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.

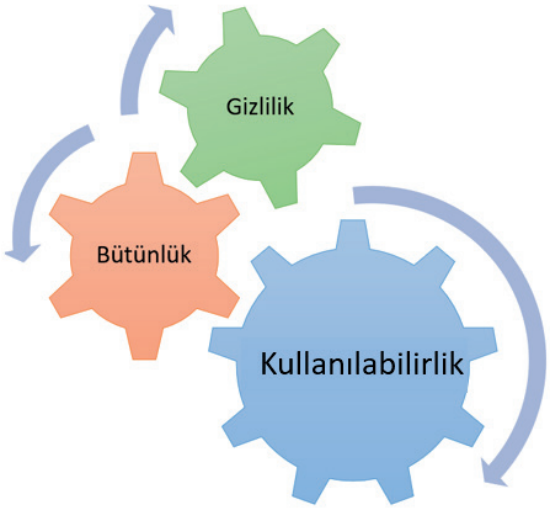
Botnet : Botnet, internet üzerindeki bir dizi bilgisayarın, akıllı cihazın veya diğer internet bağlantılı cihazın, kullanıcı izni olmadan uzaktan kontrol edildiği ve bir amaç doğrultusunda koordineli bir şekilde çalıştırıldığı bir ağdır. Bu cihazlar, kötü niyetli bir aktörün kontrolü altındayken, sahipleri 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.

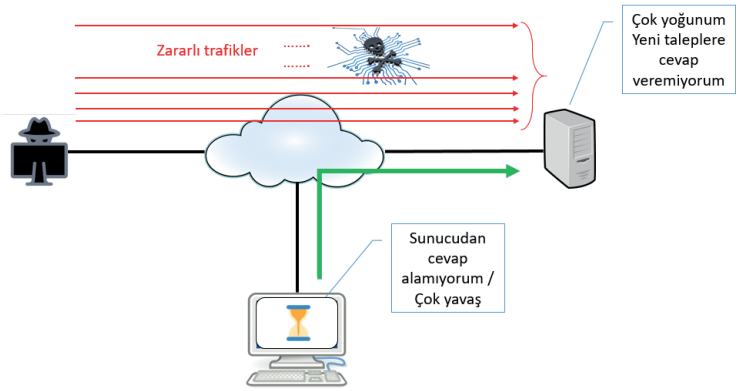
Sosyal mühendislik saldırıları genellikle kullanıcıların güvenliğe dair bilinçsiz davranışlarına dayanır. Bu tür saldırılardan korunmanın anahtarı, dikkatli olmak, şüpheli durumları hızlıca tanımak, bilgi paylaşırken dikkatli olmak ve güvenliğe dair farkındalık geliştirmektir.

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

BÖLÜM 2

AĞ GÜVENLİĞİ

ANAHTAR KAVRAMLAR

Ağ Yönetim Cihazları, Güvenlik Açıkları, Ağ Erişim Güvenliği, Saldırı Türleri, Ağ Güvenlik Ekipmanları

ÖĞRENME HEDEFLERİ

1. Bilgisayar ağlarının yönetiminde kullanılan cihazları tanır
2. Ağ cihazlarının zayıf yönlerini açıklar
3. Ağlara yönelik yapılacak saldırıları bilir
4. Ağ cihazlarını yönetmek için erişim yöntemlerini açıklar
5. Anahtarlama saldırılarını açıklar
6. Yönlendirme saldırılarını açıklar
7. Kablosuz ağlardaki zayıflıkları açıklar
8. Güvenlik açıkları için çözüm önerilerini açıklar
9. Ağ güvenliği için kullanılan donanımları bilir

İKİNCİ BÖLÜM

GİRİŞ

Bilgisayar ağları, bilgisayarlar, ağ cihazları ve diğer iletişim aygıtları arasında veri ve kaynak paylaşımını mümkün kılan bağlantılı bir yapıdır. Bu ağlar, bilgisayarların, yazıcıların, dosya sunucularının, internet erişiminin ve diğer kaynakların paylaşılmasını sağlar. Ayrıca, bilgi ve verilerin standartlar dahilinde bir noktadan diğerine iletilmesine olanak tanır.

Bilgisayar ağlarının temel amacı, iletişim ve veri transferi sağlamaktır. Bu ağlar, farklı yerlerdeki kullanıcılar arasında veri ve bilgi paylaşımını kolaylaştırarak işbirliği yapmayı, kaynakları etkili bir şekilde kullanmayı ve iletişimi artırmayı mümkün kılar. Ayrıca, internet gibi geniş çaplı ağlar aracılığıyla dünya genelindeki bilgisayarları birbirine bağlar.

Bilgisayar ağları genellikle kablolu (Ethernet, fiber optik vb.) veya kablosuz (Wi-Fi, Bluetooth vb.) bağlantılar üzerinden gerçekleştirilir. Bu ağlar, farklı büyüklüklerde olabilir; küçük ölçekli yerel alan ağlarından (LAN) büyük ölçekli geniş alan ağlarına (WAN) kadar çeşitli ölçeklerde olabilirler. Ayrıca, bilgisayar ağları farklı tiplerde de olabilir. Örneğin, internet servis sağlayıcıları tarafından sağlanan genel erişimli ağlar, özel şirket ağları veya devlet kurumları için kurulan özel ağlar gibi farklı türlerde ağlar bulunmaktadır.

Bilgisayar ağları, günümüzde bireyler, işletmeler, kurumlar ve kuruluşlar arasında bilgi alışverişini sağlayan kritik bir teknoloji haline gelmiştir. Bilgisayar ağları günlük yaşamda ve endüstriyel alanlarda birçok farklı yerde bulunur. *Evlerde kullanılan Wi-Fi ağı*, bilgisayar ağlarının en yaygın ve temel örneklerinden biridir. Bu ağlar, bilgisayarlar, akıllı telefonlar, tabletler ve diğer cihazlar arasında internet erişimi sağlar. *Yerel Alan Ağları (LAN),* işyerlerindeki bilgisayarlar ve diğer cihazlar, ofis içinde veri paylaşımı ve işbirliği yapabilmek için yerel

ağlar üzerinde bağlanır. *Okul ve Üniversite Ağları*, öğrencilere ve öğretmenlere kaynakları paylaşma, öğrenme yönetim sistemlerine erişim ve online kaynaklara bağlanma olanağı sunan geniş bilgisayar ağlarına sahiptir. *Cep Telefonu Ağları, m*obil telefonlar, cep telefonu baz istasyonlarına bağlanarak ses ve veri iletişimini mümkün kılan kablosuz ağlar üzerinden çalışır. *Kütüphane ve Açık Alanlar,* kamu alanlarındaki bilgisayarlar ve internet erişimi, kullanıcılara ücretsiz veya ücretli olarak hizmet vermek amacıyla kurulmuş ağlara bağlıdır. *Büyük Veri Merkezleri*, büyük teknoloji şirketleri ve araştırma kuruluşları, büyük veri analizi, bulut hizmetleri ve diğer yüksek performanslı hesaplama görevlerini gerçekleştirmek için karmaşık bilgisayar ağları kullanır. *Telekomünikasyon Ağları*, telefon ve internet hizmetleri sağlayan şirketler, dünya genelinde geniş alan ağları kurar ve yönetir. Bu ağlar, kara kabloları, deniz altı kabloları ve uydu bağlantıları gibi farklı teknolojileri içerir.

Bu örnekler, bilgisayar ağlarının geniş bir uygulama yelpazesi olduğunu gösterir. Günlük hayatımızda gerçekleştirdiğimiz birçok dijital işlem ağlar sayesinde sağlanır ve modern yaşamın birçok yönünde kritik bir rol oynar.

1. AĞ CİHAZLARI

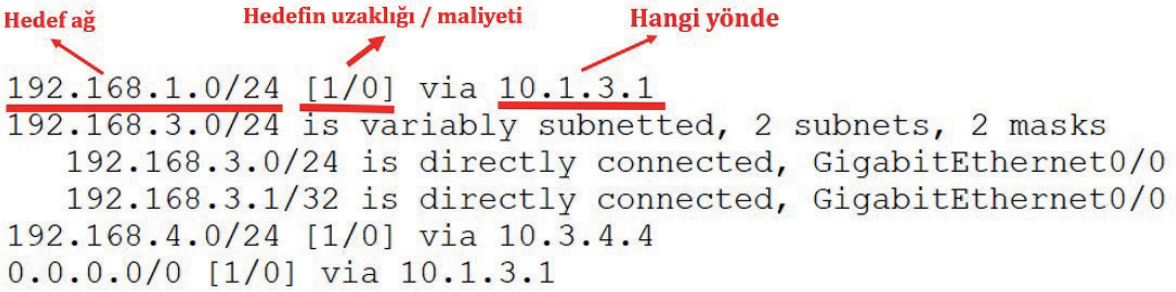
Bilgisayar ağlarında, uç cihazlar ve aracı cihazlar olmak üzere iki tür cihazların varlığından söz edilebilir. Uç cihazlar, verilerin genelde insanlarla etkileşime girdiği, PC, laptop, IP telefon, IP yazıcı, mobil telefon, tablet, sunucu gibi donanımları kapsar. Aracı cihazlar ise, verinin bir uç cihazdan diğerine doğru ve güvenli bir şekilde aktarılmasını sağlayan cihazlardır. Yönlendirici (router), anahtar (switch), kablosuz erişim noktası (Access point) ve güvenlik duvarı (firewall) bu kategoride yer alan cihazlara birer örnektir.

Ağ güvenliği söz konusu olduğunda hem uç cihazların hem de aracı cihazların güvenliğinin sağlanması bir zorunluluktur. Saldırılar ve tehditler sadece son kullanıcıların etkileşim halinde bulunduğu uç cihazlara değil, aracı cihazlara da yapılmaktadır. Bu tür cihazlara yapılan saldırılar, daha geniş bir yüzeyde bir zarara neden olabilir. Bu nedenle güvenlik için öncelikle bu cihazların kullanım amaçları, nasıl çalıştıkları ve çalışma prensipleri incelenmelidir.

Yönlendirici (Router): Yönlendiriciler, farklı ağlar arasında veri paketlerini yönlendirir. İki veya daha fazla ağ arasında veri iletimi sağlar (Şekil 1). IP adreslerini kullanarak paketleri doğru hedefe yönlendirir (Peterson & Davie, 2003).

Şekil 1. Örnel bir yönlendirici cihazının arka panel görüntüsü

Yönlendiriciler, hedef ağlara hangi yolla ulaşılacağını tanımlayan bilgiler barındırır. Bu bilgiler, bir IP paketinin doğru rotaya ulaşılmasını sağlayan ve cihazın belleğinde tutulan ve *yönlendirme tablosu* denen bir tabloda yer alır. Şekil 2'de örneği gösterilen bu tabloda yer alan bilgiler, ağ yöneticisi tarafından elle girilebildiği gibi (statik yönlendirme), yönlendiriciler arasındaki bilgi alışverişi sonucunda otomatik olarak da (dinamik yönlendirme) girilebilir.



Şekil 2. Yönlendirme tablosu örneği

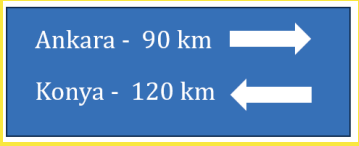
Yönlendirme tablosuna yapılacak bir saldırı sonucunda IP paketleri yanlış yerlere yönlendirilebilir, paketler saldırganların eline geçebilir, bazı durumlarda paketlerin içeriği okunabilir. Böylesi bir durumda, bu tür istismar edilmiş yönlendiriciyi kullanan tüm bilgisayarların ve uç cihazların iletişimine güvenilmez. Uç cihazlarda ne kadar güvenlik sağlanırsa sağlansın, hatalı bir yönlendirme istenmeyen durumlara neden olabilir.

Saldırganlar, yönlendiriciye erişim sağlayarak yönlendirme tablolarını değiştirilebilir, eksik yapılandırılmış dinamik yönlendirme protokollerindeki açıklardan faydalanarak yönlendirme tablosunu bozabilir, iletişimi farklı yere yönlendirebilir, verileri manipüle edebilir (*man in the middle attack*) ve çok farklı amaçlar doğrultusunda zararlı eylemlerini gerçekleştirebilir.

Ev ağı gibi küçük ölçekli ağlarda yönlendiriciler genellikle uç cihazlara IP adresi atama görevini (DHCP sunucu) de yürütürler. Yine yönlendiricilere yapılan bir manipülasyon sonucu, son kullanıcı cihazlarının hatalı IP parametrelerini (ağ geçici adres, DNS gibi) alması sağlanabilir. Benzer şekilde hatalı IP parametrelerine sahip olan bir cihazın güvenli olduğundan bahsedilemez, trafiklerine güvenilemez.

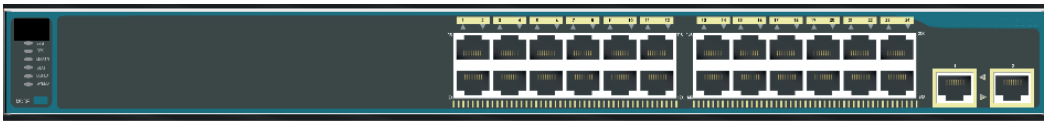
GÜNLÜK HAYATLA İLİŞKİLENDİRELİM

Yönlendiricilerin kullandıkları yönlendirme tablosu, karayollarındaki şehirlerin uzaklıklarını ve gidiş yönünü gösteren tabelalara benzetilebilir.



Bir şehirden uzak bir şehre gittiğinizde, kavşaklardaki tabelalara göre hedef şehre nasıl gideceğinizi karar verirsiniz. Yönlendirme tabloları da benzer şekilde kullanılır. IP paketleri yönlendiricilere ulaştıklarında, yönlendiriciler hedef IP adresine göre hangi arayüzden paketi göndereceklerini belirlerler. Bu işlem yol boyunca tüm yönlendiricilerde yapılır.

Anahtar (Switch): Anahtarlar, bilgisayarlar gibi uç cihazlar arasında doğrudan iletişimi sağlayan donanımlardır. Anahtarda yer alan portlara bağlı olan bilgisayarlar arasındaki veri iletimini daha hızlı ve etkili hale getirir (Şekil 3). MAC (media access control) adreslerini kullanarak paketleri doğru portlara yönlendirir (McDonald, 2013).



Şekil 3. Bir anahtarın görünümü

Anahtarlar, MAC tablosu olarak adlandırılan bir tabloyu bellekte tutarlar. Bu tabloda, hangi cihazın hangi porta bağlı olduğu fiziksel MAC adresleri üzerinden tutulur. Ayrıca bu tabloda, bir uç cihazın anahtar üzerindeki mantıksal izole grupların (VLAN) hangisine dahil olduğu bilgisi de yer alır. Bu bilgilerin saldırı sonucunda manipüle edilmesi, o anahtara bağlı olan tüm cihazların güvenliğini etkiler. Anahtarlar ile ilgili diğer bir önemli konu, son kullanıcı cihazlarının altyapı ile ilk temas noktasını oluşturmasıdır. Bu nedenle anahtarlar genelde en zayıf halkalardan biri olarak varsayılır ve tehdit aktörlerinin hedefindedirler. Anahtara yönelik yapılan saldırılar çok geniş bir yelpazede olabildiğinden ayrı bir başlıkta ele alınacaktır.

Modem (Modulator-Demodulator): Modemler, bilgisayar verilerini analog sinyallere dönüştürerek internet hizmet sağlayıcısının ağına gönderebilir ve aynı zamanda gelen analog sinyalleri dijital verilere dönüştürerek bilgisayar tarafından anlaşılabilir hale getirir. Bu, evlerimizdeki cihazların internete bağlanmasını sağlar(Shinder, 2001).

Access Point (AP): Kablosuz ağlarda kullanılan access point'ler (erişim noktaları), kablolu ağa bağlı cihazların kablosuz olarak ağa erişimini sağlar (Şekil 4). Wi-Fi sinyalleri yayarak kablosuz bağlantıları mümkün kılar(KUNDU, 2008).

Şekil 4. Access Point kablosuz bağlantı sağlar

Access Point'ler radyo frekanslarını kullanarak kablosuz iletişim sağladıkları için saldırganlar için potansiyel bir atak yüzeyidir. AP'nin kapsama alanında bulunan her cihaz teorik olarak bu sinyalleri yakalayabilir. Bu durum ciddi bir güvenlik riski oluşturur. Kablosuz ağlara yönelik yapılan saldırılar ayrı bir başlıkta ele alınacaktır.

Firewall (Güvenlik Duvarı): Güvenlik duvarları, ağ trafiğini denetler ve istenmeyen erişimleri, saldırıları veya veri trafiğini engeller. Bilgisayar ağına gelen ve ağdan çıkan verileri kontrol ederek izin verilen trafikleri geçirirken zararlı trafikleri engeller(Miller, n.d.; Stephen et al., 1996).

