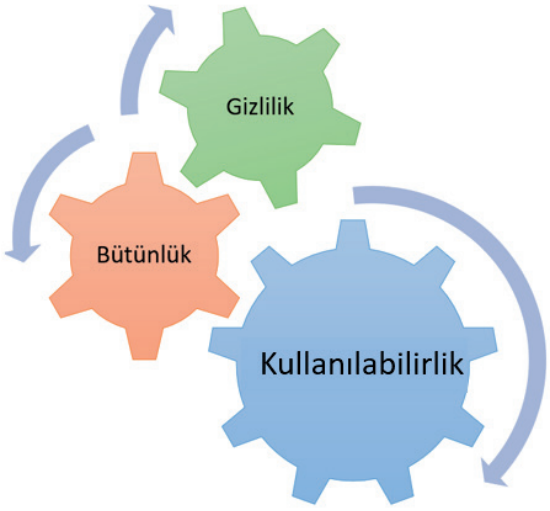
Botnet : Botnet, internet üzerindeki bir dizi bilgisayarın, akıllı cihazın veya diğer internet bağlantılı cihazın, kullanıcı izni olmadan uzaktan kontrol edildiği ve bir amaç doğrultusunda koordineli bir şekilde çalıştırıldığı bir ağdır. Bu cihazlar, kötü niyetli bir aktörün kontrolü altındayken, sahipleri genellikle bundan haberdar değildir. Bu kontrol edilen cihazlar genellikle "zombi makineler" olarak adlandırılır. Botnet'ler, genellikle Truva atları, virüsler veya kötü amaçlı yazılımlar yoluyla bilgisayarları ele geçirerek oluşturulur.

Atak vektörü ve atak yüzeyi : Atak vektörü, bir saldırganın hedef sisteme veya ağa sızmayı veya bir siber saldırı gerçekleştirmeyi planladığı *yol veya yöntemdir*. Yani, atak vektörü, bir saldırganın hedef sistem veya ağdaki zayıf noktaları nasıl kullanarak saldırı gerçekleştirebileceğini belirtir. Atak yüzeyi ise, bir organizasyonun veya sistemin siber saldırılara açık olan tüm noktaların veya *alanların toplamını* ifade eder. Yani, atak yüzeyi, potansiyel saldırı vektörlerinin var olduğu, bir saldırganın hedef alabileceği tüm alanları içerir. Bu alanlar, dış dünyayla olan iletişimi temsil edebileceği gibi, içerideki kullanıcılar, yazılım bileşenleri, veritabanları veya hizmetler gibi içsel bileşenleri de içerebilir.

2. TEMEL GÜVENLİK UNSURLARI

Veri güvenliği, dijital dünyada bilgilerin doğru, güvenilir ve yetkisiz erişimlere karşı korunmasını sağlayan önemli bir kavramdır. *Bilgi güvenliği, bilginin yetkisiz kişiler tarafından okunmasına, verinin değiştirilmesine, kullanılmasına, değiştirilmesine, ifşa edilmesine, incelenmesine, kaydedilmesine ve hasar verilmesine karşı koruma çabası olarak tanımlanabilir*(Yıldırım, 2014). Bu tanımlama Şekil 1'de gösterildiği gibi güvenliğin, *gizlilik, bütünlük ve kullanılabilirlik* gibi birbiri ile ilişkili ve tamamlayıcı temel unsurlarına dayanır(Jang-Jaccard & Nepal, 2014).

Şekil 1. C-I-A üçlüsü



Gizlilik (confidentiality), verilerin sadece yetkili kişiler tarafından erişilebilir olması anlamına gelir; yani, doğru kullanıcılar tarafından görünür ve erişilebilirdir, yetkisiz kişilerden gizlenir. Bu gizlilik temelde *şifreleme (encryption)* algoritmaları tarafından gerçekleştirilir (Alenezi ve diğerleri 2020). *Şifreleme*, bilgileri veya verileri anlaşılması zor hale getiren bir matematiksel veya algoritmik işlemler olarak tanımlanır. Bu işlem, veriyi dışarıdan gelen kişilerin veya sistemlerin okuyup anlamasını zorlaştırır, böylece veri güvenliği sağlanmış olur. Şifreleme, bilgisayarlar arası iletişimden dosya ve veritabanlarına, kullanıcı kimlik bilgilerinden kredi kartı numaralarına kadar birçok farklı türde veriyi korumak için kullanılır.

Şifreleme, verileri şifreleme anahtarı adı verilen özel bilgileri kullanarak dönüştürme işlemidir. Doğru anahtar olmadan şifrelenmiş veriyi anlamak zordur veya matematiksel olarak neredeyse imkansızdır. Sadece, doğru anahtara sahip olan alıcı, veriyi şifreleme sürecini geri alarak (çözme işlemi olarak da bilinir) orijinal veriyi elde edebilir.

Bütünlük (integrity), verilerin değiştirilmemiş, bozulmamış ve güvenilir olduğunu garanti eder. Verilerin yetkisiz değişikliklerden veya bozulmalardan koruyarak doğru ve güvenilir kalmasını sağlar. Bu işlem, verilerin kaynağından hedefine kadar güvenli bir şekilde iletilmesi ve saklanması sırasında sağlanmalıdır. Veri bütünlüğünü sağlamak için yaygın olarak *özet (hash)* fonksiyonları kullanılır (Yong-Xia & Ge, 2010). Hash fonksiyonları, verilerin benzersiz sabit uzunlukta bir özetini (hash değeri) oluşturur. Aynı veriye her zaman aynı hash değeri üretilir. Bu hash değerleri, verilerin bütünlüğünü doğrulamak için kullanılır. Veriler değiştirilirse, hash değeri değişeceği için bütünlük ihlali tespit edilebilir.

Kullanılabilirlik (availability), doğru kullanıcıların gerektiğinde verilere erişebilme yeteneğini ifade eder. Bu kavram bazen uygunluk olarak da tanımlanır. Kullanılabilirlikte önemli olan doğru verilere doğru kişilerin (veya sistemin) ulaşabilmesini sağlamaktır. Bu erişim hem dijital hem de fiziksel erişim olarak göz önünde bulundurulmalıdır. Yani bir sistemin sadece bilgisayar ağları üzerinden erişimi değil, aynı zamanda fiziksel olarak sistemlere erişimi de kontrollü olarak sınırlandırılmalıdır. Bu işlem yetkilendirme (authorization) olarak adlandırılır. Yetkilendirmeye ek olarak, verilerin olası zarar görmesi ihtimaline karşı yedeklenmesi ve gerektiğinde yedeklerden geri alınması da kullanılabilirlik ile ilişkilidir.