Bu bölümde kısaca açıklanan cihazlar, bir bilgisayar ağının temel bileşenleridir ve birlikte çalışarak bilgisayarlar arasında iletişimi ve veri paylaşımını mümkün kılarlar. Cihazlar, belirli görevleri yerine getirirken genellikle belirli protokolleri ve standartları esas alırlar, böylece veri iletimi güvenli ve etkili olur.

2. AĞ CİHAZLARINDAKİ ZAFİYETLER

Bir önceki başlıkta özetle açıklanan ağ cihazlarında çeşitli güvenlik açıkları bulunabilir. Bu açıklar kötü niyetli saldırganların ağa erişmesine veya ağdaki verilere zarar vermesine olanak tanır. Bu tür güvenlik açıkları, ağ cihazlarının yazılımında, çalışma prensibinde, yapılandırmasında veya donanımında olabilir. Ağ cihazlarındaki bazı yaygın güvenlik açıkları aşağıda ele alınmıştır.

Yetersiz Parolalar: Varsayılan parolaların değiştirilmemesi veya zayıf parolaların kullanılması, saldırganların kolayca cihazlara erişim sağlamasını mümkün kılar.

Yazılım Güncellemelerinin İhmal Edilmesi: Ağ cihazlarının işletim sistemlerinde veya yazılımında bulunan güvenlik açıklarının zamanında düzeltilmemesi, saldırılara açık kapı bırakabilir.

Zayıf Şifreleme: Kablosuz ağlarda zayıf veya kırılabilir şifreleme algoritmalarının kullanılması, verilerin güvenliğini tehlikeye atabilir.

DoS (Denial of Service) Saldırıları: Ağ cihazlarına yoğun trafiği yönlendirerek veya aşırı hizmet talepleriyle ağ kaynaklarını tüketerek cihazları hizmet dışı bırakma saldırılarıdır.

Fiziksel Erişim: Fiziksel olarak cihazlara erişim sağlanması, cihazlara zarar verme, yazılım değiştirme veya doğrudan verilere erişim sağlama gibi tehditleri beraberinde getirebilir.

Kötü Tasarlanmış Güvenlik Politikaları: Yetersiz güvenlik politikaları veya erişim kontrolü, yetkisiz erişimlere olanak tanıyabilir.

3. AĞ CİHAZLARINA ERİŞİM GÜVENLİĞİ

Ağ cihazlarına yapılandırma amacıyla erişim sağlamak için genellikle bant içi ve bant dışı olarak adlandırılan iki yöntem kullanılır. Bant içi erişimde Telnet, SSH, SNMP, HTTP/s gibi protokoller kullanılırken, bant dışı erişimde cihaza fiziksel olarak konsol kablosu ile erişilir(Odom, 2004). Aşağıda bu erişim yöntemleri açıklanmıştır.

Konsol Bağlantısı: Ağ cihazlarına fiziksel olarak yaklaşarak, seri konsol kablosu aracılığıyla doğrudan konsol portundan erişim sağlanabilir.

SSH (Secure Shell): SSH, güvenli bir şekilde uzaktan erişim sağlamak için kullanılan bir protokoldür. Kullanıcılar, SSH istemcisi kullanarak ağ cihazlarına şifrelenmiş bir bağlantı kurabilirler.

Telnet: Telnet, ağ cihazlarına uzaktan erişim sağlamak için kullanılan bir protokoldür, ancak veriler şifrelenmez ve güvensizdir. Güvenlik açısından önerilmez, ancak bazı eski cihazlarda hala kullanılabilir.

Web Tabanlı Arayüzler: Ağ cihazlarının çoğu, web tarayıcıları üzerinden yapılandırılabilir. Bu yöntem, kullanıcıların cihazlarına tarayıcıları aracılığıyla erişim sağlamalarını sağlar. Ev ağlarında kullanılan ADSL modem router yapılandırmalarında genelde bu yöntem kullanılır.

• Bu erişim yöntemleri kullanılırken, bazı güvenlik riskleriyle karşılaşılabilir.

• Zayıf veya varsayılan parolalar kullanıldığında, saldırganlar erişim sağlamak için brute-force veya şifre tahmini saldırıları gerçekleştirebilirler.

• Cihazlarda güncel olmayan yazılımların kullanılması, bilinen güvenlik açıklarını içerebilir.

• Güvenlik duvarları veya diğer güvenlik önlemleri yanlış yapılandırıldığında, yetkisiz erişim riski artar.

• Kötü amaçlı yazılımlar, ağ cihazlarına bulaşabilir ve saldırganlara uzaktan erişim sağlama imkanı tanır.

• Fiziksel olarak erişim sağlanabilen cihazlar, yetkisiz kişilerin fiziksel erişim sağlaması riskini taşır.

Bu güvenlik risklerini azaltmak ve ağ cihazlarına yapılandırma erişimini güvenli hale getirmek için çeşitli güvenlik çözümleri uygulanabilir. Aşağıda bu çözümler öneriler olarak yer almaktadır.

Güçlü Parolalar ve Kimlik Doğrulama: Güçlü ve karmaşık parolalar kullanın. İki faktörlü kimlik doğrulamayı (2FA) etkinleştirin.

Yazılım Güncellemeleri: Cihazlarınızdaki yazılımları ve işletim sistemlerini düzenli olarak güncelleyin.

Güvenlik Duvarları ve İzinler: Güvenlik duvarlarını doğru şekilde yapılandırarak sadece gerekli portları ve hizmetleri açık bırakın. İzinleri sıkı bir şekilde denetleyin.

Fiziksel Erişimi Kontrolü: Cihazlara fiziksel erişimi kısıtlamak için güvenlik önlemleri alın, örneğin erişim kontrol kartları veya biyometrik kimlik doğrulama sistemi kullanabilirsiniz.

Kötü Amaçlı Yazılım Taraması: Düzenli olarak kötü amaçlı yazılım taramaları yaparak cihazları temiz tutun.

Güvenli İletişim Protokolleri: Uzaktan erişim için SSH gibi güvenli iletişim protokolleri kullanın. Telnet gibi güvensiz protokollerden kaçının.

Bu tedbirler ve öneriler, ağ güvenliğini artırmak için alınabilecek önemli adımlardır. Güvenlik, sürekli bir süreçtir ve değişen tehditlere karşı sürekli olarak güncellenmelidir.

4. AĞ SALDIRILARI

Ağlara yönelik yapılan saldırılar, çeşitli yöntemlerle gerçekleştirilebilir ve genellikle amaçlarına, kullanılan tekniklere ve etkiledikleri bileşenlere göre sınıflandırılırlar.

4.1. Keşif Saldırıları

Keşif (Reconnaissance) saldırıları, bir saldırganın hedef ağ veya sistem hakkında bilgi toplamak için gerçekleştirdiği ön saldırı aşamasıdır(Standard ve diğerleri., 2013). Bu tür ataklar, saldırganın hedef ağın yapılanması, güvenlik zayıflıkları, kullanılan yazılımlar ve sistem yöneticileri gibi bilgilere erişmesine yardımcı olur. Bu bilgiler daha sonra daha sofistike saldırılar planlamak ve gerçekleştirmek için kullanılır. Keşif saldırıları aktif ve pasif olmak üzere iki ana kategoride değerlendirilebilir (Zaripova & Ugli, 2021).

Pasif Keşif: Bu tür keşifte saldırganlar, hedef ağ veya sistemle doğrudan etkileşime girmek yerine kamuya açık kaynaklardan, internet sitelerinden, sosyal medya hesaplarından ve diğer erişilebilir bilgilerden bilgi toplarlar. Bu bilgiler genellikle IP adresleri, alan adları, e-posta adresleri, çalışan bilgileri ve şirket yapısı gibi genel bilgileri içerir.

Aktif Keşif: Bu tür keşifte saldırganlar, doğrudan hedef ağ veya sistemle etkileşime girer. Bu, port taraması, zayıf nokta taraması ve ağ üzerinde gezinme gibi teknikleri içerebilir. Bu saldırılarla saldırganlar, hedef sistemde çalışan servisleri, açık portları ve potansiyel güvenlik açıklarını belirleyebilir.

Keşif saldırıları, ağ güvenliği açısından ciddi bir tehdit oluşturur, çünkü saldırganlar hedef sistemin zayıf noktalarını tespit edip daha sofistike saldırılar planlayabilirler. Bu tür atakları önlemek veya azaltmak için ağ güvenliği uzmanları, güçlü şifreler kullanma, güvenlik yamalarını düzenli olarak uygulama, ağ trafiğini izleme ve güvenlik duvarları gibi güvenlik önlemlerini uygulayarak sistemi koruma stratejileri geliştirirler.

4.2. Erişim Saldırıları

Erişim (Access) atakları, bir saldırganın yetkisiz şekilde bir sistem, ağ veya hizmete erişim sağlama girişimlerini ifade eder. Bu tür saldırılar, sistemlere veya verilere izinsiz erişmeye çalışmak, yetkisiz hakları kullanarak gizli bilgilere ulaşmak veya hedef sistemi kontrol etmeye çalışmak amacıyla gerçekleştirilir. Erişim atakları, çeşitli yöntemlerle gerçekleştirilebilir ve ağ güvenliğini tehdit eden önemli bir kategori olarak kabul edilir. Bazı yaygın erişim atakları aşağıda açıklanmıştır:

Brute Force Saldırıları: Brute force saldırısı, oturum açma bilgilerini veya parolaları doğru kombinasyonu bulana kadar sürekli olarak deneyerek bir sistem veya hesaba yetkisiz erişim sağlamayı amaçlayan bir tür saldırıdır. Bu tür saldırılar, saldırganın genellikle oturum açma formu veya servisi üzerindeki parola deneme sınırını aşmasını engelleyen güvenlik önlemlerine karşı bir yöntemdir. Brute force saldırıları, şifreleme kullanılan sistemlerde şifre kırma amacı taşırlar. Saldırgan, genellikle kullanıcı adı ve parola kombinasyonlarını sürekli olarak deneyerek, doğru kombinasyonu bulana kadar sistemi veya hesabı hedef alır. Bu saldırı türü, çok sayıda farklı kombinasyonu hızlı bir şekilde deneyebilen yazılım veya yazılım araçları kullanılarak gerçekleştirilebilir (Standard ve diğerleri., 2013).

Brute force saldırılarına karşı korunmak için, kullanıcılar karmaşık ve güçlü parolalar kullanmalı, aynı kullanıcı adı ve parola kombinasyonunu farklı hesaplarda kullanmaktan kaçınmalı ve sistem yöneticileri başarısız oturum açma denemelerini tespit edip engellemek için güvenlik önlemleri uygulamalıdır. Bu önlemler, oturum açma denemelerinin belli bir sıklığı veya süresi içinde sınırlanması, güçlü parola politikaları ve çift faktörlü kimlik doğrulama gibi güvenlik önlemlerini içerebilir.

Password Guessing (Parola Tahmini): Saldırgan, kullanıcıların genellikle kullanabileceği parolaları tahmin ederek giriş yapmaya çalışır. Bu tahmin doğru olarak yapıldığında hedefe erişim sağlanır.

Credential Stuffing: Saldırgan, başka bir hizmette sızdırılan kullanıcı adı ve parola kombinasyonlarını kullanarak aynı kullanıcıların diğer hesaplarına girmeye çalışır. İnsanların genelde aynı parolaları birden fazla hesapta kullanma eğiliminden yararlanır.

Session Hijacking (Oturum Kaçırma): Oturum kaçırma, bir kullanıcının oturumunu (session) ele geçirip, yetkisiz erişim sağlama amacı taşıyan bir saldırı türüdür. Bu tür saldırılar, genellikle çerez (cookie) tabanlı oturum yönetimi kullanan web sitelerinde gerçekleşir. Bir kullanıcının oturumunu ele geçirme süreci aşağıda belirtilen yöntemler ile gerçekleşebilir.

• Session Sniffing (Oturumun Ele Geçirilmesi): Saldırgan, ağdaki verileri izleyerek (sniffing) kullanıcının oturum kimliği (session ID veya cookie) gibi bilgileri ele geçirir. Bu bilgi, kullanıcının web sitesine kimlik doğrulamasız erişim sağlayan bir anahtardır.

• Cookie Theft (Çerezlerin Çalınması): Kullanıcının tarayıcısında saklanan çerezler, oturumu koruyan bir tür anahtardır. Eğer saldırgan kullanıcının tarayıcısındaki çerezleri ele geçirebilirse, bu çerezleri kullanarak kullanıcının oturumunu taklit edebilir ve yetkisiz erişim sağlayabilir.

• Cross-Site Request Forgery- CSRF (Çapraz Site İstek Sahteciliği): Saldırgan, kullanıcıyı, oturumu ele geçirilmiş bir siteye yönlendiren ve kullanıcının farkında olmadığı istekleri gönderen zararlı bir siteye yönlendirebilir. Kullanıcı, güvenilir bir sitede oturum açıkken, bu CSRF saldırısı ile oturumu ele geçirilmiş bir siteye istekler gönderebilir.

Saldırgan, ele geçirdiği oturumu kullanarak kullanıcının adına işlem yapabilir, yetkisiz verilere erişebilir veya kullanıcının hesabında zararlı

aktivitelerde bulunabilir. Bu tür saldırılara karşı korunmak için web uygulamaları, güvenli oturum yönetimi protokolleri kullanmalı, oturum kimlikleri (session IDs veya çerezler) güvenli bir şekilde yönetilmeli ve kullanıcı girişleri, güvenlik duvarları ve güvenlik politikaları ile doğrulamalıdır.

Man-in-the-Middle (MITM) Saldırıları: Saldırgan, veri iletişimini dinleyerek veya değiştirerek kullanıcılar arasına girer. Bu şekilde, veri akışını izleyebilir veya manipüle edebilir (Standard ve diğerleri., 2013).

Zero-Day Exploits: Saldırgan, henüz keşfedilmemiş güvenlik açıklarını kullanarak sisteme erişmeye çalışır. Bu, güncellenmemiş yazılımlardan veya sistemlerden yararlanarak gerçekleştirilir.

Privilege Escalation (Ayrıcalık Yükseltme): Saldırgan, düşük düzeydeki bir hesaptan daha yüksek düzeydeki bir hesaba erişim sağlamak için açıklar veya hataları kullanarak sistemi manipüle eder. Privilege escalation genellikle dikey ve yatay olmak üzere iki şekilde gerçekleşir.

• Vertical Privilege Escalation (Dikey Ayrıcalık Yükseltme): Bu tür privilege escalation, kullanıcının kendi hesabındaki izinleri artırmasını içerir. Örneğin, bir kullanıcı normalde sadece sınırlı bir uygulamaya erişim sağlayan bir hesaba sahipse, bu kullanıcı kendisini daha fazla ayrıcalığa sahip bir hesaba yükseltebilir. Bu tür bir hak yükseltme genellikle uygulama veya sistemdeki bir güvenlik açığından kaynaklanır.

• Horizontal Privilege Escalation (Yatay Hak Yükseltme): Bu tür privilege escalation, bir kullanıcının aynı seviyede (örneğin, iki kullanıcı da yönetici düzeyinde) bulunan bir başka kullanıcının hesabına erişim sağlamasını içerir. Bu, genellikle paylaşılan parolalar veya oturum açma bilgileri gibi güvenlik zayıflıklarından kaynaklanır.

Erişim ataklarına karşı korunmak için güçlü parolalar kullanma, çok faktörlü kimlik doğrulama uygulama, sistemleri ve yazılımları düzenli olarak güncelleme, güvenlik yamalarını hızla uygulama ve ağ trafiğini izleme gibi önlemler alınmalıdır.

5. ANAHTARLAMA (SWİTCHİNG) ZAFİYETLERİ

Anahtarlar son kullanıcı cihazlarının kritik altyapı ile ilk temasının sağlandığı noktadır. Bu nedenle anahtarlar ve anahtarlama çoğunlukla bir ağın en zayıf noktalarından biri olarak görülür. Anahtara yönelik yapılan saldırılar çok geniş bir yelpazede yer alır. Bu saldırılar, ağ güvenliği açısından ciddi tehditler oluşturabilir. Aşağıda anahtarlara yönelik yapılan bazı önemli saldırılar yer almaktadır.

MAC Spoofing (MAC Sahteciliği): Saldırgan, ağdaki başka bir cihazın MAC adresini taklit ederek anahtara kendisini meşru bir cihaz olarak tanıtabilir. Bu şekilde, saldırgan meşru bir cihaz gibi davranabilir ve ağ trafiğini izleyebilir veya yönlendirebilir.

MAC Flooding (MAC Seli): Saldırgan, anahtara çok sayıda sahte MAC adresi göndererek MAC adres tablosunu doldurabilir. Bu durumda anahtar, bir hub gibi çalışıp tüm trafikleri herkese gönderebilir. Bu durum anahtarın normal işlevselliğini bozabilir, doğru kullanıcıların ağa erişimini engelleyebilir veya ağdaki trafiği izlemesine olanak tanır.

ARP Spoofing/Poisoning (ARP Sahteciliği): Saldırgan, ARP tablosunu manipüle ederek anahtara sahte IP-MAC adres eşlemeleri gönderebilir. Bu saldırı, saldırganın veri trafiğini yönlendirmesine ve hatta izlemesine olanak tanır.

VLAN Hopping: VLAN hopping saldırıları, switch konfigürasyonu hatalarını veya zayıflıkla-

rını kullanarak bir VLAN'dan diğerine geçmeyi sağlar. Bu, normalde izin verilmeyen trafiği diğer VLAN'lara yönlendirebilir.

Spanning Tree Protocol (STP) Saldırıları: STP, bir ağdaki ikinci katman döngülerini önlemek için kullanılan bir protokoldür. Saldırganlar, STP saldırıları kullanarak anahtarın ağ topolojisini manipüle edebilir veya anahtarı devre dışı bırakabilir. Ağ topolojisi değiştiğinde, yapılan saldırı türüne bağlı olarak saldırgan ağda döngü oluşmasını sağlayarak ağı (dolayısıyla anahtara bağlı olan tüm cihazları) ağ trafiği üretemez hale getirebilir.

DHCP Starvation (DHCP Açlık) Saldırısı : Açlık saldırısı, ağdaki DHCP sunucularını tükenmeye zorlayan bir tür ağ saldırısıdır. DHCP sunucuları, ağdaki cihazlara (bilgisayarlar, telefonlar, tabletler vb.) IP adresi ve diğer ağ yapılandırma bilgilerini dinamik olarak atar. DHCP sunucusu, IP adreslerini bir havuzda tutar ve bu adresleri cihazlara tahsis etmek için kullanır. DHCP Starvation saldırısı, saldırganın ağdaki tüm IP adreslerini talep etmesiyle gerçekleşir. Bu tür bir saldırıda, saldırganlar sahte MAC adresleri (Media Access Control) ile bir dizi DHCP talebi oluşturarak DHCP sunucusunu aşırı yüklemeye çalışır. DHCP sunucusu, her talebe yanıt vererek IP adreslerini tahsis etmeye çalışır, ancak bu sahte talepler nedeniyle gerçek cihazlara IP adresi tahsis edemez. Sonuç olarak, meşru cihazlar ağa bağlanamaz hale gelebilir, çünkü tüm IP adresleri tükenmiştir. DHCP Starvation saldırısı, ağ performansını düşürebilir, ağa erişimi engelleyebilir ve güvenlik açıklarına yol açabilir.

DHCP Spoofing (DHCP Sahteciliği): Saldırgan, ağdaki DHCP sunucusu gibi davranarak IP adresleri dağıtabilir. Bu, saldırganın verileri yönlendirmesine ve izlemesine olanak tanır.

DNS Spoofing (DNS Sahteciliği): Saldırgan, DNS isteklerini yanıtlayarak kullanıcılara yanıltıcı veya zararlı web sitelerine yönlendirebilir. Bu, kullanıcıları phishing (kimlik avı) saldırılarına maruz bırakabilir.

Anahtarlamaya yönelik yapılan saldırıların çözümünde birden çok güvenlik yönteminin birlikte kullanılması gerekebilir. Aşağıda bu çözüm önerilerine kısaca değinilmiştir.

Port Güvenliği: Kullanılmayan portları devre dışı bırakın ve gerekirse port güvenliği ayarlarını yapılandırın.

802.1X Kimlik Doğrulama: Port bazlı kimlik doğrulama kullanarak yalnızca yetkilendirilmiş cihazların ağa bağlanmasını sağlayın.

Güvenli VLAN Konfigürasyonu: VLAN'lara erişimi kontrol etmek için güvenlik politikaları oluşturun.

Güçlü Parola Kullanımı: Switch yönetim arayüzüne güçlü parolalar ve kimlik doğrulama yöntemleri uygulayın.

Yazılım Güncellemeleri: Switch'in işletim sistemini ve yazılımını güncel tutarak güvenlik yamalarını uygulayın.

Güvenlik Duvarları: Ağınıza gelen ve ağdan çıkan trafiği izlemek ve filtrelemek için güvenlik duvarları kullanın.

Bu önlemler, anahtarlara yönelik saldırıları önlemek ve ağ güvenliğini artırmak için alınabilecek temel adımlardır.

5.1. Yönlendirme (Routing) Zafiyetleri

Yönlendirme işlemi Router (yönlendirici) tarafından ağda gerçekleştirilen, IP paketlerin doğru hedefe gitmesini sağlayan bir süreçtir. Daha önce kısaca değinildiği gibi, bu yönlendirme süreci saldırganlar için bir atak vektörü olabilir.

Routing Tablosu Saldırıları: Saldırganlar, router'ın routing tablosunu manipüle ederek trafik yönlendirmeyi değiştirebilir, bu da trafiği yanlış yönlendirebilir veya ele geçirebilir.

Routing Protocol Saldırıları: Routing protokollerin (örneğin, RIP, OSPF, BGP) zayıf güvenlik mekanizmalarını hedef alarak yanıltıcı veya zararlı routing bilgileri gönderme.

IP Spoofing: Saldırganlar, meşru bir kaynaktan geliyormuş gibi görünen sahte IP adreslerini kullanarak router'ı yanıltabilir.

Fragmentation Saldırıları: Saldırganlar, IP paketlerini parçalayarak, trafik akışı sırasında güvenlik duvarlarını aşabilecek şekilde manipüle edebilir.

Bu saldırıların çözümlerinde öncelikle erişim güvenliğinin sağlanması önemlidir. Saldırganın cihaza uzaktan veya fiziksel olarak erişememesi gerekir. Erişim güvenliğinin sağlanmasının ardından çeşitli yöntemlere yönlendirmeye yönelik çözümler geliştirilebilir. Bu çözümler aşağıda özetle gösterilmiştir.

Güvenilir Routing Protokolleri Kullanımı: Kimlik doğrulama ve şifreleme yeteneği olan güvenli yönlendirme protokolleri kullanılmalıdır. Bu protokoller, doğrulama ve güvenlik önlemleri sağlamak için yapılandırılabilir.

Güncel Yazılım ve Firmware Kullanımı: Ağ cihazlarınızın işletim sistemleri, yazılımları ve firmware'leri güncel olmalıdır. Üretici tarafından yayınlanan güvenlik güncellemelerini düzenli olarak kontrol edilmelidir.

Ağ İzleme: Ağ trafiğini izlemek ve anormal durumları tespit etmek için ağ izleme araçları kullanılmalıdır. Bu şekilde potansiyel saldırıları daha hızlı tespit edebilir ve önlem alınabilir.

ARAŞTIRALIM

Kablosuz ağlarda ne gibi güvenlik riskleri vardır? Bu güvenlik riskleri nasıl azaltılabilir? Araştıralım.

5.2. Kablosuz Zafiyetler

Kablosuz ağlara yönelik bir dizi özgün saldırı türü bulunmaktadır. Bu saldırılar, kablosuz iletişimdeki özelliklerden kaynaklanan güvenlik zayıflıklarını hedef alır ve çeşitli teknikler kullanarak kablosuz ağları hedef alabilirler.

Rogue Access Point (Sahte Erişim Noktası): Saldırganlar, sahte bir erişim noktası oluşturarak, kullanıcıları gerçek ağ yerine kendi oluşturdukları ağa yönlendirebilir. Bu şekilde, kullanıcılar verilerini saldırgana açabilirler.

Evil Twin Attack (Kötü İkiz Saldırısı): Saldırgan, gerçek ağa benzeyen sahte bir kablosuz ağ oluşturarak kullanıcıları kandırabilir. Kullanıcılar, kötü amaçlı ağa bağlandıklarında, saldırgan trafiği izleyebilir ve kişisel verileri çalabilir.

Deauthentication (Deauth) Saldırısı: Saldırgan, hedef ağdaki cihazları deaktive edebilir, böylece bu cihazlar ağa erişemeyerek kullanıcıları hizmet dışı bırakır.

Man-in-the-Middle (MITM) Saldırıları: Saldırgan, kablosuz ağ trafiğini dinleyebilir, değiştirebilir veya çalabilir. Bu, şifrelenmemiş ağlarda daha kolay gerçekleştirilebilir.

Packet Sniffing: Saldırganlar, kablosuz ağdaki veri paketlerini dinleyebilir, bu da hassas bilgilerin ele geçirilmesine olanak tanır.

Wi-Fi Jamming: Saldırganlar, radyo frekanslarına müdahale ederek kablosuz sinyali bozabilir, bu da kullanıcıların ağa bağlanmasını engeller.

WPS (Wi-Fi Protected Setup) Saldırıları: WPS, kullanıcıların kolayca kablosuz ağlara bağlanmalarını sağlayan bir özelliktir. Ancak WPS PIN brute-force saldırılarıyla kolayca kırılabilir.

Kablosuz Güvenlik Protokollerine Yönelik Saldırılar: WEP (Wired Equivalent Privacy) ve bazı eski WPA (Wi-Fi Protected Access) protokollerine yönelik saldırılar, güçlü olmayan şifreleme nedeniyle zayıf noktaları hedef alır.

Kablosuz ağlar, doğası gereği radyo frekansları ile veri iletimi yapar, bu da fiziksel erişime dayalı olmayan saldırıların gerçekleştirilebilmesine olanak tanır. Ancak, bu saldırılar yalnızca kablosuz ağları hedef almaz; çoğu durumda, aynı saldırılar kablolu ağlarda da gerçekleştirilebilir. Bu nedenle, güvenlik önlemleri hem kablosuz hem de kablolu ağlarda etkili bir şekilde uygulanmalıdır.

6. AĞ GÜVENLİK DONANIMLARI

Ağ güvenliğini sağlamak için kullanılan çeşitli donanım cihazları bulunmaktadır. Yaygın olarak kullanılan ağ güvenlik donanımlarından bazıları maddeler halinde sıralanmıştır.

Firewall (Güvenlik Duvarı): Firewall, ağdaki veri trafiğini izleyen ve filtreleyen bir güvenlik cihazıdır(Odom, 2004). İzin verilen ve engellenen trafik kurallarına göre trafiği kontrol eder. Paket filtreleme, durumlu paket incelemesi ve proxy gibi hizmetleri sunarlar. Firewall cihazları ağ giriş noktalarında, iç ağlarda ve veri merkezlerinde kullanılır.

Intrusion Detection System (IDS) ve Intrusion Prevention System (IPS): IDS (saldırı tespit sistemleri), ağda anormal aktiviteleri izler ve belirli saldırı desenlerini tanımlar. IPS (saldırı önleme sistemleri) ise saptanan tehditlere otomatik olarak tepki verir, saldırıları durdurur (Zaripova & ugli, 2021). IDS/IPS sistemleri, tıpkı antivirüs yazılımlarında olduğu gibi, daha önce analiz yapılmış saldırıların karakteristik özelliklerinin yer aldığı imza veritabanlarını kullanabilir. Bu tür sistemlere imza tabanlı IDS/IPS sistemleri denir. Daha gelişmiş sistemlerde ise anomali tabanlı saldırı analizi yapılabilir. Buna göre ağın normal davranışı analiz edilir ve bir temel çizgi (baseline) çıkarılır. Sistem, bu temel çizgiden yaşanan sapmalara göre anormal davranışları tespit edebilir. Bunların haricinde davranış bazlı çalışan IPS sistemleri, makine öğrenmesi tabanlı çalışan gelişmiş ve modern IDS/IPS sistemleri de bulunmaktadır.

IDS/IPS sistemleri, trafik izleme, saldırı algılama, saldırı engelleme, anormal davranış algılama gibi fonksiyonları sunarlar. Genelde internet gibi dışarıdan gelen saldırıları karşılamak üzere ağ giriş noktalarında veya iç ağlarda kullanılır.

Virtual Private Network (VPN) Cihazları: Güvenli bir şekilde uzak kullanıcıları veya uzak ofisleri ağa bağlamak için kullanılır. Veriyi şifreler ve güvenli bir şekilde iletimini sağlar. Şifreleme, kimlik doğrulama, güvenli tünel oluşturma gibi fonksiyonları yerine getirir.

Proxy Sunucular: Proxy sunucular, istemci cihazların ve sunucuların ağa erişimini kontrol eder ve izler. İstemci ve sunucular ile internet arasında ara bir nokta oluşturur. Web filtreleme, İnternet erişimi kontrolü, İnternet anonimliği sağlama gibi fonksiyonları sağlar. Kurumsal ağlarda, içeriği filtreleme ve kullanıcı izleme için kullanılır.

Load Balancer (Yük Dengeleyici): Load balancer, gelen ağ trafiğini dengeler ve farklı sunuculara yönlendirerek yükü dağıtır. Bu, hizmet sürekliliği sağlamak ve performansı artırmak için kullanılır. Trafik dengeleme, sunucu yedekleme ve hizmet sürekliliği gibi doğrudan güvenlik ile ilgili olmayan ancak oldukça faydalı fonksiyonları gerçekleştirir. Yük dengeleyiciler, web siteleri, uygulamalar ve veri merkezlerinde yaygın olarak kullanılır.

Distributed Denial of Service (DDoS) Koruma Cihazları: DDoS koruma cihazları, DDoS saldırıla-

rına karşı ağ ve sunucuları korumak için kullanılır. Ağ trafiğini izler, anormal aktiviteleri belirler ve saldırıları filtreler. Trafik analizi, DoS/DDoS saldırı algılama, saldırıları engelleme görevlerini yaparlar.

Web Security Appliance: Web Security Appliance (WSA), ağlarını güvenli tutmak isteyen organizasyonlar için kullanılan bir güvenlik cihazıdır. WSA, web trafiğini izler, filtreler ve güvenlik tehditlerine karşı koruma sağlar. Bu cihaz, kullanıcıların internet üzerinden güvenli bir şekilde gezinmelerini ve web tabanlı tehditlere karşı savunmalarını güçlendirmelerini sağlar.

URL filtreleme, antivirus ve antimalware koruma, SSL izleme ve içerik filtreleme, uygulama denetimi, veri kaybını önleme, gelişmiş tehdit izleme, raporlama ve analiz görevlerini sağlayabilir. Web Security Appliance, kurumsal ağlarda, okullarda, devlet kurumlarında ve diğer organizasyonlarda kullanılan bir güvenlik çözümüdür. Bu tür bir güvenlik cihazı, çalışanları ve ağı web tabanlı tehditlere karşı korumak için önemli bir rol oynar.

e-Mail Security Appliance, organizasyonların e-posta iletilerini korumak için kullanılan bir güvenlik cihazıdır. Bu cihaz, zararlı e-postaları algılamak, istenmeyen içerikleri engellemek, phishing girişimlerini durdurmak ve gizli verilerin sızmasını önlemek gibi görevleri yerine getirir.

NAC, Network Access Control'ün (Ağ Erişim Kontrolü) kısaltmasıdır ve ağ güvenliği yönetiminde kullanılan bir güvenlik çözümüdür. NAC sistemleri, güvenlik politikalarını uygular, ağa erişmeye çalışan cihazları kimlik doğrular ve yetkilendirir ve yalnızca güvenilir ve uyumlu cihazların ağa bağlanmasını sağlar.

• Kimlik doğrulama: NAC çözümleri, ağa erişim sağlamadan önce kullanıcıları ve cihazları kimlik doğrular. Bu kimlik doğrulama süreci, kullanıcı adı ve şifre, dijital sertifikalar veya çok faktörlü kimlik doğrulama gibi çeşitli yöntemleri içerebilir.

• Yetkilendirme: Kimlik doğrulandıktan sonra, NAC sistemleri, kullanıcıya veya cihaza önceden tanımlanmış güvenlik politikalarına dayalı olarak hangi erişim düzeyini vereceğini belirler. Örneğin, çalışanlara, misafirlere veya taşeronlara farklı erişim seviyeleri atanabilir.

• Uyumluluk Kontrolleri: NAC sistemleri, güvenlik politikalarına uygunluğu kontrol etmek için cihazların güvenlik durumunu değerlendirir. Bu, işletim sisteminin ve antivirüs yazılımının güncel olup olmadığını kontrol etmek, güvenlik yamalarının varlığını doğrulamak ve belirli güvenlik yapılandırmalarının olduğundan emin olmak gibi kontrolleri içerebilir.

• Düzeltme: Bir cihazın güvenlik politikalarına uygun olmadığı tespit edilirse, NAC çözümleri, cihazı karantinaya alabilir, onu düzeltme ağına yönlendirebilir veya kullanıcıya cihazlarını güncellemek için talimatlar verebilir.

• İzleme ve Raporlama: NAC sistemleri sürekli olarak ağ aktivitesini izler, bağlı cihazları takip eder ve güvenlik olayları, uyumluluk durumu ve kullanıcı aktiviteleri hakkında raporlar oluşturur. Bu izleme, potansiyel güvenlik tehditlerini ve gerçek zamanlı olarak tespit edilebilecek olan zayıf noktaları belirlemeye yardımcı olur.