Temel güvenliğin bu üç unsurunun haricinde, kimlik doğrulama, inkar edilememezlik gibi destekleyici unsurlar da eklenebilir.

Kimlik doğrulama (authenticity), kullanıcıların gerçek kimliklerini doğrulamayı gerektirir ve sadece doğru kişilere veri erişim izni verilir. Bir kullanıcının veya sistem tarafından sunulan kimlik bilgilerinin gerçekliğini doğrulama sürecini ifade eder. Bu süreç, yetkisiz erişimleri önlemek ve doğru kullanıcılara doğru kaynaklara erişim sağlamak için kritik öneme sahiptir.

Şekil 2. Biometrik kimlik doğrulama örnekleri

Kimlik doğrulama işlemleri parola, dijital imza, biyometrik unsurlar (retina, parmak izi, avuç içi vb), tanımlayıcı fiziksel nesneler (kimlik kartı, RFID etiket vb) çeşitli yöntemlerle sağlanabilir.

İnkar edilememezlik (non-repudiation), bir kullanıcı veya sistem tarafından gerçekleştirilen bir eylemin reddedilemeyeceği anlamına gelir. Yani, bir kişi veya sistem bir işlemi gerçekleştirdiğinde, bu işlemi gerçekleştirdiğini reddedemez. İnkâr edilememezlik, özellikle dijital iletişim ve elektronik ticaret gibi alanlarda önemlidir. Bir mesajın veya işlemin alıcı tarafından doğrulanabilir ve ispatlanabilir bir şekilde gönderici tarafından gerçekleştirildiğini kanıtlayan güvenlik mekanizmalarını içerir. Bu tür güvenlik önlemleri, elektronik imzalar, dijital sertifikalar ve günlük kayıtları gibi teknolojileri içerebilir. İnkar edilememezlik, özellikle yasal anlaşmazlıkların ve ticari işlemlerin güvenli ve güvenilir bir şekilde yürütülmesi için önemli bir role sahiptir. Bu sayede, taraflar gerçekleştirdikleri işlemleri inkar edemezler, bu da güvenli elektronik iletişim ve işlem süreçleri için gereklidir.

Bu temel kavramlar, bilgi güvenliğinde güvenilir ve istikrarlı bir yapı oluşturarak bilgilerin doğru kullanımını ve yetkisiz erişimlere karşı korunmasını sağlar.

ARAŞTIRALIM

Parola ile şifre aynı şey midir? Araştıralım.

3. PAROLA GÜVENLİĞİ

Veri güvenliğinde kimlik doğrulama sürecinde en yaygın kullanılan ve basit olan yöntemlerden biri, *parola (password)* kullanımıdır. Doğru parolaya sahip kullanıcı, yetkisi dahilindeki sisteme giriş yapabilecektir. Parolalar sistemlere girişte engelleyici ve dolayısıyla doğrulayıcı ilk aşamadır. Bu nedenle oldukça önemlidir. Hatalı ve zayıf parola kullanımı hâlen en yaygın güvenlik tehdit sebebidir (OWASP, 2023). Bu nedenle güvenlik için güçlü parola kullanılması kritik derecede önemlidir.

Aşağıda güçlü ve güvenli parolalar oluşturmak için çeşitli öneriler yer almaktadır.

Uzunluk ve Karmaşıklık: Parolaların uzun ve karmaşık olması önemlidir. En az 8 karakterlik bir parola tercih edilmelidir(Joe Dibley, 2022). Parolada büyük harfler, küçük harfler, rakamlar ve özel karakterler (örneğin, !, @, #, $) bulunmalıdır.

Varsayılan Parolalardan Kaçınma: Kimi yazılım veya donanımlar varsayılan bir parola ile gelir. Bu parolaların kullanılmaması ve güçlü parolalar ile değiştirilmesi gerekir.

Kişisel Bilgilerden Kaçınma: Parola içerisinde isim, doğum tarihi, kullanıcı adı veya diğer kolayca tahmin edilebilecek bilgiler olmamalıdır.

Farklı Parola Kullanımı: Farklı hesaplar veya platformlar için aynı parolayı kullanmamak gerekir. Her hesap için farklı ve benzersiz parolalar kullanılmalıdır. Parolalardan herhangi biri ele geçirilirse, diğer hesapların riske girmesi önlenmiş olur.

Yaygın İfadelerden Kaçınma: Parola oluşturulurken yaygın kullanılan deyim, şarkı sözü film adı gibi bilgiler kullanılmamalıdır. Benzer şekilde herhangi bir dildeki sözlükte yer alan kelimelerin de kullanımından kaçınılmalıdır.

Parola Yöneticisi Kullanımı: Parola yöneticileri, güçlü ve benzersiz parolalar oluşturmayı sağlayabilir ve hesap bilgilerini güvenli bir şekilde saklayabilir. Ayrıca, otomatik olarak giriş yapma olanağı tanır.

Düzenli Olarak Değiştirme: Parolalar belirli aralıklarla (örneğin, altı ayda bir) değiştirilmelidir. Böylece, kullanıcı hesabının uzun süre savunmasız kalması önlenir.

İki Faktörlü Doğrulama (Two-Factor Authentication - 2FA): İki faktörlü kimlik doğrulama, parolanın yanı sıra telefona SMS ile gönderilen bir doğrulama kodu gibi ikinci bir doğrulama ekler. Bu ek güvenlik katmanı, hesabın daha güvenli olmasını sağlar.

Parola güvenliği, çevrimiçi hesapları ve kişisel verileri korumanın temel bir adımıdır. Güçlü ve benzersiz parolalar oluşturarak dijital güvenlik arttırılabilir. Tablo 1'de güçlü ve zayıf parola örnekleri yer almaktadır.

Tablo 1. Güçlü ve zayıf parola örnekleri

Parola	Güçlü / Zayıf	Açıklama
1992	Zayıf	• Karmaşık değil • Kişisel veriye (doğum tarihi) işaret edebilir. • Çok kısa
qwerty	Zayıf	• Karmaşık değil • Klavye sıralı harfleri içeriyor • Kısa
Ankara06	Zayıf	• Kişisel bilgi içeriyor • Karmaşık değil
prenses	Zayıf	• Sadece harf • Sözlük kelimesi
ILoveYou	Zayıf	• Sadece harf • Yaygın cümle kullanımı
Password123	Zayıf	• Yaygın kullanılan parola • Sözlük kelimesi
Im!F0tS+13pT)	Güçlü	
A@b8%hYsT1p	Güçlü	
I10vEmy#T0mC@t	Güçlü	