NAC, yetkisiz erişimi önleyerek, hassas verileri güvenli hale getirerek ve ağa bağlanan tüm cihazların kuruluşun güvenlik standartlarını karşıladığından emin olarak ağ güvenliğini artırmada önemli bir rol oynar. Özellikle günümüzde çeşitli ve karmaşık ağ ortamlarında, dizüstü bilgisayarlar, akıllı telefonlar, tabletler ve IoT cihazları gibi farklı cihazların güvenli bir şekilde ağa entegre edilmesi gerektiği durumlarda büyük önem taşır.

BÖLÜM ÖZETİ

Bilgisayar ağlarında kullanılan iki tür cihazdan bulunur. Uç cihazlar genellikle insanlarla etkileşim halinde bulunan cihazları içerirken, aracı cihazlar verinin güvenli bir şekilde iletilmesini sağlar. Yönlendiriciler, farklı ağlar arasında veri iletimini yönlendirir. Yönlendirme tablosu, bu iletimi sağlamak için kullanılır ve saldırılara açık olabilir. Anahtarlar, bilgisayarlar arasında doğrudan iletişimi hızlandırır. MAC tablosu, hangi cihazın hangi porta bağlı olduğunu gösterir. Modemler, bilgisayar verilerini analog sinyallere dönüştürerek internete bağlanmayı sağlar. Access point'ler kablosuz ağlara bağlantıyı mümkün kılar, ancak güvenlik riski taşır. Güvenlik duvarları, istenmeyen erişimleri engeller. Bu cihazlar, belirli protokoller ve standartlarla çalışarak veri iletimini güvenli ve etkili bir şekilde sağlarlar. Ağ cihazlarında güvenlik açıkları bulunabilir. Bu açıklar, yetersiz parolalar, yazılım güncellemelerinin ihmal edilmesi, zayıf şifreleme, DoS saldırıları, fiziksel erişim ve kötü tasarlanmış güvenlik politikaları gibi faktörlerden kaynaklanabilir. Ağ cihazlarına erişim güvenliği için konsol bağlantısı, SSH, Telnet, web tabanlı arayüzler ile sağlanır. Bu yöntemler ile ilgili güvenlik riskleri, güçlü parolalar ve kimlik doğrulama, yazılım güncellemeleri, güvenlik duvarları ve izinlerin doğru yapılandırılması, fiziksel erişim kontrolü ve kötü amaçlı yazılım taramaları gibi çözümler ile önlenebilir. Ağ saldırıları, ağ güvenliği için ciddi bir tehdit oluşturur ve bu tür saldırılara karşı korunmak için alınması gereken önlemler büyük önem taşır. Keşif saldırıları, saldırganların hedef ağ veya sistem hakkında bilgi toplamak için yaptığı ön saldırıları ifade eder. Pasif keşif (kamuya açık kaynaklardan bilgi toplama) ve aktif keşif (doğrudan hedef sisteme etkileşimde bulunma) olmak üzere iki türü vardır. Bu tür saldırıları önlemek için güçlü şifreler kullanma, güvenlik yamalarını düzenli olarak uygulama ve ağ trafiğini izleme gibi önlemler alınabilir. Erişim saldırıları, saldırganların yetkisiz şekilde bir sistem, ağ veya hizmete erişim sağlamak için yaptığı girişimleri ifade eder. Bu tür saldırılara karşı güçlü parolalar kullanma, çok faktörlü kimlik doğrulama uygulama ve yazılım güncellemelerini düzenli olarak yapma gibi önlemler alınabilir. Anahtarlamaya yönelik yapılan saldırılar, ağ güvenliğini ciddi şekilde tehdit edebilir. Bu saldırıları önlemek için kullanılmayan portları devre dışı bırakma, 802.1X kimlik doğrulama kullanma, güvenli VLAN konfigürasyonu oluşturma gibi önlemler alınabilir. Yönlendirme işlemi sırasında yapılan saldırılar, ağ trafiğini yanıltabilir veya ele geçirebilir. Bu tür saldırıları önlemek için erişim güvenliğini sağlama, güvenilir routing protokolleri kullanma ve güncel yazılım ve firmware kullanma gibi önlemler alınabilir. Tüm bu önlemler, ağ güvenliğini artırmak ve saldırılara karşı daha güvende olmak için hayati öneme sahiptir. Ancak unutulmamalıdır ki güvenlik, sürekli bir süreçtir ve ağınızdaki tehditler zaman içinde değişebilir, bu nedenle güvenlik önlemlerinizi sürekli güncellemek önemlidir. Ağ güvenliğini sağlamak için kullanılan çeşitli donanım cihazlar kullanılır. Firewall (Güvenlik Duvarı): Ağdaki veri trafiğini izler ve izin verilen ve engellenen trafik kurallarına göre trafiği kontrol eder. Intrusion Detection System (IDS) ve Intrusion Prevention System (IPS): Ağda anormal aktiviteleri izler ve belirli saldırı desenlerini tanımlar. Virtual Private Network (VPN) Cihazları, Uzak kullanıcıları veya uzak ofisleri güvenli bir şekilde ağa bağlamak için kullanılır. Proxy Sunucular, İstemci cihazların ve sunucuların ağa erişimini kontrol eder ve izler. Load Balancer (Yük Dengeleyici), ağ trafiğini dengeler, farklı sunuculara yönlendirir ve hizmet sürekliliği sağlar. Distributed Denial of Service (DDoS) Koruma Cihazları: DDoS saldırılarına karşı ağ ve sunucuları korumak için kullanılır. Web Security Appliance, e-Mail Security Appliance ve Network Access Control (NAC) gibi özel güvenlik cihazları web tabanlı tehditlere karşı koruma sağlamak, zararlı e-postaları algılamak ve ağa güvenli erişimi kontrol etmek gibi özel görevlere yöneliktir.

GÖZDEN GEÇİRELİM

1. **Ağ cihazlarında güvenlik açıkları oluşmasına neden olan yaygın bir durum aşağıdakilerden hangisidir?**
   a) Fiziksel Erişim
   b) SSH Kullanımı
   c) İyi Yapılandırılmış Güvenlik Duvarları
   d) Yazılım Güncellemeleri

2. **Aşağıdaki güvenlik önlemlerinden hangisi kötü amaçlı yazılım taramasını içerir?**
   a) Fiziksel Erişim Kontrolü
   b) Güçlü Parolalar ve Kimlik Doğrulama
   c) Yazılım Güncellemeleri
   d) Kötü Amaçlı Yazılım Taraması

3. **Ağ cihazlarına yapılandırma amacıyla uzaktan erişimde güvenli bir seçenek olarak tavsiye edilen protokol hangisidir?**
   a) Telnet
   b) HTTP
   c) SSH
   d) FTP

4. **Keşif saldırıları hangi iki ana kategoride değerlendirilebilir?**
   a) Pasif ve aktif
   b) Harici ve içsel
   c) Doğrudan ve dolaylı
   d) Fiziksel ve dijital

5. **Brute-force saldırılarına karşı korunmak için aşağıdaki yöntemlerden hangisi etkili olabilir?**
   a) Kısa ve basit şifreler kullanmak
   b) Aynı parolayı farklı hesaplarda kullanmak
   c) Güçlü parolalar kullanmak ve çift faktörlü kimlik doğrulamayı uygulamak
   d) Parolaları kamuya açık kaynaklarda paylaşmak

6. **Man-in-the-Middle (MITM) saldırısı nedir?**
   a) Saldırganın doğrudan sisteme fiziksel erişim sağlaması
   b) Saldırganın kullanıcılar arasında veri iletişimini dinleyerek veya değiştirerek girmesi
   c) Saldırganın sisteme henüz keşfedilmemiş güvenlik açıklarını kullanarak erişim sağlaması
   d) Saldırganın bir kullanıcının oturumunu ele geçirmesi

7. **MAC Spoofing (MAC Sahteciliği) nedir?**
   a) Gerçek bir cihazın MAC adresini taklit ederek anahtara yetkisiz erişim sağlama saldırısıdır.
   b) Saldırganın anahtara çok sayıda sahte MAC adresi göndererek anahtarın normal işlevselliğini bozma saldırısıdır.
   c) Saldırganın ARP tablosunu manipüle ederek sahte IP-MAC adres eşlemeleri gönderme saldırısıdır.
   d) Saldırganın DNS isteklerini yanıtlayarak kullanıcıları yanıltıcı veya zararlı web sitelerine yönlendirme saldırısıdır.

8. **DHCP Starvation (DHCP Açlık) Saldırısı nedir?**
   a) Saldırganın ağdaki tüm IP adreslerini talep ederek DHCP sunucusunu aşırı yüklemeye çalışmasıdır.
   b) Saldırganın sahte IP adresleri kullanarak anahtara yanıltıcı veri yönlendirmesi yapmasıdır.
   c) Saldırganın DNS isteklerini yanıtlayarak kullanıcıları zararlı web sitelerine yönlendirme saldırısıdır.
   d) Saldırganın ağdaki cihazları deaktive etmesi ve kullanıcıları ağa erişimden mahrum bırakmasıdır.

9. **Aşağıdakilerden hangisi kablosuz ağlara yönelik bir saldırı türüdür?**
   a) Brute Force Saldırısı
   b) MAC Spoofing
   c) Rogue Access Point (Sahte Erişim Noktası)
   d) Spanning Tree Protocol (STP) Saldırısı

10. **Aşağıdaki ağ güvenlik cihazlarından hangisi imza verita banına göre yapılan saldırıyı tespit eder ve önler?**
    a) Yönlendirici
    b) Access Point
    c) NAC
    d) IPS

Yanıt Anahtarı: 1A, 2-D, 3-C, 4-A, 5-C, 6-B, 7-A, 8-A, 9-C, 10-D

Kaynakça

KUNDU, S. (2008). *Fundamentals of Computer Networks*. PHI Learning. https://books.google.com.tr/books?id=OMoHmEQHosAC

McDonald, J. C. (2013). *Fundamentals of Digital Switching*. Springer US. https://books.google.com.tr/books?id=haXqBwAAQBAJ

Miller, R. (n.d.). *Computer Networking: Network+ Certification Study Guide for N10-008 Exam 4 Books in 1: Enterprise Network Infrastructure, Network Security \& Network Troubleshooting Fundamentals*. Richie Miller. https://books.google.com.tr/books?id=_BCeEAAAQBAJ

Odom, W. (2004). *Computer Networking First-step*. Cisco Press. https://books.google.com.tr/books?id=-VoXXwpE_YoMC

Peterson, L. L., & Davie, B. S. (2003). *Computer Networks: A Systems Approach*. Elsevier Science. https://books.google.com.tr/books?id=XUkIKfJbFCUC

Shinder, D. L. (2001). *Computer Networking Essentials*. Cisco Press. https://books.google.com.tr/books?id=ZMizSUW7XF4C

Standard, S., Greenlaw, R., Phillips, A., Stahl, D., & Schultz, J. (2013). Network Reconnaissance, Attack, and Defense Laboratories for an Introductory Cyber-Security Course. *ACM Inroads*, *4*(3), 52–64. https://doi.org/10.1145/2505990.2506002

Stephen, T. D., Harrison, T. M., & Stephen, T. (1996). *Computer Networking and Scholarly Communication in the Twenty-First-Century University: An Introduction to Isaac Breuer's Philosophy of Judaism*. State University of New York Press. https://books.google.com.tr/books?id=Jkuen2GW2H8C

Zaripova D.A and Makhmudov Abdukhalil Abdurakhmon ugli 2021. Network security issues and effective protection against network attacks. International Journal on Integrated Education. 4, 2 (Feb. 2021), 79-85. DOI:https://doi.org/10.17605/ijie.v4i2.1204.

Okuma Listesi

S. Çelik and B. Çeliktaş , "Güncel Siber Güvenlik Tehditleri: Fidye Yazılımlar", Cyberpolitik Journal, vol. 3, no. 5, pp. 105-132, Jul. 2018

G. Canbek and Ş. Sağıroğlu , "BİLGİSAYAR SİSTEMLERİNE YAPILAN SALDIRILAR VE TÜRLERİ: BİR İNCELEME", Erciyes Üniversitesi Fen Bilimleri Enstitüsü Fen Bilimleri Dergisi, vol. 23, no. 1, pp. 1-12, Feb. 2007

Sağıroğlu, Ş. & Mohammmed, M. (2009). Mobil Ortamlara Yapılan Saldırılar Üzerine Bir İnceleme. TÜBAV Bilim Dergisi , 2 (2) , 138-147.

BÖLÜM 3

AĞ YÖNETİMİNDE KULLANILAN PROTOKOLLER

ANAHTAR KAVRAMLAR

Temel Ağ Protokolleri, TCP/IP Protokol Kümesi, Ağ Yönetim Protokolleri, Http ve Https, DHCP, DNS, SNMP

ÖĞRENME HEDEFLERİ

1. Bilgisayar ağlarının çalışma prensibini bilir
2. OSI referans modeline göre ağın çalışmasını açıklar
3. TCP/IP referans modelini bilir
4. IP protokolünü açıklar
5. TCP ve UDP protokollerini açıklar
6. http ve https protokollerinin amacını bilir
7. Ağ yönetiminde kullanılan protokolleri açıklar

ÜÇÜNCÜ BÖLÜM

GİRİŞ

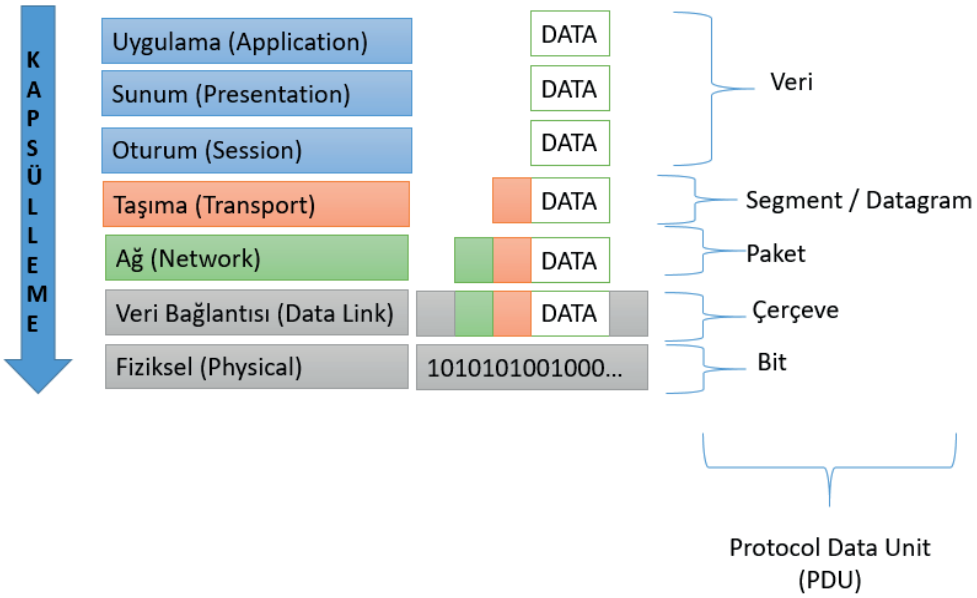
İnsanlar arasındaki iletişim esnasında geçerli olan dil, konuşma hızı, cümle yapısı, sıra beklemek, söz kesmemek, anlaşılamadığında tekrar etme ve anlaşıldığına dair onay almanın gibi kurallar, bilgisayar ağları dünyasında da önemli bir yer tutar. Bu kurallar bütünü, iletişimi hem gönderici hem de alıcı açısından anlaşılır kılmakla sorumlu olan protokoller olarak adlandırılır. Yani, protokoller, farklı üreticilerin çeşitli ürünlerinin aynı platformda uyumlu bir şekilde iletişim kurabilmesini sağlayan standartları belirler.

Bilgisayar ağları, dünyanın dört bir yanındaki bilgisayarları birbirine bağlayan ve veri iletişimini sağlayan temel altyapıları oluşturur. Bu ağlar, internetten şirket içi ağlara, kablosuz ağlardan devasa veri merkezlerine kadar çeşitli şekillerde karşımıza çıkar. Bu karmaşık ağlar, düzgün çalışmalarını sağlamak ve veri iletişimini yönetmek için belirli kurallara ve standartlara ihtiyaç duyar. Ağ protokolleri tam olarak bu noktada devreye girer.

Ağ protokolleri, bilgisayarlar arasında veri iletişimini sağlamak için kullanılan kurallar, standartlar ve işlemlerdir. Bu protokoller, veri paketlerinin nasıl yönlendirileceği, hedefe nasıl ulaştırılacağı, hataların nasıl düzeltileceği gibi detayları belirler. Ağ protokolleri, güvenli ve etkili veri iletişimini sağlamak için tasarlanmıştır.