GÜNLÜK HAYATLA İLİŞKİLENDİRELİM

Günlük hayatımızda farklı platformlar için parolalar kullanıyoruz. Ancak kullandığımız parolaların daha önce saldırganlar tarafından kullanılan listelerde yer alıp almadığını bilmiyoruz. Saldırganlar sık kullanılan parolaları, tespit ettikleri veya kırdıkları parolaları bir liste halinde tutabilirler. Aşağıda bağlantısı yer alan sayfada parolanız ve hesabınız ile ilgili bu tarz bir güvenlik riski değerlendirilmektedir.
https://haveibeenpwned.com/Passwords

4. ZARARLI YAZILIMLAR

Zararlı yazılımlar (malware), bilgisayar sistemlerine, ağlara ve diğer dijital cihazlara zarar vermek, bilgileri çalmak, izinsiz erişim sağlamak veya sistemlerin normal işleyişini bozmak amacıyla tasarlanmış kötü amaçlı yazılım türlerini ifade eder. Bu yazılımlar, kullanıcıların haberi olmadan bilgisayarlarına veya cihazlarına bulaşabilir ve çeşitli zararlı faaliyetlerde bulunabilir. Zararlı yazılım türleri arasında virüsler, solucanlar, truva atları, fidye yazılımları, casus yazılımlar ve botnetler gibi çeşitli kategoriler bulunur. Bu yazılımlar genellikle kullanıcıları kandırmak veya güvenlik açıklarını sömürmek suretiyle yayılır ve sıklıkla kişisel veri hırsızlığı, finansal dolandırıcılık ve sistemlerin çökmesi gibi olumsuz sonuçlara yol açabilir. Bu başlık altında en çok karşılaşılan zararlı yazılımlar özetle açıklanacaktır.

4.1. Virüs

Virüs, bilgisayar sistemlerine zarar verebilmek, bilgileri çalmak, izinsiz erişim sağlamak veya sistemlerin normal işleyişini bozmak amacıyla tasarlanmış kötü amaçlı bir yazılım türüdür. Bir virüs, genellikle kullanıcının haberi olmadan diğer programlara bulaşarak kendisini kopyalar ve yayılır. Virüsler, enfekte olmuş dosyalar veya programlar çalıştırıldığında aktif hale gelirler. Ancak bu işlem için kullanıcı etkileşimi gerekir. Yani kullanıcının virüs bulaşmış bir dosyayı açması, bir programı çalıştırması gibi etkileşim sonucunda zararlı etkinlikler devreye girer.

İlk bilgisayar virüsü, 1971 yılında John Draper tarafından yaratılan "Creeper" olarak adlandırılan bir programdı. Creeper, ARPANET (İnternetin öncüsü) üzerindeki DEC PDP-10 bilgisayarlarına bulaşan ve kendisini ekranda görüntüleyen ilk bilgisayar virüsü olarak kabul edilir. Bu virüs daha çok bir oyun olarak kabul edilse de, günümüzdeki zararlı yazılımların temel işleyiş prensiplerini taşımaktadır.

Virüsler genellikle üç ana bileşenden oluşur:

• **Enfekte Edici Kod**: Bu kod, virüsün diğer programlara veya dosyalara bulaşmasını sağlar. Enfekte edici kod, hedef sistemin çalıştırdığı programlara veya dosyalara yerleştirilir.

• **Çoğalma Mekanizması**: Virüsün kendisini kopyalayıp yayabilmesi için kullanılan mekanizmayı ifade eder. Bu, enfekte edici kodun başka programlara veya dosyalara bulaşmasını sağlar.

• **Tetikleyici (Trigger)**: Bu bileşen, virüsün aktivasyon şartlarını belirler. Örneğin, belirli bir tarih veya belirli bir olay gerçekleştiğinde virüs etkinleşebilir.

Virüslere karşı koruma amacıyla antivirüs yazılımları kullanılabilir. Bunun haricinde virüslere karşı korunmanın bazı temel yöntemleri aşağıda maddeler halinde açıklanmıştır:

• *Güvenilir Kaynaklardan Yazılım İndirme*: Yazılımları güvenilir kaynaklardan indirme, virüs bulaşma riskini azaltır. Resmi web siteleri veya güvenilir uygulama mağazaları gibi yerlerden yazılım indirmek önemlidir.

• *Güncel Antivirüs Yazılımı Kullanma*: Güçlü bir antivirüs programı kullanmak, bilgisayarınızı virüs ve diğer zararlı yazılımlardan korur. Bu yazılımlar, bilgisayarınıza indirilen dosyaları ve e-posta eklerini tarar.

• *E-posta Eklerine Dikkat Etme*: Bilinmeyen veya şüpheli kaynaklardan gelen e-posta eklerini ve bağlantıları açmamak önemlidir. E-postalar, virüslerin yayılması için sık kullanılan yöntemlerden biridir.

• *Sistem ve Yazılım Güncellemelerini Yapma*: İşletim sistemi ve diğer yazılımlarınızın güncel olduğundan emin olun. Üreticiler, güvenlik açıklarını düzeltmek için düzenli olarak güncellemeler

yayınlarlar. Bu güncellemeleri yükleyerek sisteminizi koruyabilirsiniz.

• *Farkındalık*: İnternet üzerinde dolaşırken dikkatli olmak, zararlı sitelere ve içeriklere karşı korunmanın en temel yöntemlerindendir. Bilinmeyen kaynaklardan gelen dosyaları açmamak ve tıklamamak önemlidir.

• *Yedekleme*: Önemli verileri düzenli olarak yedeklemek, virüs veya diğer veri kaybına neden olabilecek durumlar için önleyici bir tedbirdir. Yedekleme sayesinde verileri geri yüklemek mümkün olabilir.

4.2. Solucan (Worm)

Solucanlar, bilgisayar ağlarında kendiliğinden yayılabilen ve çoğalabilen programlardır. Diğer kötü amaçlı yazılımlardan farklı olarak, solucanlar kendilerini başka bilgisayar sistemlerine otomatik olarak kopyalar ve yayılırlar. Bu, solucanın bir ana bilgisayardan diğerine geçiş yapabilmesi anlamına gelir.

Solucanlar genellikle ağ üzerinden yayılırlar. İnternet veya yerel ağlar gibi bağlantıları kullanarak, bir bilgisayardan diğerine bulaşabilirler. Solucanlar, genellikle bilgisayar ağlarındaki zayıf noktaları veya güvenlik açıklarını hedef alarak sisteme girebilirler. Bir bilgisayara bulaşan solucan, orada bulunan e-posta adreslerini, dosyaları veya diğer ağ kaynaklarını kullanarak otomatik olarak diğer bilgisayarlara bulaşabilir.

Solucanlar, zararlı eylemlerini gerçekleştirmek için çeşitli özelliklere sahip bileşenlerden (veya yeteneklerden) oluşur.

Replikasyon Yeteneği: Solucanlar, kendi kendilerini kopyalama yeteneğine sahiptirler. Bu, bir sistemde bulunan solucanın, sistemi enfekte ettiği bir dosya veya ağ üzerinden diğer sistemlere otomatik olarak kopyalanabilmesi anlamına gelir.

Yayılma Mekanizması: Solucanlar, yayılmak için bilgisayar ağlarını, e-posta adres defterlerini veya diğer bağlantılı sistemleri hedef alabilirler. Kendi kendilerini yayabilmek için güvenlik açıklarını veya zayıf noktaları kullanabilirler.

Gizlilik Düzeyi: Solucanlar, enfekte ettikleri sistemlerdeki verilere erişme yeteneğine sahip olabilirler. Bu veriler, kullanıcı hesaplarından şifrelere ve diğer hassas bilgilere kadar çeşitli verileri içerebilir.

Zararlı Eylemler: Solucanlar, bulaştıkları sistemlerde dosyaları silme, verileri şifreleme, kullanıcı bilgilerini çalma veya diğer zararlı faaliyetlerde bulunma gibi zararlı eylemler gerçekleştirebilirler.

Gizli Kalma Yeteneği: Solucanlar, keşfedilmemek için kendilerini gizlemek üzere tasarlanmış olabilirler. Bu, antivirüs yazılımlarını atlatma ve tespit edilmeyi önleme yeteneklerini içerebilir.

Uzaktan Kontrol Yeteneği: Bazı solucanlar, bir saldırgan tarafından uzaktan kontrol edilebilir. Bu yetenek, solucanın davranışını değiştirme veya ek komutlar alarak yeni eylemler gerçekleştirme yeteneğini içerir.

Bazı meşhur solucanlar ve etkileri aşağıda açıklanmıştır.

Conficker: 2008 yılında ortaya çıkan Conficker solucanı, Windows işletim sistemine sahip bilgisayarları hedef aldı. Bilgisayarlar arasında kendiliğinden yayılabiliyor, güvenlik yazılımlarını devre dışı bırakabiliyor ve kötü amaçlı yazılım yükleyebiliyordu. Conficker, büyük ölçüde yayıldığı için ciddi bir küresel tehdit oluşturdu.

ILOVEYOU: 2000 yılında ortaya çıkan bu solucan, e-posta aracılığıyla yayılan bir kötü amaçlı yazılımdı. Alıcıya "ILOVEYOU" başlığıyla gelen bir e-posta mesajını açtığında, bilgisayarında bulunan dosyaları silmeye başlıyor ve kendini

e-posta adresi defterindeki diğer kişilere otomatik olarak gönderiyordu.

Sasser: 2004 yılında ortaya çıkan Sasser solucanı, Windows işletim sistemine sahip bilgisayarları hedef aldı. Solucan, bir bilgisayardan diğerine ağ üzerinden yayılan bir açıktan faydalanarak bulaşıyordu. Sasser, bilgisayarları yeniden başlatmaya neden oluyor ve bu da bilgisayar ağlarının performansını olumsuz etkiliyordu.

WannaCry: 2017 yılında ortaya çıkan WannaCry solucanı, birçok ülkedeki sağlık kuruluşları ve büyük şirketleri hedef aldı. Solucan, Windows işletim sistemine sahip bilgisayarları hedef alıyordu. Bilgisayarları şifreleyerek dosyalara erişimi engelliyor ve fidye talep ediyordu. WannaCry, EternalBlue adı verilen bir güvenlik açığından faydalanarak yayıldı.

4.3. Truva Atı (Trojan Horse)

Trojan Horse, zararsız veya yararlı gibi görünerek bilgisayarlara veya diğer cihazlara sızabilen kötü amaçlı yazılımlardır. Adını, Antik Yunan mitolojisindeki Odysseus'un Truva Savaşı'ndaki kandırmaca ile zafer elde ettiği dev ahşap attan alır. Truva atı kullanıcıya zararsız gibi görünen bir dosya veya program olarak sunulur, ancak açıldığında sisteme çeşitli zararlar verir.

Truva atları, kullanıcı farkına varmadan sisteme sızabilir ve çalışabilir. Adını, boyutunu veya diğer özelliklerini değiştirerek kendini gizleyebilir. Bu sayede saldırgan, enfekte olan sistem üzerinde kontrol sahibi olabilir. Bu kontrol, kullanıcının dosyalarını silme, veri çalma, başka zararlı yazılımlar indirme veya sistem kaynaklarını kullanarak diğer saldırıları gerçekleştirme gibi zararlı eylemler olabilir.

Truva atları, enfekte olan sistemde arka kapı açarak kullanıcı adı, parola, kredi kartı bilgileri gibi hassas kullanıcı verilerini çalabilir. Virüs ve solucanlara benzer şekilde sistemdeki güvenlik açıklarını kullanarak kendilerini yayabilirler. Bu sayede, kullanıcının güvenlik yazılımlarını atlatarak sisteme girebilirler. Bir trojan bünyesinde virüs, solucan veya klavyeden basılar her tuşu kaydeden keylogger gibi zararlı yazılımları barındırabilir.

Truva atları, büyük çaplı saldırılara neden olmuş ve geniş kullanıcı kitlesine zarar vermişlerdir. Önemli ve meşhur Truva atlarından bazıları aşağıda verilmiştir.

• **Zeus**: Zeus, bilgisayar korsanları tarafından finansal bilgileri çalmak için kullanılan en ünlü trojanlardan biridir. Banka hesaplarına ve kredi kartı bilgilerine erişim sağlamak için kullanılmıştır.

• **Conficker**: 2008'de ortaya çıkan Conficker, büyük bir botnet oluşturarak milyonlarca bilgisayarı etkisi altına almıştır. Sistemlere sızma, kişisel bilgileri çalma ve diğer zararlı faaliyetlerde bulunma yeteneğine sahiptir.

• **Sasser ve Netsky**: Bu iki trojan, 2004 yılında büyük çaplı saldırılara neden olmuş, milyonlarca bilgisayarı etkisi altına almış ve internet trafiğini yavaşlatmıştır.

• **Stuxnet**: Stuxnet, endüstriyel kontrol sistemlerine (ICS) yönelik bir saldırıda kullanılan son derece sofistike bir zararlı yazılımdır. 2010 yılında keşfedilen Stuxnet, İran'daki nükleer tesislerin santrifüjlerini hedef alarak zarar vermiş ve büyük ses getirmiştir.

• **WannaCry**: WannaCry, 2017 yılında ortaya çıkan bir fidye yazılımıdır. Dünya çağında birçok bilgisayarı kilitlemiş ve fidye ödenmediği takdirde verileri kalıcı olarak silme tehdidi içermiştir.