1. REFERANS MODELLERİ

Bir ağın yönetimi ve güvenliğinin sağlanması, ağın nasıl çalıştığını, ağ protokollerinin ve iletişim standartların anlaşılmasına bağlıdır. Ağın çalışma prensibini açıklayan, ISO'nun geliştirdiği Open System Interconnection (OSI) ve Amerikan Savunma Bakanlığı'nın geliştirdiği TCP/IP adlı iki yaygın referans modeli bulunmaktadır. Her iki model de ağın çalışma sistemini adım adım açıklayan modellerdir.



Şekil 1. OSI referans modeli

OSI referans modeline göre, ağın çalışması yedi adımda incelenmektedir (Şekil 1). Her adımın işlevi ve o adımda yapılması gerekenler kesin olarak belirlenmiştir. Ağın çalışma prensiplerinin belirlendiği bu adımlara "Layer (Katman)" denir. OSI'nin bu mimarisindeki katmanlar birbirinden bağımsız olarak çalışır. Bu standardizasyon sayesinde farklı üreticilerin ürünleri OSI modeline göre tasarlandığı için birbirleri ile haberleşebilir.

Application Layer (Uygulama Katmanı), kullanıcı ile etkileşimin olduğu, uygulamaların bulunduğu katmandır. Örneğin bir web sayfasına bağlanmak için Internet Explorer, Firefox, Chrome gibi bir web tarayıcı uygulaması çalıştırmak gerekir.

Presentation Layer (Sunum Katmanı), uygulama katmanından gelen verilerin şekillendirildiği (sıkıştırma, şifreleme vb.), yani karşıdaki uygulamanın ya da hizmetin anlayabileceği bir biçimde sunulmasının gerçekleştiği katmandır.

Session Layer (Oturum Katmanı), cihazlar arasında sanal oturumların kurulduğu, yönetildiği ve sonlandırıldığı katmandır.

Transport Layer (Taşıma Katmanı), üst katmanlardan gelen verilerin alt katmanları ile iletişimini sağlayan katmandır. Diğer bakış açısıyla, alt katmanlardan gelen verinin, üst katmanlarda hangi uygulama ya da servis ile iletişime geçeceğinin belirlendiği katmandır. Bu belirleme temelde bir sayı olan port numaraları ile sağlanır.

Network Layer (Ağ Katmanı), mantıksal adreslemenin yapıldığı katmandır. Burada veriyi gönderen ve alacak olan cihazların mantıksal adresleri bulunur. Mantıksal adres olarak burada Internet Protocol (IP) adresleri eklenecektir. IP adresi dışında IPX, AppleTalk gibi mantıksal adresler bulunmakla beraber büyük bir çoğunlukla IP kullanıldığı için bu kitap boyunca IP adresleri örnek olarak gösterilecektir.

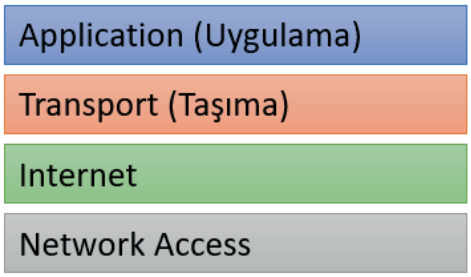
Data – Link Layer (Veri Bağı Katmanı), Veri bağlantısı olarak da adlandırılan bu katman fiziksel adreslemelerin yapıldığı yerdir. Yerel ağdaki, gönderici ve alıcı cihazların fiziksel adreslerinin belirlendiği aşamadır. Burada Fiziksel Adres olarak MAC adresleri kullanılır.

Physical Layer (Fiziksel Katman), verilerin taşınacak ortama (kablo, hava gibi) aktarılmak üzere fiziksel sinyallere dönüştürüldüğü katmandır.

OSI modeline göre çeşitli aşamalarda verilerin başına (header-başlık bilgisi) veya sonuna (trailer – art bilgi) eklenir ve bir alt katmana aktarılır. Bu sürece kapsülleme (encapsulation) denir. Her katmanda oluşan veri ve başlık/artbilgiden oluşan birime Protocol Data Unit (PDU) denir. Katmanların PDU isimleri Şekil 1'de gösterilmiştir.

Alıcı tarafta ise kapsülleme işlemin tersi gerçekleşir. Yani fiziksel ortamdan alınan sinyaller, başlık bilgileri her katmanda çıkarılıp bir üst katmana aktarılır.

TCP/IP (Transmission Control Protocol/Internet Protocol) modeli, bilgisayar ağlarındaki veri iletişimini düzenleyen ve temel protokollerin bir kombinasyonunu tanımlayan bir ağ iletişim modelidir. Bu model, veri iletişimi sürecini dört aşamada açıklar.



Şekil 2. TCP/IP modelinin dört aşaması

Uygulama (Application): Bu aşama, kullanıcı uygulamalarının ağ üzerinden iletişimini yönetir. HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol) gibi uygulama protokolleri bu aşamada çalışır. OSI modelindeki 5-7 arasındaki üç katmana denk gelir.

Taşıma (Transport): Bu aşama, veri iletişiminin güvenilir ve doğru bir şekilde gerçekleşmesinden sorumludur. TCP (Transmission Control Protocol) ve UDP (User Datagram Protocol) bu aşamada çalışır.

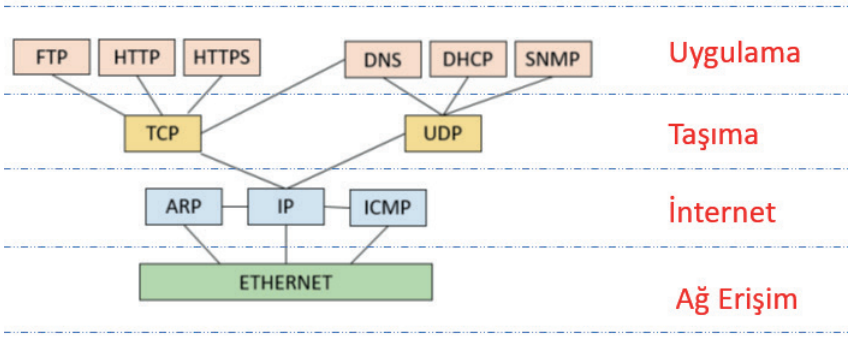
Internet (Internet): Bu aşama, veri paketlerinin kaynak adresinden hedef adresine yönlendirilmesini sağlar. IP (Internet Protocol) bu katmanda çalışır ve ağdaki farklı cihazlar arasındaki veri iletişimini yönlendirir.

Ağ Erişim (Network Access): Bu aşama, ağ donanımını ve fiziksel bağlantıyı yönetir. Ethernet veya Wi-Fi gibi teknolojileri içerir ve veri paketlerinin doğru cihazlara iletildiğinden emin olur.

TCP/IP modeli, internet üzerinde veri iletişimini standartlaştırmak ve farklı cihazların birbiriyle iletişim kurabilmesini sağlamak için kullanılır.

2. TEMEL AĞ PROTOKOLLERİ

Ağ ve internet ortamındaki cihazların sorunsuz çalışabilmesi standartlara ve dolayısıyla protokollere bağlıdır. Günümüzde internet ağlarında en yaygın kullanılan protokoller TCP/IP (Transmission Control Protocol/Internet Protocol) adı verilen bir protokol kümesinde toplanmıştır. Bu protokol kümesinde farklı işlevleri gören ve farklı amaçlara hizmet eden birçok protokol yer almaktadır (Şekil 3). TCP ve IP bu protokollerden en önemli sayılabilecek ikisidir. Bu nedenle protokol kümesinin adı TCP/IP olarak adlandırılır.



Şekil 3. TCP/IP modeline göre bazı protokoller ve Ethernet

TCP/IP protokol kümesi, bilgisayar ağlarında veri iletişimini sağlamak ve farklı cihazlar arasında güvenli ve doğru veri transferini kolaylaştırmak amacıyla tasarlanmıştır. Bu küme, veri paketlerini bölerek, ileterek ve yeniden birleştirerek verilerin güvenli ve hatasız bir şekilde iletilmesini sağlar. Ayrıca, TCP/IP kümesi, cihazlar arasındaki benzersiz kimlikleri yönetir, veri yollarını belirler ve internet üzerinden iletişimi standardize eder. Sonuç olarak, TCP/IP kümesi, dünya genelindeki bilgisayarlar arasındaki etkili ve güvenilir iletişimi mümkün kılan temel bir yapı sağlar. Aşağıda bu TCP/IP kümesinde yer alan temel protokollerden bazıları kısaca açıklanmıştır.

IP : "Internet Protocol" kısaltmasıyla bilinen bir iletişim protokolüdür ve bilgisayar ağlarında veri paketlerini yönlendirmek ve iletmek için kullanılır. IP, verilerin kaynak cihazdan hedef cihaza güvenli ve doğru bir şekilde iletilebilmesini sağlayan anahtar rolü oynar.

Bilgisayar ağlarındaki iletişimde IP'nin adresleme, yönlendirme, paketleme ve rotalama gibi birçok rolü bulunmaktadır. *Adresleme* rolünde, her cihaza benzersiz bir tanımlayıcı olan bir IP adresi atanır. IP adresleri, cihazların ağ içindeki konumlarını belirtir. Bu adresleme sayesinde, veri paketleri doğru hedefe yönlendirilebilir.

GÜNLÜK HAYATLA İLİŞKİLENDİRELİM

Bir arkadaşınıza bir paketi kargoladığınızı düşünün. Bu kargonun arkadaşınıza sorunsuz ulaşabilmesi için alıcı adresi yazan yere arkadaşınızın bulunduğu konumu yazmalısınız. Bu konum adresinin benzersiz olduğuna dikkat edin. Ayrıca paketi teslim ettiğiniz noktadan arkadaşınıza ulaşıncaya kadar çeşitli toplama noktalarından geçtiğine dikkat edin. Benzer işlemler IP iletişiminde de geçerlidir. Ağ ortamında gönderdiğiniz bir verinin doğru alıcıya gidebilmesi için benzersiz bir adrese ihtiyacı vardır. Bilgisayar ağlarındaki bu adrese IP adresi denir ve hedef cihazın konumunu belirler. Kargo örneğindeki gibi, IP paketlerinin içerisine gömülen veriler çeşitli toplama noktalarından geçer ve nihai olarak hedef cihaza ulaşır.

Cihazların konumu belirleyen IP adresleri 32-bitlik sayılardır. Ancak günlük hayatta adresleri bit olarak yazmak hataya neden olabileceğinden, bu 32-bitlik sayı bayt bayt ayrılır ve her bir bayt onluk sayı sistemine dönüştürülür. Ardından bu onluk gösterimler arasına "." konur. Örnek bir IP adresi aşağıdaki gibidir:

32-bitlik gösterim	11000000101010000000001100000111
Noktalı ondalık gösterim	192.168.3.7

IP'nin ağ iletişimindeki diğer bir fonksiyonu *paketlemedir*. Bilgisayar ağları üzerinden gönderilmek istenen veri, IP protokolü tarafından yönlendirilebilir paketlere bölünür. Her paket, hedefe ulaştırılması gereken verinin bir parçasını içerir. Bu paketler, ağ üzerinden ayrı ayrı iletilir ve ardından hedefte yeniden birleştirilir. IP'nin *yönlendirme* işlevinde, veri paketleri kaynaktan hedefe doğru yönlendirir. Verileri taşıyan bu IP paketlerinin ağdaki en iyi yolu izleyerek hedefe ulaştırılması sağlanır. En iyi yol seçimi, birçok etmene bağlı olabilir. Bu işlem ağdaki trafik yoğunluğu, maliyet ve diğer faktörleri değerlendirerek yönlendiricilerdeki yönlendirme tablosuna göre gerçekleştirilir.

IP, bilgisayarlar arasında güvenli, düzenli ve doğru veri iletişimini sağlayarak, modern internet ve bilgisayar ağlarının temelini oluşturur. Bu protokol, internetin ve küresel ağların çalışmasını mümkün kılar.

TCP : İnternet ve ağ iletişiminde verilerin uygulamalar arasında taşınmasından sorumlu olan güvenilir bir protokoldür. Yani verinin hangi uygulamadan çıkıp hedef cihazdaki hangi uygulamaya gideceğini belirler. Hedef ve kaynak uygulamalar port numaraları olarak adlandırılan sayılar aracılığıyla belirlenir. TCP'nin güvenilir olması veri paketlerinin sıralı, onaylı ve hatasız bir şekilde gönderilip alınmasını sağlayacak şekilde tasarlanmış olmasındandır. TCP protokolü, veri transferi sırasında bir dizi özel özelliği yönetir. Bu özellikler aşağıda maddeler halinde gösterilmiştir.

• Güvenilir Veri Transferi: TCP, veri paketlerinin güvenli bir şekilde kaynaktan hedefe ulaşmasını sağlamak için güvenilir veri iletimini yönetir. Veri paketleri, hedef cihaza ulaşmadan önce kaynak cihazda yeniden oluşturulur ve varsa hatalar düzeltilir.

• Sıralı Veri İletimi: TCP, veri paketlerinin hedefe gönderildikleri sırayla alınmasını sağlar. Bu, veri paketlerinin kaynaktan gönderildikleri sırayla hedefe ulaşmasını sağlayarak veri bütünlüğünü korur.

• Akış Kontrolü: TCP, veri transferi sırasında alıcı cihazın veri akışını kontrol etmesine olanak tanır. Bu özellik, alıcı cihazın kendi hızında veri almasını ve aşırı yüklenme durumlarının önlemesini sağlar.

• Bağlantı Yönetimi: TCP, veri transferi başlamadan önce ve iletim esnasında bağlantıyı yönetir. İletişim kurma, veri transferi ve bağlantıyı sonlandırma gibi aşamaları düzenler.

• Hata Tespiti ve Düzeltme: TCP, veri paketlerinin iletim sırasında kaybolduğunu veya bozulduğunu tespit eder. Bu hataları düzeltmek veya kaybolan paketleri yeniden göndermek için gerekli mekanizmaları içerir.

• Akış Denetimi: TCP, ağdaki trafiği dengelemek için akış kontrolü yapabilir. Bu, ağ üzerindeki yoğunluğu düzenler, böylece ağdaki cihazlar arasındaki veri transferi dengelenir.

TCP, internet üzerindeki veri iletişiminin temelini oluşturan protokollerden biridir. Web sayfalarının, dosyaların, e-postaların ve diğer verilerin güvenli bir şekilde transfer edilmesini sağlamak için yaygın olarak kullanılır.

UDP (User Datagram Protocol): Verilerin uygulamalar arasında taşınmasını sağlayan diğer bir

protokol de UDP protokolüdür. TCP ile benzer şekilde port numaralarını kullanarak kaynak ve hedef uygulamaları tanımlar. Ancak UDP oldukça basit bir yapıdadır ve TCP kadar yetenekli bir protokol değildir. Bu nedenle genelde TCP ile karşılaştırılarak yapamadıkları ile açıklanır. Örneğin TCP kullanan uygulamalarda paket kayıpları TCP tarafından yeninden gönderim ile telafi edilebilir, ancak UDP için bu özellik söz konusu değildir. TCP ile kıyaslandığında en önemli avantajı, ek özellikleri olmadığından hızlı olmasıdır. Bu nedenle paket kayıplarının önemsenmediği durumlarda UDP kullanılabilir. Ağ yönetiminde UDP kullanan birçok protokol ve uygulama yer almaktadır. DNS, SNMP gibi protokollerin yanı sıra, genelde ses ve video trafikleri UDP protokolünü kullanır.

DİKKAT EDELİM

UDP paket kayıplarını telafi etmek için bir mekanizma içermez ancak UDP kullanan diğer protokoller bu telafiyi yapabilirler.

HTTP/HTTPS (Hypertext Transfer Protocol/Secure Hypertext Transfer Protocol): Son kullanıcıların en çok yaptığı işlemlerden biri web sayfalarında gezinmektir. Bu durumda http protokolü çalışır ve web tarayıcı kullanarak iletişimi başlatan (istemci) ile web hizmetini veren (sunucu) arasında istemci-sunucu mimarisinde birtakım kurallar çerçevesinde iletişim gerçekleşir.

HTTP, web tarayıcıları ve sunucular arasında metin, grafik, ses, video gibi içeriklerin iletilmesini sağlayan protokoldür. HTTPS ise bu iletişimi şifreleyerek güvenli hale getirir.

Şekil 4. http isteği ve cevabı

İstemci tarafından gönderilen http isteğine (*http request*) sunucu tarafından yanıtlar (*http response*) verilir ve veri takası gerçekleşir. Böylece istenilen sunucudan web sayfası talep edilmiş olur. Şekil 4'te yer alan örnekte, google.com adresine http isteği gönderilmesi gösterilmiştir.

ARAŞTIRALIM

http ile https arasındaki fark nedir? Güvenlik ve yönetim açısından araştırınız.

DNS (Domain Name System): DNS, insanların anlayabileceği domain isimlerini (örneğin, www.ankara.edu.tr) IP adreslerine çeviren bir protokoldür. Bu sistem, internet üzerindeki adreslerin daha kolay hatırlanabilmesini sağlar.