• **NotPetya/Petya/ExPetr**: 2017'de yayılan bu zararlı yazılım, bir fidye yazılımı olarak başlamıştır, ancak daha sonra amacını değiştirerek bilgisayarları kalıcı olarak bozmuş ve zarar vermiştir. Çeşitli büyük şirketleri etkisi altına almıştır.

4.4. Fidye yazılımı (RansomWare)

Bilgisayar sistemlerini veya dosyalarını şifreleyerek ya da kullanıcının erişimini engelleyerek kullanıcıdan fidye isteyen kötü niyetli bir yazılım türüdür. Şekil 3'te bu zararlı yazılımın etkilendiği bir sistemin ekran görüntüsü yer almaktadır. Fidye yazılımı, genellikle e-posta ekleri, tehlikeli web siteleri veya güvenlik açıklarını kullanarak sistemlere sızabilir.

Şekil 3. Ransomware bulaşmış bir sistem

Bazı fidye yazılımı türleri, kullanıcının bilgisayarına veya dosyalarına erişimini tamamen engeller. Bilgisayar açılamaz hale gelebilir veya dosyalar açılamaz hale gelebilir. Ardından, kullanıcı bilgisayarını veya dosyalarını geri alabilmek için fidye ödemesi talep edilir. Fidye ödendiği takdirde, saldırgan kullanıcıya şifre veya anahtar verebilir. Böylece kullanıcının dosyalarını veya bilgisayarını geri almasını sağlar. Ancak ödeme yapmak garantili bir çözüm değildir ve saldırganlar genellikle ödeme sonrası bile şifre veya anahtar sağlamamaktadır.

4.5. Sosyal Mühendislik Saldırıları

Sosyal mühendislik saldırıları, teknolojinin ötesine geçerek insanların güvenini ve bilgilerini istismar eden sofistike taktikler içerir. Bu tür saldırılar, siber suçluların kullanıcıları aldatmak, manipüle etmek ve kişisel veya hassas bilgilere erişim sağlamak için psikolojik yöntemler kullandığı bir türdür. Kurbanları yanıltarak, güvenlik protokollerini aşarak veya sahte kimliklerle, saldırganlar hedeflerine ulaşmak için insan doğasının zayıf noktalarını kullanırlar.

Oltalama (Phishing): Kullanıcılardan hassas bilgileri (örneğin, kullanıcı adları, parolalar, kredi kartı bilgileri) elde etmek için sahte web siteleri veya e-posta iletişimleri kullanmaktır.

Pretexting: Saldırganlar, güvendikleri bir figür veya kuruluş gibi davranarak, kurbanlarından hassas bilgileri ifşa etmelerini sağlamaya çalışırlar. Örneğin, sahte bir müşteri hizmetleri temsilcisi olarak görünüp kullanıcıyı kandırabilirler.

Baiting: Saldırganlar, kullanıcıları zararlı yazılım içeren dosyaları indirmeye ikna etmek için cazip teklifler veya içerikler kullanır. Bu teklifler genellikle kullanıcının merakını uyandıracak türden şeyler içerir.

Quid Pro Quo: Saldırganlar, kullanıcıya bir hizmet veya avantaj sunarak, karşılığında kullanıcının bilgilerini veya erişim izinlerini talep edebilirler. Örneğin, ücretsiz bir ürün veya hizmet karşılığında kullanıcı adı ve parola talep edebilirler.

Tailgating (Piggybacking): Saldırganlar, fiziksel erişim gerektiren bir alana girmek için gerçek

çalışan gibi davranarak, güvenlik bariyerlerini aşmaya çalışırlar. Örneğin, bir çalışanın yanında yürüyerek güvenli bir binaya girmeye çalışabilirler.

Çöplük Dalışı (Dumpster Diving): Fiziksel güvenlik zafiyetlerini hedef alan sosyal mühendislik taktiklerinden biridir. Bu saldırı türünde, saldırganlar fiziksel olarak hedef organizasyonun çöp kutularını veya geri dönüşüm konteynerlerini karıştırarak, içinde hassas veya gizli bilgilerin olduğu dokümanları veya malzemeleri ararlar.

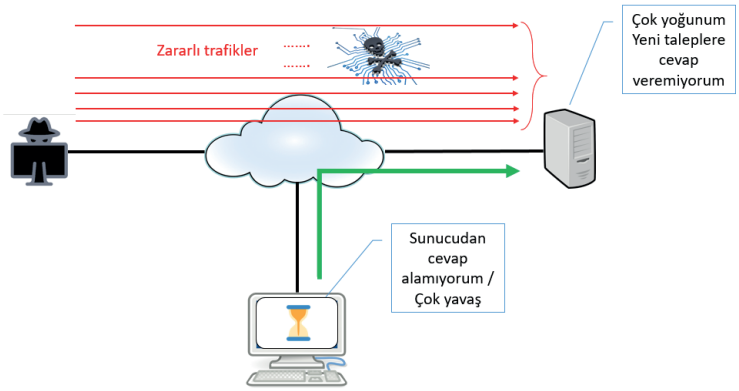
Sosyal mühendislik saldırıları genellikle kullanıcıların güvenliğe dair bilinçsiz davranışlarına dayanır. Bu tür saldırılardan korunmanın anahtarı, dikkatli olmak, şüpheli durumları hızlıca tanımak, bilgi paylaşırken dikkatli olmak ve güvenliğe dair farkındalık geliştirmektir.

4.6. Diğer Bazı Saldırılar

Bilişim dünyasında hemen her gün çok fazla sayıda saldırı ve saldırı aracı ortaya çıkmaktadır. Bilgi güvenliği uzmanlarının bu saldırıları tanıması çözüm geliştirmesinde faydalı olacaktır. Bu başlıkta bazı diğer saldırı türleri kısaca açıklanacaktır.

Deneme Yanılma (Brute Force) Saldırıları: Brute Force saldırısına bazen 'Kaba Kuvvet Saldırısı' da denir. Parola, PIN veya şifrelenmiş veriler gibi korunan sistemlere veya hesaplara erişim sağlamak için tüm olası kombinasyonları deneyerek gerçekleştirilen bir saldırı türüdür. Bu saldırı türünde saldırgan, genellikle oturum açma bilgileri (kullanıcı adı ve parola) gibi doğrulama bilgilerini elde etmeye çalışır. Deneme yanılma saldırısı, saldırganın tüm olası kombinasyonları sisteme veya hesaba uygulayarak doğru kombinasyonu bulana kadar denemeye devam etmesidir. Bu yöntem, doğru kombinasyonu bulana kadar sürebilir, özellikle güçlü ve karmaşık parolalar kullanıldığında, bu tür saldırılar çok zaman alacaktır.

Denial of Service (DoS) Saldırıları: Hedeflenen bir sistem veya ağa aşırı miktarda trafik gönderilerek, normal hizmet sunumunu engellemeye çalışma saldırısıdır (Şekil 4). Diğer bir yöntem de, bilinçli bir şekilde hatalı ayarlanmış IP paketleri ile gerçekleştirilir.



Şekil 4. DoS saldırısı

Distributed Denial of Service (DDoS) Saldırıları: Birçok farklı kaynaktan aynı anda hedeflenen, bir sistem veya ağa aşırı miktarda trafik gönderilerek, hizmetin çalışmasını engellemeye çalışma saldırısıdır.

Man-in-the-Middle (MitM) Saldırıları: İletişim halindeki iki taraf arasına giren saldırgan, veriyi izleyebilir, manipüle edebilir veya çalabilir.

SQL Injection Saldırıları: Web uygulamalarına kötü niyetli SQL kodları enjekte ederek, veri tabanı ile etkileşimde bulunma ve veri çalma veya manipüle etme girişimleridir.

Cross-Site Scripting (XSS) Saldırıları: Web uygulamalarına zararlı komutlar ekleyerek, kullanıcıların tarayıcılarında çalışacak şekilde web sayfalarına gömülü zararlı kodları enjekte etmektir.

5. TEHDİT AKTÖRLERİ

Dijital dünyadaki tehditlerin arkasındaki güçleri anlamak ve tanımlamak, siber güvenlik uzmanlarının ve organizasyonların en büyük önceliklerinden biri haline gelmiştir. Tehdit aktörleri, siber dünyada zararlı faaliyetlerde bulunan, bilgisayar sistemlerine, ağlara veya diğer dijital varlıklara yönelik saldırıları gerçekleştiren kişiler, gruplar veya organizasyonlardır. Bu aktörler, siber casuslar, siber suçlular, devlet destekli saldırganlar veya siber teröristler gibi çeşitli türlerde olabilirler. Her biri farklı motivasyonlarla hareket ederken, hedefleri genellikle hassas verilere erişim, finansal kazanç, itibar zararı veya ulusal güvenliği tehdit etmektir.

Saldırıların karmaşıklığı ve yöntemlerindeki artış, siber güvenlik uzmanlarını sürekli olarak bu tehdit aktörlerini analiz etmeye, izlemeye ve karşı önlemler geliştirmeye yönlendirmiştir. Bu çaba, güvenlik uzmanlarının, savunma stratejilerini güçlendirmek, güvenlik açıklarını kapatmak ve organizasyonları gelecekteki saldırılara karşı daha dirençli hale getirmek için siber saldırganları anlamalarını sağlar.

Hacker (Bilgisayar Korsanı): Genel olarak bilgisayar sistemlerini ve ağları inceleyen, değiştiren, geliştiren veya güvenlik açıklarını keşfeden kişilere verilen geniş bir terimdir. Ancak, terim zamanla farklı anlamlar kazanmıştır. Hackerlar genellikle beyaz şapkalı, gri şapkalı ve siyah şapkalı olmak üzere üç ana kategori altında incelenir.

• *Beyaz Şapkalı Hackerlar (White Hat Hackers)*: Bu hackerlar, bilgisayar sistemlerinin güvenliğini test etmek, güvenlik açıklarını keşfetmek ve düzeltmek için yasal olarak çalışan profesyonellerdir. Bilgi teknolojilerinde güvenlik konusunda uzmanlaşmışlar ve organizasyonlarına veya müşterilerine güvenlik konusunda yardımcı olurlar.

• *Gri Şapkalı Hackerlar (Grey Hat Hackers):* Gri şapkalı hackerlar, genellikle yasal olmayan yollarla bilgisayar sistemlerine sızma veya güvenlik açıklarını keşfetme eylemlerinde bulunurlar, ancak zarar verme veya kişisel kazanç sağlama amacı gütmeyebilirler. Gri şapkalı hackerlar, keşfettikleri güvenlik açıklarını sistem sahiplerine bildirme eğiliminde olabilirler, ancak yine de yasa dışı faaliyetlerde bulunmuş olabilirler.

• *Siyah Şapkalı Hackerlar (Black Hat Hackers):* Siyah şapkalı hackerlar, bilgisayar sistemlerine yasa dışı olarak sızan, zararlı yazılım yayarak bilgi çalan, hizmet kesintilerine neden olan veya diğer zararlı faaliyetlerde bulunan kişilerdir. Bu tür hackerlar genellikle kişisel kazanç, oltalama, fidye veya başka kötü niyetli nedenlerle hareket ederler.

Tehdit aktörleri, amaçlarına, yeteneklerine, kaynaklarına ve faaliyetlerine göre çeşitli şekillerde sınıflandırılabilir. En yaygın sınıflandırma kriterlerine dayalı olarak tehdit aktörleri aşağıda belirtildiği gibi sınıflandırılabilirler.

Siber Suçlular (Cyber Criminals): Finansal kazanç elde etmek amacıyla siber suçları gerçekleştiren kişiler veya gruplardır. Kredi kartı dolandırıcılığı, fidye yazılımları, kimlik avı gibi yöntemlerle kullanıcıları ve organizasyonları hedef alırlar.

Devlet Destekli Aktörler (State-Sponsored Actors): Bir devlet veya devlet kurumu tarafından desteklenen veya finanse edilen tehdit aktörleridir. Bu gruplar genellikle casusluk, ulusal güvenliği tehdit etme veya dış politika amaçları için siber saldırılar gerçekleştirir.

Aktivizm Grupları (Hacktivist Groups): Politik veya sosyal amaçlar için siber saldırılar düzenleyen gruplardır. Bu gruplar genellikle protesto amaçlı, sansür karşıtı veya aktivizm temelli nedenlerle hareket ederler.

Siber Teröristler (Cyber Terrorists): Korku ve paniği yaymak, bir hükümeti yıkmak veya

toplumda kaos yaratmak gibi terör amaçları için siber saldırılar düzenleyen gruplardır.

Casusluk Grupları (Espionage Groups): Casusluk faaliyetleri yürüten, hassas bilgileri çalmak için devlet, şirket veya rakip ülkeleri hedef alan gruplardır. Bu gruplar genellikle gizli bilgileri ele geçirmek ve hedef organizasyonun iç işleyişini anlamak için çalışırlar.

İç Tehditler (Insiders): Organizasyon içinde çalışan veya organizasyonla bağlantılı olan kişiler, bilerek veya bilmeyerek güvenlik açıklarını veya hassas bilgileri ifşa edebilirler.