SMTP/POP3/IMAP (Simple Mail Transfer Protocol/Post Office Protocol/Internet Message Access Protocol): Bu protokoller, e-posta iletişimini yönetmek için kullanılır. SMTP, e-postaları göndermek için, POP3 ve IMAP ise e-postaları almak için kullanılır.

FTP (File Transfer Protocol): FTP, dosyaların bir bilgisayardan diğerine transfer edilmesini sağlayan bir protokoldür. Büyük dosyaların paylaşımı ve güncellenmesi için kullanılır.

Ağ protokollerinin etkili yönetimi, ağın güvenliği, performansı ve verimliliği açısından kritiktir. Ağ yöneticileri, ağ trafiğini izler, güvenlik önlemlerini uygular, hataları giderir ve ağ performansını optimize eder. Ağ protokollerinin doğru bir şekilde yapılandırılması ve yönetilmesi, bilgisayar ağlarının sağlıklı ve güvenli bir şekilde çalışmasını sağlar.

Bilgisayar ağlarının yönetimi için kullanılan ağ protokolleri ve bu protokollerin etkili bir şekilde yönetilmesi, modern dünyada bilgi paylaşımı ve iletişimin temelini oluşturur. Bu protokoller, internet, iş ağları, veri merkezleri ve diğer birçok alandaki iletişimi mümkün kılar, böylece dünya genelindeki bilgisayar sistemleri birbiriyle etkileşimde bulunabilir ve bilgi paylaşabilir.

3. AĞ YÖNETİMİ PROTOKOLLERİ

Ağ yönetimi için tasarlanmış protokoller, ağ trafiğini izleme, hataları teşhis etme, performansı optimize etme, güvenlik önlemlerini uygulama ve diğer ağ yönetim görevlerini gerçekleştirmek için kullanılan özel protokollerdir. Ağ yönetimi için tasarlanmış bazı önemli protokoller aşağıda verilmiştir.

*SNMP (Simple Network Management Protocol):*SNMP, ağ cihazlarının durumunu izlemek, hataları teşhis etmek ve yönetmek için kullanılan bir protokoldür. SNMP uyumlu cihazlar, ağ yöneticilerinin bu cihazlarla iletişim kurarak performans verilerini toplamasını sağlar.

NetFlow: Cisco tarafından geliştirilmiş bir ağ trafiği analizi protokolüdür. Ağ trafiğini izlemek, analiz etmek ve kapasite planlaması yapmak için kullanılır. NetFlow, ağdaki trafiği detaylı bir şekilde inceleyerek performans problemlerini tespit etmeye yardımcı olur.

ICMP (Internet Control Message Protocol): Bir ağ ortamında gerek sorun giderme için gerek iletişimin varlığının doğrulanması için kontrol edilmesi ihtiyacı vardır. ICMP, bu amaç doğrultusunda geliştirilmiş, belirli bir IP'nin erişilebilir olup olmadığını doğrulamak için kullanılan bir protokoldür. Erişimin olup olmadığının yanı sıra, erişim ile ilgili, erişiminin olmamasının olası nedeni, erişilen cihaza ve uzaklığına dair çeşitli bilgiler de sunan yararlı bir protokoldür. Ağ yöneticileri, ICMP mesajlarını kullanarak ağdaki bazı problemleri teşhis edebilirler. Örneğin belirli bir IP'nin veya alan adının erişilebilir olup olmadığını doğrulamak için kullanılan ping komutu, ICMP protokolünü kullanır.

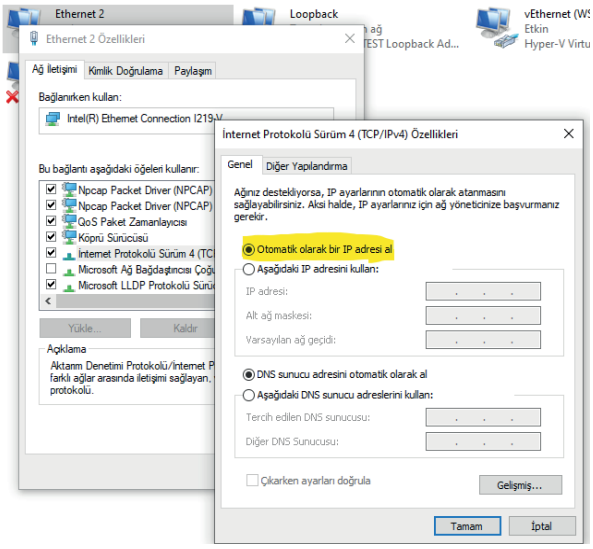
```
C:\>ping www.google.com

Pinging www.google.com [142.250.184.132] with 32 bytes of data:
Reply from 142.250.184.132: bytes=32 time=21ms TTL=53
Reply from 142.250.184.132: bytes=32 time=21ms TTL=53
Reply from 142.250.184.132: bytes=32 time=22ms TTL=53
Reply from 142.250.184.132: bytes=32 time=22ms TTL=53

Ping statistics for 142.250.184.132:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 21ms, Maximum = 22ms, Average = 21ms
```

Şekil 5. ping komutu ile erişilebilirlik kontrolü

Şekil 5'te yer alan örnekte www.google.com adresinin erişilebilir olup olmadığı sorgulanmış (ping www.google.com) ve gelen cevaptan uzaktaki sunucunun erişilir olduğu görülmüştür. Şekilde kontrol için 4 ICMP paketi gönderilmiş ve hepsinden kayıpsız (%0 loss) cevap alınmıştır.

DHCP (Dynamic Host Configuration Protocol): Bilgisayar ağlarında cihazların benzersiz IP adreslerinin olması gerektiğini hatırlayın. Ayrıca sağlıklı bir iletişim cihazların ağının sınırlarını belirlemesini sağlayan *maske*, ağdan çıkış noktasını (ağ geçidi - gateway) ve DNS sunucusunun adresinin de tanımlı olması gerekir. Bu parametreler cihazlara elle verilebilir. Ancak özellikle çok sayıda cihazın bulunduğu ağlarda bu bilgilerin elle verilmesi zaman alıcı ve hataya neden olabilir. Bu nedenle cihazların bu parametreleri dinamik olarak almasını sağlayan DHCP isimli bir protokol geliştirilmiştir.

DHCP, ağdaki cihazlara otomatik olarak IP adresi ve diğer ağ konfigürasyon bilgilerini atayan bir protokoldür. Bu, ağ yöneticilerinin IP adresi tahsisini otomatikleştirmelerine ve merkezi olarak yönetmelerine olanak tanır.



Şekil 6. DHCP kullanarak otomatik IP alma

Şekil 6'daki görüntüde gösterildiği gibi "Otomatik olarak bir IP adresi al" seçeneği seçildiğinde cihazlar DHCP protokolünü kullanarak gerekli bilgileri bir sunucudan alır. Örneğin ev ortamında sıklıkla kullanılan ADSL modem-yönlendiriciler, varsayılan olarak DHCP hizmeti verecek şekilde tasarlanmıştır. Yani bir ev ağı için ADSL modem aynı zamanda bir DHCP sunucusudur. Kurumsal büyük ağlarda ise genelde bu işlem için bağımsız sunucular kullanılır.

RADIUS (Remote Authentication Dial-In User Service): RADIUS, ağ kaynaklarına erişim yetkisini doğrulamak için kullanılan bir protokoldür. Özellikle büyük ölçekli ağlarda, merkezi bir sunucu üzerinden kimlik doğrulama ve yetkilendirme işlemlerini sağlar.

SSH (Secure Shell) : SSH, uzaktaki bilgisayarlara güvenli bir şekilde erişim sağlamak için kullanılan bir ağ protokolüdür. SSH, verilerin şifrelenmesini ve güvenli bir şekilde iletilmesini sağlayarak, kullanıcıların uzak sunuculara güvenli bir şekilde bağlanmasına ve komutlarını uzaktaki sunucularda çalıştırmasına olanak tanır.

Bu protokoller, ağ yöneticilerinin ağlarını izlemek, güvenliği sağlamak, hataları teşhis etmek ve ağ performansını optimize etmek için kullandığı önemli araçlardır. Bu protokoller, modern ağ yönetimi için temel taşlar olarak kabul edilir.

BÖLÜM ÖZETİ

İnternet ağlarındaki cihazların sorunsuz çalışabilmesi için protokoller ve standartlar yer alır. TCP/IP protokolü, veri iletişimini sağlamak, güvenli ve doğru veri transferini kolaylaştırmak amacıyla tasarlanmıştır. IP, veri paketlerini yönlendirme ve iletim için kullanılırken, TCP verilerin güvenli taşınmasından sorumludur. UDP ise veri iletimi için kullanılan basit bir protokoldür, ancak paket kayıplarını telafi etme özelliği yoktur ve hızlı iletim sağlar. Bu protokoller, internet ve ağ iletişiminin temelini oluşturur. Open System Interconnection (OSI) ve TCP/IP olmak üzere iki yaygın referans modeli yer almaktadır. OSI modeli, ağın çalışmasını yedi adımda inceler: Uygulama Katmanı, Sunum Katmanı, Oturum Katmanı, Taşıma Katmanı, Ağ Katmanı, Veri Bağı Katmanı ve Fiziksel Katman. Her katman belirli bir işlevi yerine getirir ve verilerin iletimini sağlar. Bu katmanlar, farklı cihazlar arasında iletişimi standardize eder ve veri iletimi sürecini açıklar. Kapsülleme (encapsulation) adı verilen bir süreçle veriler, her katmanda başlık bilgileriyle birlikte taşınır ve Protocol Data Unit (PDU) adını alan birime dönüşür. Alıcı tarafta ise kapsülleme işlemi tersine çevrilir ve veriler bir üst katmana aktarılır. Bu model, ağ iletişiminin temel prensiplerini açıklar. Diğer bir referans modeli de Uygulama, Taşıma, İnternet ve Ağ Erişimi isimli 4 aşamadan oluşan TCP/IP modelidir. Bilgisayar ağlarındaki iletişimi sağlayan temel protokollerden olan IP (Internet Protocol) adresleme, yönlendirme, paketleme ve rotalama gibi önemli rolleri üstlenir ve bilgilerin güvenli ve doğru bir şekilde iletilmesini sağlar. TCP (Transmission Control Protocol) ise verilerin güvenilir bir şekilde taşınmasından sorumludur ve güvenilir veri transferi, sıralı veri iletimi, akış kontrolü, bağlantı yönetimi, hata tespiti ve düzeltme, akış denetimi gibi özellikleri yönetir. UDP (User Datagram Protocol) ise daha basit bir yapıda olup hızlı veri transferine olanak tanır. Diğer önemli protokoller arasında HTTP/ HTTPS (web sayfalarının iletişimi), DNS (domain isimlerinin IP adreslerine çevrilmesi), SMTP/POP3/ IMAP (e-posta iletişimi) ve FTP (dosya transferi) yer alır. Bu protokoller, bilgisayar ağlarının sağlıklı ve güvenli bir şekilde çalışmasını sağlamak için kullanılır ve ağ yöneticileri tarafından dikkatlice yönetilir. Ağ yönetimi için çeşitli protokoller kullanılır. SNMP, ağ cihazlarının durumunu izlemek ve yönetmek için kullanılırken, NetFlow ağ trafiğini analiz etmek ve kapasite planlaması yapmak için kullanılır. ICMP, ağlardaki erişim sorunlarını teşhis etmek için kullanılır, örneğin, “ping” komutu ICMP protokolünü kullanarak belirli bir IP adresine erişilebilirlik kontrolü yapar. DHCP, ağdaki cihazlara otomatik olarak IP adresleri ve diğer ağ konfigürasyon bilgilerini atayan bir protokoldür. RADIUS, ağ kaynaklarına erişim yetkisini doğrulamak için kullanılırken, SSH güvenli bir şekilde uzaktaki bilgisayarlara erişim sağlamak için kullanılır. Bu protokoller, ağ yöneticilerinin ağlarını izlemek, güvenlik sağlamak, hataları teşhis etmek ve ağ performansını optimize etmek için kullandığı araçlardır.

GÖZDEN GEÇİRELİM

1. **TCP/IP protokol kümesi ne amaçla tasarlanmıştır?**
   a) Video oyunlarını desteklemek için
   b) Veri iletişimini sağlamak ve güvenli veri transferini kolaylaştırmak için
   c) Müzik indirmek için
   d) Sadece e-posta gönderimi için

2. **IP adresi nedir ve ne amaçla kullanılır?**
   a) Bilgisayarların renk kodu
   b) Cihazlara benzersiz bir tanımlayıcı atanması için
   c) Yemek tarifleri saklamak için
   d) İnternet tarayıcılarını güncellemek için

3. **UDP protokolünün en büyük avantajı nedir?**
   a) Hızlı iletim sağlamak
   b) Paket kayıplarını telafi etme yeteneği
   c) Verileri şifreleme yeteneği
   d) Bağlantıyı sürdürme süresi

4. **OSI modeline göre, aşağıdaki katmanlardan hangisi kullanıcı ile etkileşimin olduğu uygulamaların bulunduğu katmandır?**
   a) Transport Layer (Taşıma Katmanı)
   b) Network Layer (Ağ Katmanı)
   c) Application Layer (Uygulama Katmanı)
   d) Data – Link Layer (Veri Bağı Katmanı)

5. **Ağ iletişiminde verilerin başlık bilgileriyle birlikte taşınması sürecine ne ad verilir?**
   a) Kriptografi
   b) Kapsülleme (Encapsulation)
   c) Modülasyon
   d) Kod çözme

6. **TCP/IP modelinde verilerin sinyallere dönüştürülmesi hangi aşamada gerçekleşir?**
   a) Uygulama
   b) Taşıma
   c) İnternet
   d) Ağ Erişim

7. **IP (Internet Protocol) protokolü hangi aşamada kullanıcılara benzersiz tanımlayıcı olan IP adresi atar ve veri paketlerini doğru hedefe yönlendirilmesini sağlar?**
   a) Adresleme rolünde
   b) Paketleme işlevinde
   c) Rotalama aşamasında
   d) Yönlendirme işlevinde

8. **TCP (Transmission Control Protocol) protokolü hangi özelliğiyle veri paketlerinin sıralı, onaylı ve hatasız bir şekilde gönderilip alınmasını sağlar?**
   a) Hata Tespiti ve Düzeltme
   b) Akış Denetimi
   c) Güvenilir Veri Transferi
   d) Bağlantı Yönetimi

9. **DHCP protokolü aşağıdakilerden hangisini gerçekleştirir?**
   a) Ağ trafiğini izleme
   b) Ağdaki cihazların benzersiz IP adreslerini otomatik olarak atama
   c) Ağ kaynaklarına erişim yetkisini doğrulama
   d) Uzaktaki bilgisayarlara güvenli bir şekilde erişim sağlama

10. **RADIUS protokolü hangi amaçla kullanılır?**
   a) Uzaktaki bilgisayarlara güvenli bir şekilde erişim sağlama
   b) Ağ kaynaklarına erişim yetkisini doğrulama
   c) Ağdaki cihazların benzersiz IP adreslerini otomatik olarak atama
   d) Ağ trafiğini izleme

Yanıt Anahtarı: 1-B, 2-B, 3-A, 4-C, 5-B, 6- D, 7-A, 8-C, 9-B, 10-B

Kaynakça

Comer, D. E. (2018). The Internet book: everything you need to know about computer networking and how the Internet works. CRC Press.

Edelman, J., Lowe, S. S., & Oswalt, M. (2018). Network Programmability and Automation: Skills for the Next-Generation Network Engineer. O'Reilly Media. https://books.google.com.tr/books?id=PjJKDwAAQBAJ

GUPTA, P. C. (2006). Data Communication and Computer Networks. PHI Learning. https://books.google.com.tr/books?id=-kNn_p6WA38C

Halsall, F. (1995). Data communications, computer networks and open systems. Addison Wesley Longman Publishing Co., Inc.

Kurose, J., & Ross, K. (2018). Computer Networking: A Top-Down Approach, Global Edition. Pearson Education. https://books.google.com.tr/books?id=IUh1DQAAQBAJ

Mitrou, N. (2004). Networking 2004: Networking Technologies, Services, and Protocols ; Performance of Computer and Communications Networks ; Mobile and Wireless Communications ; Third International IFIP-TC6 Networking Conference, Athens, Greece, May 9 - 14, 2004 ; Proceedings. Kluwer Academic Publishers.

Newman, M. (2018). Networks. Oxford university press.

Robertazzi, T. G. (2000). Computer networks and systems: queueing theory and performance evaluation. Springer Science \& Business Media.

Bergel C. Bilgisayar Ağları Ve Güvenlik. Sakarya University Journal of Science. 2004; 8(1): 5-8.