Bu sınıflandırmalar, tehdit aktörlerinin genel türlerini temsil etmektedir, ancak karmaşıklık arttıkça bu grupların sınıflandırılması da daha ayrıntılı hale gelir. Her bir grup, farklı motivasyonlara sahiptir ve organizasyonlar, bu farklı motivasyonları anlayarak ve analiz ederek güvenlik stratejilerini buna göre şekillendirebilirler.

BÖLÜM ÖZETİ

Bilgi güvenliği, dijital dünyada bireylerin ve organizasyonların güvenliğini sağlamak için kritik bir öneme sahiptir. Bu güvenliği sağlamanın ilk adımı, temel güvenlik kavramlarını bilmekten geçer. Güvenlik, kişisel ve kurumsal verilerin korunması için temel olan yetkisiz erişimden korunma, veri bütünlüğü, gizlilik, kimlik doğrulama ve şifreleme gibi kavramları içerir. Bu unsurlar, dijital tehditleri anlamak ve korunma stratejileri geliştirmek için temel oluşturur.

Bilgi güvenliği, gizlilik, bütünlük ve kullanılabilirlik gibi temel unsurlara dayanır. Gizlilik, verilerin yetkisiz kişilerden gizlenmesini, bütünlük verilerin değiştirilmemesini, bozulmamasını ve güvenilir kalmasını, kullanılabilirlik ise doğru kişilerin gerektiğinde verilere erişebilme yeteneğini ifade eder. Şifreleme, bilgileri anlaşılması zor hale getirerek gizliliği sağlar. Bütünlük, verilerin değiştirilmesini veya bozulmasını engelleyen özet (hash) fonksiyonları ile güvence altına alır. Kimlik doğrulama, doğru kullanıcılara doğru kaynaklara erişim sağlamak için gerçek kimliklerin doğrulanması sürecini ifade eder. İnkar edilemezlik, bir eylemin gerçekleştirildiğinin reddedilemeyeceği güvenlik önlemlerini içerir ve elektronik iletişimde ve ticarette önemlidir. Parola güvenliği, dijital dünyada hesapların ve kişisel verilerin korunması için temel bir önlemdir. Güçlü parolalar oluşturmak ve kullanmak, yetkisiz erişimleri önlemek ve hesapları korumak için kritik önem taşır. Uzun ve karmaşık parolalar tercih edilmeli, büyük harfler, küçük harfler, rakamlar ve özel karakterler içermelidir. Varsayılan parolalar kullanılmamalı, kişisel bilgilerden kaçınılmalı ve farklı hesaplar için benzersiz parolalar kullanılmalıdır. Yaygın ifadelerden ve sözlük kelimelerinden kaçınılmalı, parola yöneticileri kullanılarak güçlü parolalar oluşturulmalıdır. Parolalar düzenli olarak değiştirilmeli ve iki faktörlü kimlik doğrulama gibi ek güvenlik önlemleri kullanılmalıdır. Sosyal mühendislik saldırıları, insanların güvenini ve bilgilerini istismar etmek için psikolojik taktikler kullanan sofistike yöntemler içerir. Oltalama, sahte web siteleri veya e-postalarla kullanıcıları aldatarak hassas bilgileri elde etmeyi içerirken, Pretexting kurbanlarına güvendikleri figürleri taklit ederek bilgileri ifşa etmeye çalışır. Baiting, kullanıcıları zararlı içerikleri indirmeye ikna etmek için cazip teklifler kullanırken, Quid Pro Quo karşılığında hizmet veya avantaj sunarak bilgi talep eder. Tailgating, fiziksel erişim gerektiren alanlara gerçek çalışan gibi davranarak güvenlik bariyerlerini aşmaya çalışırken, Çöplük Dalışı ise fiziksel güvenlik zafiyetlerini hedef alarak çöp kutularını karıştırarak hassas bilgilere ulaşmaya çalışır. Bu tür saldırılardan korunmanın anahtarı, dikkatli olmak, şüpheli durumları hızlıca tanımak, bilgi paylaşırken dikkatli olmak ve güvenliğe dair farkındalık geliştirmektir. Tehdit aktörleri, bilgisayar sistemlerine, ağlara veya diğer dijital varlıklara yönelik saldırıları gerçekleştiren kişiler, gruplar veya organizasyonları ifade eder. Bu aktörler, siber casuslar, siber suçlular, devlet destekli saldırganlar, hacktivist grupları, siber teröristler, casusluk grupları ve iç tehditler gibi çeşitli türlerde olabilirler. Hackerlar genellikle beyaz şapkalı (yasal olarak çalışan güvenlik uzmanları), gri şapkalı (yasa dışı ancak zarar verme amacı olmayan) ve siyah şapkalı (zarar verme veya kişisel kazanç amacı güden) olmak üzere üç ana kategoride incelenir. Tehdit aktörleri, motivasyonlarına ve yeteneklerine göre farklı şekillerde sınıflandırılabilirler, örneğin siber suçlular finansal kazanç sağlamak için saldırırken, devlet destekli aktörler genellikle casusluk veya ulusal güvenlik tehdit etme amacıyla hareket ederler.

GÖZDEN GEÇİRELİM

1. **Aşağıdakilerden hangisi bilgisayar sistemlerinde veya yazılımlarda var olan güvenlik açıklarını hedefleyen ve yetkisiz erişim, veri sızdırma gibi zararlı faaliyetleri gerçekleştiren yazılım veya kod parçasını tanımlar?**
   a) Tehdit
   b) Saldırı
   c) Güvenlik açığı
   d) Exploit

2. **Siber güvenlikte "risk" nasıl tanımlanır?**
   a) Bir organizasyonun veya bireyin dijital varlıklarını tehdit eden olası bir olayın gerçekleşme olasılığı ve olumsuz etkilerin derecesi.
   b) Bilgisayar sistemlerinin güvenliğini test etmek için çalışan profesyoneller.
   c) Bilgisayar sistemlerine, ağlara veya dijital verilere yönelik zarar verebilecek potansiyel tehlikeler.
   d) Bilgisayar sistemlerini siber saldırılardan, veri sızıntılarından koruma disiplini.

3. **Atak vektörü ve atak yüzeyi arasındaki fark nedir?**
   a) Atak vektörü, bir organizasyonun dijital varlıklarını tehdit eden olası olayları tanımlar, atak yüzeyi ise bu olayların gerçekleşme olasılığını ve etkilerini değerlendirir.
   b) Atak vektörü, bir saldırganın hedef sisteme veya ağa sızmayı veya bir siber saldırı gerçekleştirmeyi planladığı yol veya yöntemdir; atak yüzeyi ise potansiyel saldırı vektörlerinin var olduğu tüm alanları ifade eder.
   c) Atak yüzeyi, bir saldırganın hedef sistemdeki güvenlik açıklarını keşfetmesi için kullanılan bir yazılım aracını temsil eder, atak vektörü ise bu açıkları sömürme metodunu belirtir.
   d) Atak vektörü, bir organizasyonun güvenlik duvarının koruyabildiği maksimum uzaklığı ifade eder, atak yüzeyi ise bu uzaklıkta yer alan tüm sistemleri temsil eder.