Sütçü, C. "Bilgisayar ve Bilgisayar Ağları". Marmara İletişim Dergisi 5 (1994): 145-152

Okuma Listesi

https://www.sbb.gov.tr/wp-content/uploads/2022/08/Bilgisayar-Aglari-ile-Ilgili-Suclar-Siber-Suclar-Oguz-Turhan.pdf

https://acikders.ankara.edu.tr/pluginfile.php/155273/mod_resource/content/0/1.1.%20A%C4%9F%20T%C3%BCrleri.pdf

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

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

BÖLÜM 4

SANAL ÖZEL AĞ

ANAHTAR KAVRAMLAR

Sanal Özel Ağ, Şifreleme Fonksiyonları, Bütünlük Fonksiyonları, Kimlik Doğrulama Algoritmaları, Ipsec, VPN Türleri, VPN'in Avantajları

ÖĞRENME HEDEFLERİ

1. VPN teknolojisine neden ihtiyaç duyulduğunu açıklar
2. VPN'in çalışma prensibini açıklar
3. VPN yapısında kullanılan kriptografik algoritmaları açıklar
4. Simetrik ve asimetrik şifreleme algoritmalarına örnekler verir
5. Hash fonksiyonlarının amacını açıklar
6. IPsec çerçevesini açıklar
7. VPN türlerini bilir
8. VPN türlerinin kullanım amacını açıklar

DÖRDÜNCÜ BÖLÜM

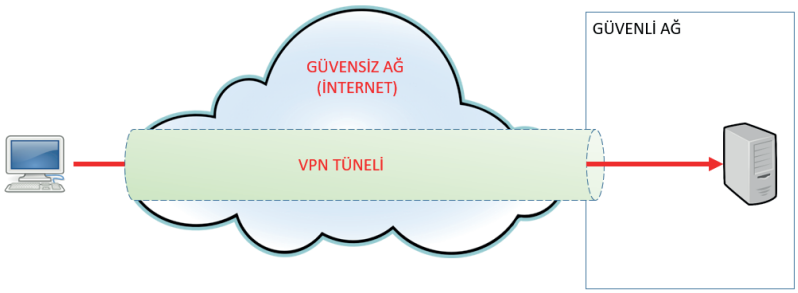
GİRİŞ

Bilgisayar ağlarının devasa bir koleksiyonu olan İnternet, genelde güvensiz bir ortam olarak düşünülür. Kurumlar veya bireyler, siber güvenlik ilkelerini uygulamadıkları taktirde, bu güvensiz ortam üzerinden IP paketleri aracılığıyla taşınan veriler güvende değildir. Bu durumda veriler potansiyel olarak üçüncü taraflarca okunabilir ve değiştirilebilir. Bu nedenle özellikle hassas verilerin güvenliğinin sağlanması gerekir.

Siber güvenliğin üç temel unsuru, gizlilik, bütünlük ve kullanılabilirliktir. İster sabit bir diskte saklanan durağan veriler olsun, ister ağdan akan hareket halindeki veriler olsun, verilerin güvenliğinin sağlanması bu üç temel unsura bağlıdır. Yani veriler internet ortamındaki IP paketleri içerisinde akışı esnasında şifrelenmesi (gizlilik), verinin değişip değişmediğinin belirlenmesi (bütünlük) ve verilerin kaynağının doğrulanması siber güvenliğin gerektirdiği bir ihtiyaçtır.

İnternet ve ağ ortamında hareket eden veriler IP paketlerinin içerisinde belirli boyutlarda yükler olarak taşınırlar. IP ise tasarımı gereği güvenli bir protokol değildir. Yani şifreleme, kimlik doğrulama ve bütünlük tasarım olarak IP protokolünde yoktur. Bu nedenle IP'nin güvenli bir şekilde taşınabilmesi için geliştirilen çeşitli yöntemlerden biri **Sanal Özel Ağ (Virutal Private Network - VPN)** kullanmaktır.

VPN teknolojisinde iletişim kuran taraflar arasında *tünel* olarak adlandırılan özel kanallar kullanılır. Şekil 1'de basit bir VPN tüneli yapısı gösterilmektedir.



Şekil 1. VPN Tünelinin yapısı

VPN tüneli, internet trafiğini şifreleyerek ve güvenli bir şekilde ileterek, kullanıcıya veya kuruma güvenli bir şekilde veri iletim imkânı sunar(P. Ferguson & Huston, 1998).

VPN, çeşitli kriptografik algoritmalar ve teknikler kullanılarak, IP'de tasarımsal olarak var olmayan özelliklerin sonradan eklenmesini sağlayan bir teknoloji kümesidir(Ezra ve diğerleri, 2022). VPN sayesinde IP paketlerinin içerikleri (yükleri) desteklenen çeşitli kriptografik algoritmalar aracılığıyla şifrelenebilir. Benzer şekilde verilerin değişip değişmediğini doğrulamak için bütünlük sağlayıcı kriptografik algoritmalar VPN yapısında kullanılır. Yine VPN yapısında kimlik doğrulama ve inkâr edilememezlik sağlayan kriptografik fonksiyonlar kullanılabilir. Bu nedenle bu bölümde öncelikle VPN için son derece önemli olan kriptografik algoritmalar kısaca açıklanacaktır.

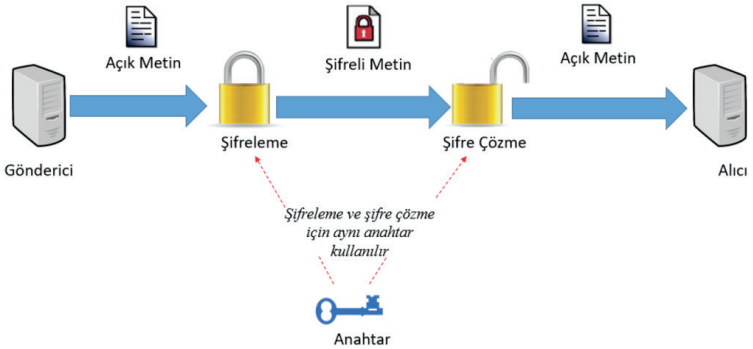
1. KRİPTOGRAFİK ALGORİTMALAR

VPN yapısında kullanılan kriptografik algoritmalar, internet trafiğini şifrelemek ve güvenli bir şekilde iletmek için kritik bir rol oynar. Bu algoritmalar, kullanıcı verilerini koruyarak gizliliği sağlamak, veri bütünlüğünü korumak ve güvenli bir iletişim kanalı oluşturmak amacıyla özenle seçilir ve konfigüre edilir.

2. ŞİFRELEME ALGORİTMALARI

Şifreleme algoritmaları veri gizliliğini sağlayan kriptografik matematiksel fonksiyonlardır. Şifreleme, verileri anahtar (key) denen bir veri ile dönüştürerek, yalnızca doğru anahtara sahip olan kişilerin veya sistemlerin verileri okuyabilmesini sağlar. Bir şifreleme algoritması, metni veya veriyi şifrelerken belirli bir anahtarla birlikte matematiksel operasyonları uygular. Şifreleme, bilgisayarlar arası iletişimden veri depolamaya, çevrimiçi bankacılıktan dosya şifrelemeye kadar birçok farklı uygulamada kullanılır. Şifreleme, hassas verilerin güvenliğini sağlamak için temel bir araçtır ve kritik bir öneme sahiptir.

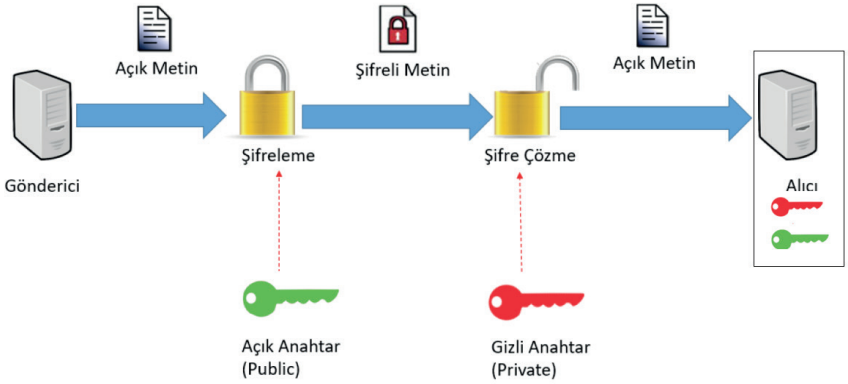
Genelde simetrik ve asimetrik olmak üzere iki tür şifreleme algoritması bulunur. Simetrik şifrelemede veriyi şifrelemek ve şifreyi çözmek için aynı anahtar kullanılır(Alenezi ve diğerleri, 2020) (Şekil 2).



Şekil 2. Simetrik şifreleme

Simetrik şifrelemede kullanılan anahtar, gönderici ve alıcı tarafından bilinmelidir. Bu anahtar sadece bu iki taraf arasında paylaşılır ve gizli kalır. Bu nedenle bu tür anahtarlara *gizli anahtar* denir.

Asimetrik şifrelemede ise veriyi şifrelemek ve deşifre etmek için birbiri ile matematiksel ilişkili bir anahtar çifti kullanılır. Bu anahtar çiftinden şifrelemeyi sağlayan anahtara açık anahtar (public key), şifre çözmeyi sağlayan anahtara ise gizli anahtar (private key) denir. Şekil 3'te asimetrik anahtar yapısı gösterilmektedir.



Şekil 3. Asimetrik şifreleme

Açık anahtar, veriyi şifrelemek isteyen herkes ile açık bir şekilde paylaşılabilir. Açık anahtar şifre çözme için kullanılamayacağı için, anahtara sahip farklı kişiler olsa bile şifrelenmiş veri çözümlenemez. Şifre çözme için kullanılan anahtar ise sadece bir tarafta ve paylaşılmadan gizli olarak tutulur. Böylece açık anahtara sahip olan herkes birbirlerinin verilerini deşifre edemeden güvenli bir şekilde gönderebilir. Şifre çözme işlemi sadece gizli anahtara sahip tarafça yapılır.

Simetrik ve asimetrik şifreleme, VPN yapısında farklı amaçlar doğrultusunda kullanılır. Simetrik şifreleme hızlı olduğu için genelde IP paketlerinin şifrelenmesinde kullanılırken, asimetrik şifreme kimlik doğrulama sürecinde anahtar değişimi için kullanılır. VPN yapısında yaygın olarak kullanılan simetrik şifreleme algoritmaları şunlardır:

Veri Şifreleme Standardı (DES) : Verileri şifrelemek için kullanılan eski bir simetrik şifreleme algoritmasıdır. DES, Amerika Birleşik Devletleri Ulusal Standartlar Enstitüsü (NIST) tarafından 1977 yılında yayınlanmıştır ve daha sonraki yıllarda daha güvenli şifreleme algoritmalarıyla yer değiştirmiştir. DES, 64-bit bloklar halinde çalışır ve 56-bitlik bir anahtar kullanır. Yani, şifrelenecek metin 64-bitlik bloklara bölünür ve bu bloklar aynı anahtar kullanılarak şifrelenir. Dezavantajı, 56-bitlik anahtarın günümüz standartlarında yeterince güvenli olmamasıdır; modern bilgisayar gücü, kısa anahtarları daha hızlı kırabilir.

Bu nedenle, DES günümüzde genellikle daha güçlü ve güvenli şifreleme algoritmalarına yerini bırakmıştır. Ancak DES, şifreleme tarihinde önemli bir dönemeç olarak kabul edilir ve simetrik şifreleme alanında temel bir anlayışı temsil eder.

Gelişmiş Şifreleme Standardı (AES) : Verileri şifrelemek için kullanılan güçlü ve yaygın bir simetrik şifreleme algoritmasıdır. AES, DES gibi eski şifreleme standartlarını yerine geçmek üzere 2001 yılında Amerika Birleşik Devletleri Ulusal Standartlar Enstitüsü tarafından belirlenmiştir(Su ve diğerleri., 2019).

AES, 128-bit, 192-bit ve 256-bit olmak üzere üç farklı anahtar uzunluğunu destekler. Bu, daha güçlü şifreleme seçeneklerini sunar ve şifrelenmiş verilerin daha güvenli hale getirilmesine olanak tanır(Muttaqin & Rahmadoni, 2020). AES,

bilgisayarlar arası iletişimden dosya şifrelemeye kadar bir dizi uygulamada kullanılır ve günümüzde genellikle standart şifreleme ihtiyaçlarını karşılamak için tercih edilen bir algoritmadır. AES, hızlı ve etkili bir şekilde çalışırken güçlü güvenlik sağlar. Bu özellikleri nedeniyle, VPN, veri depolama ve diğer birçok uygulama için yaygın olarak kullanılır. AES, bilgisayar güvenliği açısından kritik bir rol oynar ve dünya genelinde birçok şifreleme uygulamasında standart olarak kabul edilir(Mouha ve diğerleri, 2021).

VPN'lerde sıkça kullanılan asimetrik şifreleme algoritmalarından bazıları aşağıda özetle açıklanmıştır.

RSA (Rivest-Shamir-Adleman): RSA, genel anahtar altyapısını kullanan en yaygın asimetrik şifreleme algoritmalarından biridir. Anahtar değişiminde ve dijital imzalarda sıklıkla kullanılır(Obaid, 2020).

Diffie-Hellman Anahtar Değişimi: Diffie-Hellman (DH) anahtar değişimi protokolü, iki taraf arasında güvenli bir şekilde ortak bir anahtar oluşturmak için kullanılır(Purohit ve diğerleri, 2020). Bu anahtar daha sonra simetrik şifreleme anahtarlarını güvenli bir şekilde değiştirmek için kullanılabilir.

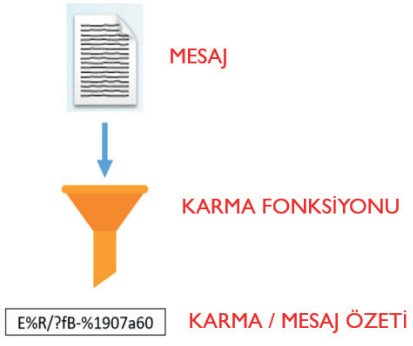
Eliptik Eğri Kriptografisi (ECC): ECC, daha küçük anahtar uzunluklarıyla güçlü şifreleme sağlayabilen bir asimetrik şifreleme algoritmasıdır(Miller, 1985). ECC, daha düşük hesaplama gücü ve daha az bant genişliği kullanımıyla özellikle mobil cihazlar için idealdir.

Bu algoritmalar, VPN'lerde güvenli anahtar değişimi ve dijital imzalama için kullanılır. VPN sağlayıcıları genellikle kullanıcılara güvenli bir anahtar değişimi için uygun algoritmaları seçmelerini sağlar ve genellikle güvenlik standartlarına ve kullanım senaryolarına bağlı olarak uygun olan algoritmaları belirler.

3. BÜTÜNLÜK ALGORİTMALARI

Bütünlük (integrity) algoritmaları, verilerin bütünlüğünü sağlamak için VPN yapısında kullanılır. Bu algoritmalar, verilerin iletim sırasında değiştirilip değiştirilmediğini doğrular. Verilerin güvenli bir şekilde iletilmesi esnasında, verilerin bütünlüğü sağlanarak, verilerin izinsiz değiştirilmesi veya bozulması önlenir.

Veri bütünlüğünü sağlamak için *hash* (bazen karma veya özet olarak da adlandırılır) fonksiyonları kullanılır (Şekil 3).



Şekil 4. Hash algoritmalarının çalışma mantığı

Kriptografi alanında hash fonksiyonu, bir girdiyi (mesaj, veri veya dosya) hash değeri veya mesaj özeti (message digest) olarak bilinen sabit boyutlu bir karakter dizisine dönüştürme işlemidir. Bu dönüşüm, girdi verisine matematiksel bir algoritma uygulanarak elde edilir. Karma işlemin sonucu, orijinal mesajın sabit uzunluktaki bir parmak izi olarak düşünülebilir. Bu nedenle bazen bir mesaj özeti olarak da adlandırılır.

En yaygın kullanılan bütünlük algoritmaları şunlardır:

HMAC (Hash-based Message Authentication Code): HMAC, bir hash fonksiyonu (örneğin, SHA-256) kullanarak verilere özel bir doğrulama kodu ekler. Bu işlem hem bütünlüğü doğrular hem de verinin doğruluğunu sağlar.

SHA-2 (Secure Hash Algorithm 2): SHA-2 ailesi, 224, 256, 384, 512 bitlik hash fonksiyonları içerir. Özellikle SHA-256 ve SHA-512, genellikle bütünlük doğrulaması için kullanılır(Gupta & Kumar, 2014).

MD5 (Message Digest Algorithm 5): MD5, 128-bit hash değeri üreten eski bir hash fonksiyonudur(Yong-Xia & Ge, 2010). Ancak, günümüzde güvenlik açıkları nedeniyle önerilmez(Gupta & Kumar, 2014).