4. **Aşağıdakilerden hangisi bir bilgisayar sistemi, yazılım, ağ veya uygulamada var olan ve istenmeyen saldırıların gerçekleştirilmesine olanak tanıyan zayıf bir noktayı ifade eder?**
   a) Atak vektörü
   b) Sömürü
   c) Güvenlik açığı
   d) Tehdit

5. **Gizlilik (confidentiality) kavramı aşağıdakilerden hangisiyle ilgilidir?**

a) Verilerin değiştirilmemesini ve bozulmamasını sağlar.

b) Verilerin sadece yetkili kişiler tarafından erişilebilir olmasını sağlar.

c) Verilere doğru kişilerin gerektiğinde erişebilme yeteneğini ifade eder.

d) Verilerin şifrelenerek korunmasını sağlar.

6. **Bütünlük (integrity) nasıl sağlanır?**

a) Verilerin değiştirilmesini ve bozulmasını engelleyen özet (hash) fonksiyonları kullanılarak.

b) Verilere doğru kişilerin gerektiğinde erişebilme yeteneğini ifade eder.

c) Verilerin sadece yetkili kişiler tarafından erişilebilir olmasını sağlar.

d) Verilerin kaynağından hedefine kadar güvenli bir şekilde iletilmesi sırasında sağlanır.

7. **Kimlik doğrulama (authenticity) hangi durumu ifade eder?**

a) Verilerin değiştirilmesini ve bozulmasını engelleyen özet (hash) fonksiyonları kullanılarak.

b) Doğru kullanıcılara doğru kaynaklara erişim sağlamak için gerçek kimliklerin doğrulanması sürecini ifade eder.

c) Verilerin sadece yetkili kişiler tarafından erişilebilir olmasını sağlar.

d) Verilerin kaynağından hedefine kadar güvenli bir şekilde iletilmesi sırasında sağlanır.

8. **Güçlü ve güvenli bir parola oluşturmanın önemli bir adımı, parolada kişisel bilgilerin kullanılmasını içerir.**

Doğru ☐

Yanlış ☐

9. **Parola yöneticileri, güçlü ve benzersiz parolalar oluşturmayı sağlar ve hesap bilgilerini güvenli bir şekilde saklar.**

Doğru ☐

Yanlış ☐

10. **Tehdit aktörleri hangi tür amaçlarla hareket edebilir?**

a) Sadece finansal kazanç için

b) Yalnızca ulusal güvenliği tehdit etmek için

c) Yalnızca siber suçları gerçekleştirmek için

d) Farklı motivasyonlara sahip olabilirler, örneğin finansal kazanç, casusluk veya aktivizm gibi.

11. **Beyaz şapkalı hackerlar kimdir ve ne tür bir rol üstlenirler?**

a) Yasal çalışan güvenlik uzmanlarıdır, bilgisayar sistemlerini yasal olarak test ederler ve güvenlik açıklarını düzeltirler.

b) Yasa dışı yollarla bilgisayar sistemlerine sızarlar ve zarar verme amacı güderler.

c) Politik veya sosyal amaçlar için siber saldırılar düzenlerler.

d) Hesap sahiplerinin kimlik doğrulamalarını çalmak amacıyla phishing saldırıları gerçekleştirirler.

12. Sosyal mühendislik saldırıları aşağıdaki taktiklerden hangisini içerebilir?

a) Yüksek güvenlikli şifreleri zorla kırmak

b) Fiziksel güvenlik sistemlerini hacklemek

c) Kullanıcıları aldatmak ve bilgilerini istismar etmek için psikolojik yöntemler kullanmak

d) Sadece teknolojik zafiyetleri hedef almak

13. Oltalama (Phishing) saldırısı aşağıdakilerden hangisini içerir?

a) Kullanıcıları zararlı yazılımlarla enfekte etmek

b) Fiziksel güvenlik bariyerlerini aşmak

c) Hassas bilgileri ifşa etmeye yönelik sahte web siteleri veya e-postalar kullanmak

d) Sadece fiziksel erişim gerektiren alanlara girmek için kullanılır

Yanıt Anahtarı: 1-D, 2-A, 3-B, 4-C, 5-D, 6-A, 7-B, 8-YANLIŞ, 9-DOĞRU, 10-D, 11-A, 12-C, 13-C

Kaynakça

Alenezi, M. N., Alabdulrazzaq, H., & Mohammad, N. Q. (2020). Symmetric encryption algorithms: Review and evaluation study. *International Journal of Communication Networks and Information Security*, *12*(2), 256–272.

Diakun-Thibault, N. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *2014*.

Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. *Arabian Journal for Science and Engineering*, *45*. https://doi.org/10.1007/s13369-019-04319-2

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. https://doi.org/https://doi.org/10.1016/j.jcss.2014.02.005

Joe Dibley. (2022). *What are NIST Password Guidelines?* Netwrix.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/https://doi.org/10.1016/j.egyr.2021.08.126

Mustafa Hakan, S., & Seval, K. S. (2019). İşletmelerde Siber Risklerin Analizinde, Haritalanmasında Ve Değerlendirilmesinde İç Denetimin Rolü. *Journal*, *19*(57), 1–18.

OWASP. (2023). *OWASP Top 10 API Security Risks – 2023*. Https://Owasp.Org/API-Security/Editions/2023/En/0x11-T10/.

Yıldırım, H. M. (2014). Bilgi güvenliği ve kriptoloji. *Uluslararas Adli Bilişim Sempozyum. Ankara*.

Yong-Xia, Z., & Ge, Z. (2010). MD5 research. *2010 Second International Conference on Multimedia and Information Technology*, *2*, 271–273.

Okuma Listesi

Tunca, S. (2019). Modern Çağda Siber Güvenlik Kavramı . Dumlupınar Üniversitesi İİBF Dergisi , (3-4), 1-7.

https://dsy.usom.gov.tr/usom/19/02/190211082958_siber_guvenlige_giris_ve_temel_kavramlar.pdf

Aydın, H. (2022). Yönetim Bilgi Sistemlerinde (YBS) Siber Güvenliğin Önemi . Bilgisayar Bilimleri ve Teknolojileri Dergisi, 3 (2) , 38-45 . DOI: 10.54047/bibted.1138252

https://www.kaspersky.com.tr/resource-center/threats/trojans

https://www.trendmicro.com/tr_tr/what-is/ransomware.html