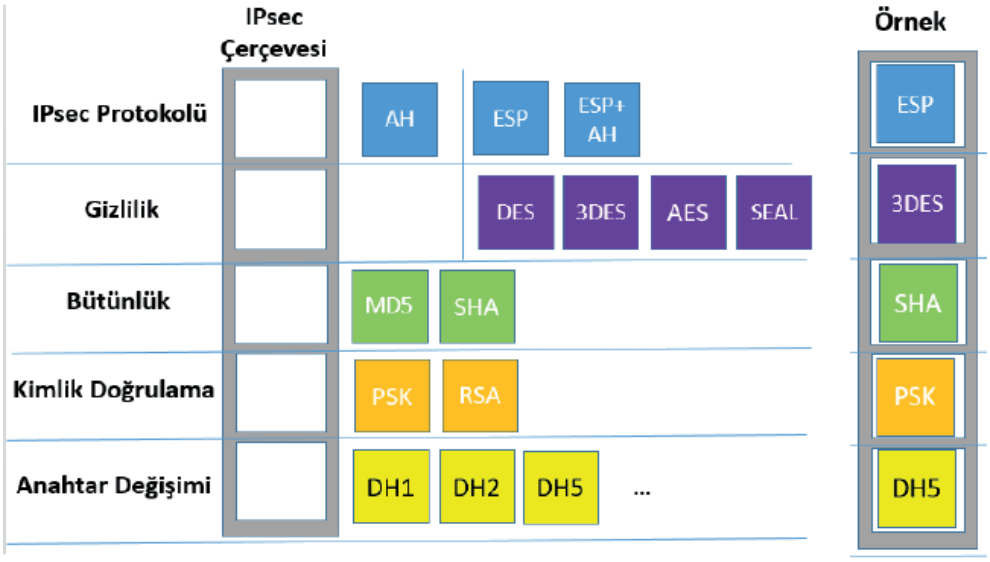
Bu algoritmalar, verilerin bütünlüğünü doğrulamak için kullanılır. Hangi algoritmanın tercih edileceği, kullanım senaryosuna ve güvenlik gereksinimlerine bağlı olarak değişebilir. Daha yüksek güvenlik seviyeleri gerektiren durumlarda HMAC ve SHA-2 gibi güçlü ve güvenilir algoritmalar tercih edilir.

4. IPsec ÇERÇEVESİ

IPsec (Internet Protocol Security), internet üzerinden veri iletimini güvenli hale getirmek için kullanılan bir güvenlik çerçevesidir (framework) (N. Ferguson & Schneier, 1999). IPsec, veri bütünlüğünü doğrulama, verileri şifreleme ve kimlik doğrulama gibi güvenlik hizmetlerini sağlayarak internet trafiğini korur. IPsec, genellikle VPN bağlantılarında, uzaktan erişimde, güvenli ağ bağlantılarında ve sanal özel ağlarda (VLAN) kullanılır.

IPsec, IP paketlerini şifreleyerek ve/veya doğrulayarak iletim sırasında verilerin gizliliğini ve bütünlüğünü sağlar. Ayrıca, IPsec, veri iletimi sırasında paketleri kimlik doğrulama sürecinden geçirerek güvenilirliği artırır. Bu şekilde, internet üzerinden veri iletimi güvenli hale gelir ve izinsiz erişim, veri değişiklikleri veya veri manipülasyonu gibi tehditlere karşı koruma sağlanır.

IPsec, iki ana bileşenden oluşur: AH (Authentication Header) ve ESP (Encapsulating Security Payload)(Madson & Glenn, 1998). AH, veri bütünlüğünü doğrularken, ESP, verileri şifreleyerek ve/veya doğrulayarak güvenlik sağlar. IPsec, özellikle şirket içi ağlardan uzaktan erişime kadar bir dizi uygulama senaryosunda güvenli iletişim sağlamak için kullanılır.



Şekil 5. IPsec çerçevesi ve örnek poliçe

Şekil 5'te gösterilen IPsec çerçevesi, IP'nin güvenli transferi için gereken gizlilik, bütünlük ve kimlik doğrulama gibi ek özellikleri sağlar. Şekil 5'deki örnekte desteklenen ek özellikler ile bir poliçe oluşturulur. Böylece bu poliçeyi destekleyen taraflarla güvenli VPN bağlantısı kurulabilir.

5. VPN TÜRLERİ

İnternet üzerinde güvenli bir şekilde veri iletimi sağlamak için kullanılan VPN'ler, farklı kullanım senaryolarına uygun olarak farklı türlerde olabilir. Yaygın olarak kullanılan VPN türlerinin bazıları aşağıda tanımlanmıştır.

Uzaktan Erişim VPN (Remote Access VPN): Uzaktan erişim VPN'leri, uzak kullanıcıların güvenli bir şekilde şirket içi ağa veya başka bir özel ağa erişmesine olanak tanır. Bu tür VPN'ler, evden çalışan personel veya seyahat eden çalışanlar gibi uzaktan çalışan kullanıcılar için idealdir.

Remote Access VPN'in çalışma şekli aşağıda adımlar halinde ifade edilmiştir.

• *Kimlik Doğrulama*: Uzaktan erişim VPN'i kullanıcılardan kimlik doğrulama bilgilerini (kullanıcı adı, şifre, vb.) talep eder. Bu adım, doğru kullanıcıların sisteme giriş yapmasını sağlar.

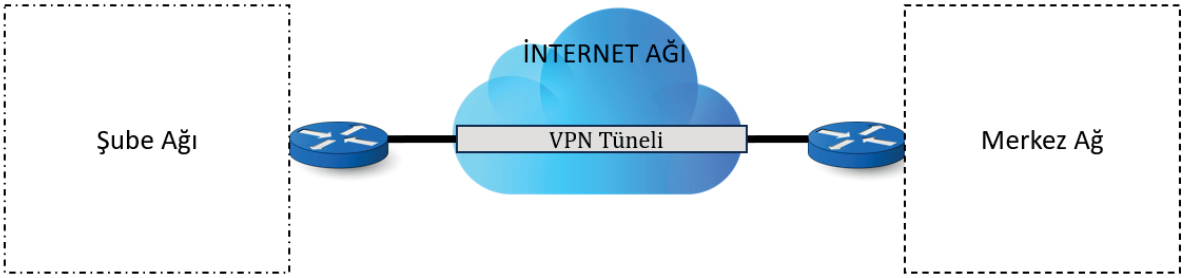
• *Şifreleme*: Kullanıcının bilgisayarındaki VPN istemcisi, şirket içi ağa giden veriyi şifreler. Bu şifreleme, verilerin güvenli bir şekilde iletilmesini sağlar. Genellikle SSL/TLS veya IPSec protokolleri kullanılarak şifreleme gerçekleştirilir.

• *Uzaktan Bağlantı Kurma*: Kullanıcı, VPN istemcisini kullanarak uzaktan şirket içi ağa bağlanır. Bağlantı, genellikle internet üzerinden yapılır. VPN istemcisi, kullanıcının cihazı ve şirket içi ağ arasında güvenli bir tünel oluşturur.

• *Tünel Oluşturma*: Şirket içi ağdaki VPN sunucusu, uzaktaki kullanıcıya özel bir ağ tüneli oluşturur. Bu tünel, kullanıcının verilerinin şifrelenmiş bir şekilde şirket içi ağa iletilmesini sağlar.

• *Güvenli Erişim*: Uzaktan erişim VPN'i ile kullanıcılar, şirket içi ağda bulunan kaynaklara (dosyalar, yazıcılar, veritabanları, uygulamalar vb.) güvenli bir şekilde erişebilir. Bu erişim, sanki kullanıcı şirket içi ağda fiziksel olarak bulunuyormuş gibi sağlanır.

Site-to-Site VPN: Site-to-Site VPN'ler, iki veya daha fazla şirket içi ağı arasında güvenli bir bağlantı sağlar. Bu tür VPN'ler, genellikle şirketler veya uzak şubeler arası güvenli veri paylaşımı gerektiğinde kullanılır(Santoso et al., 2021). Şekil 5'te Site-to-Site VPN örneği gösterilmiştir.



Şekil 6. Site-to-Site VPN örneği

Site-to-Site VPN yapısında, uzak iki ağın güvensiz bir ortamda tünel kurularak güvenli iletişim yapması sağlanır. VPN yapılandırması her iki ağın sınır cihazlarında yapılır. Bu sayede ağ içerisinde yer alan kullanıcıların herhangi bir yapılandırma yapmasına gerek kalmaz(Rathore et

al., 2009). Ayrıca çoğu durumda son kullanıcılar VPN'in varlığından haberi olmaz.

Site-to-Site VPN'in çalışma şekli aşağıda adımlar halinde verilmiştir.

• *Noktadan Noktaya Bağlantı*: Farklı konumlardaki şirket içi ağlar, internet üzerinden noktadan noktaya (site-to-site) bağlantı kurarlar. Bu bağlantılar genellikle internet bağlantıları üzerinden gerçekleştirilir.

• *Tünel Oluşturma*: Şirket içi ağlardaki VPN cihazları (genellikle VPN gateway'ler olarak adlandırılır), şifreli bir tünel oluşturur. Bu tünel, şifrelenmiş verilerin güvenli bir şekilde iletilmesini sağlar. Genellikle IPSec protokolü kullanılarak şifreleme yapılır.

• *Güvenli Veri İletimi*: Veriler, şifrelenmiş tünelden geçerek güvenli bir şekilde diğer şirket içi ağına iletilir. Bu şifreleme, verilerin güvenliği ve gizliliği için önemlidir.

• *Farklı Kaynaklara Erişim*: Bağlı şirket içi ağlar, birbirlerine ait kaynaklara (dosyalar, sunucular, yazıcılar, uygulamalar vb.) güvenli bir şekilde erişebilirler. Bu durum, farklı ofisler veya şirket içi departmanlar arasında işbirliği ve veri paylaşımını mümkün kılar(Dhall et al., 2012).

Extranet VPN: Extranet VPN'ler, farklı şirketler veya organizasyonlar arasında güvenli veri paylaşımını mümkün kılar. Extranet VPN'ler, iş ortakları veya tedarikçiler gibi harici kullanıcılarla güvenli bir şekilde bilgi paylaşımını destekler.

Intranet VPN: Intranet VPN'ler, aynı şirket veya organizasyonun farklı fiziksel konumları arasında güvenli bir ağ bağlantısı oluşturur. Bu tür VPN'ler, farklı ofisler veya departmanlar arasında güvenli veri paylaşımını sağlamak için kullanılır.

Mobile VPN: Mobile VPN'ler, hareket halindeki kullanıcılara güvenli bir şekilde bağlanma imkanı sağlar(Shneyderman & Casati, 2003). Bu tür VPN'ler, mobil cihazlar (cep telefonları, tabletler) üzerinden güvenli bir internet erişimi sağlayarak kullanıcıların güvenli bir şekilde gezinmesini sağlar.

SSL VPN (Secure Sockets Layer Virtual Private Network): SSL VPN internet üzerinden güvenli bir şekilde uzaktan erişim sağlamak için kullanılan bir VPN türüdür. SSL VPN, SSL/TLS (Secure Sockets Layer/Transport Layer Security) protokollerini kullanarak güvenli şifreleme ve kimlik doğrulama sağlar. Bu şekilde, kullanıcılar şirket içi ağa veya kaynaklara güvenli bir şekilde erişebilirler.

SSL VPN, genellikle web tarayıcıları üzerinden erişim sağlama imkânı sunar. Bu, kullanıcıların özel bir VPN istemcisi yerine sadece bir web tarayıcısı ile güvenli erişime sahip olmalarını sağlar. Kullanıcılar, güvenli bir SSL bağlantısı aracılığıyla özel şirket kaynaklarına, dosya sunucularına, veritabanlarına veya web uygulamalarına erişebilir.

SSL VPN, kullanıcıların herhangi bir yerden ve herhangi bir cihazdan (bilgisayar, tablet, cep telefonu) güvenli bir şekilde şirket içi ağlarına veya kaynaklarına erişmelerini sağlayarak mobil çalışma ve uzaktan erişim için ideal bir çözümdür.

Her bir VPN türü, farklı kullanım senaryolarına ve güvenlik gereksinimlerine uygun olarak seçilir ve yapılandırılır.

5.1. VPN'in Avantajları

VPN, internet üzerindeki veri iletimini şifreleyerek güvenli bir şekilde IP iletişimi sağlar. Bu, verilerin izinsiz erişim veya manipülasyondan korunmasını sağlanır. Ayrıca VPN, kullanıcılara ve kurumlara güvenliğin haricinde bir dizi avantaj da sunar. Bu avantajlar aşağıda özetle ifade edilmiştir.

Uzaktan Erişim: Uzaktan erişim VPN'leri, çalışanların veya uzaktan kullanıcıların şirket içi ağa

güvenli bir şekilde erişmesini sağlar. Bu, uzaktan çalışma olanaklarını artırır.

Gizlilik ve Anonimlik: VPN, kullanıcıların çevrimiçi aktivitelerini gizleyerek ve gerçek IP adreslerini gizleyerek anonim kalmasını sağlar.

Verimlilik ve Güvenlik: VPN, şirket içi çalışanlar veya uzaktan kullanıcılar için güvenli bir şekilde veri paylaşımını sağlar. Bu, işbirliğini artırır ve verimliliği destekler.

Açık WiFi Ağlarında Güvenlik: VPN, açık veya kamu WiFi ağlarında güvenli bir bağlantı sağlayarak kullanıcıları siber saldırılardan korur.

Daha Fazla Gizlilik Kontrolü: Kurumsal VPN'ler, şirket içi verilerin kontrol edilmesi ve izlenmesi için ek araçlar sağlayarak gizliliği artırır.

Maliyet Tasarrufu: VPN, özel ağ kiralama maliyetinden tasarruf sağlar. Uzaktan çalışanlar veya uzak ofisler arasındaki güvenli iletişim için ekstra maliyetli hatlar gerekmez.

Bu avantajlar, VPN'lerin kullanımını yaygınlaştırmış ve çeşitli sektörlerde güvenli iletişim ihtiyaçlarını karşılamak için önemli bir araç haline getirmiştir.

BÖLÜM ÖZETİ

Bu bölümde, VPN teknolojisinin temel prensiplerini, kriptografik algoritmaları ve çeşitli VPN türleri ele alınmıştır. VPN, internet üzerinde veri iletimini güvenli hale getirmek için kullanılan bir teknolojidir. Temel amaçlarından biri, verilerin güvenli bir şekilde iletilmesini sağlamak, gizliliği korumak, bütünlüğü doğrulamak ve kimlik doğrulamayı gerçekleştirmektir. VPN'ler, farklı kullanım senaryolarına uygun olarak farklı türlerde olabilir. Uzaktan erişim VPN'leri, uzak kullanıcıların güvenli bir şekilde şirket içi ağa veya başka bir özel ağa erişmesine olanak tanır. Site-to-Site VPN'ler, iki veya daha fazla şirket içi ağı arasında güvenli bir bağlantı sağlar. Extranet VPN'ler, farklı şirketler veya organizasyonlar arasında güvenli veri paylaşımını mümkün kılar. Intranet VPN'ler, aynı şirket veya organizasyonun farklı fiziksel konumları arasında güvenli bir ağ bağlantısı oluşturur. Mobile VPN'ler, hareket halindeki kullanıcılara güvenli bir şekilde bağlanma imkânı sağlar. SSL VPN ise internet üzerinden güvenli bir şekilde uzaktan erişim sağlamak için kullanılan bir VPN türüdür. VPN kullanmanın avantajları arasında uzaktan erişim imkânı gizlilik ve anonimlik, verimlilik ve güvenlik, açık WiFi ağlarında güvenlik, daha fazla gizlilik kontrolü ve maliyet tasarrufu yer alır. VPN, açık WiFi ağlarında güvenli bir bağlantı sağlayarak kullanıcıları siber saldırılardan korurken, aynı zamanda şirket içi verilerin güvenli bir şekilde paylaşılmasını ve iş birliğini destekler. VPN teknolojisi, günümüzde birçok organizasyon ve birey için temel bir güvenlik önlemi olarak önemli bir rol oynamaktadır.

GÖZDEN GEÇİRELİM

1. **Siber güvenliğin temel unsurları nelerdir?**
   a) Yalnızca gizlilik
   b) Bütünlük, gizlilik ve kullanılabilirlik
   c) Yalnızca bütünlük
   d) Bütünlük ve güvenilirlik

2. **VPN nedir?**
   a) Veritabanı Yönetim Sistemi
   b) Virüs Programı
   c) Sanal Özel Ağ
   d) İnternet Tarayıcısı

3. **Simetrik şifreleme ile ilgili doğru bir ifade hangisidir?**
   a) Aynı anahtar kullanılır veriyi şifrelemek ve çözmek için
   b) Farklı anahtarlar kullanılır veriyi şifrelemek ve çözmek için
   c) Açık anahtar kullanılır
   d) Şifreleme kullanılmaz

4. **SHA-2 hangi türde bir kriptografik algoritmadır?**
   a) Hash Fonksiyonu
   b) Asimetrik Şifreleme
   c) Simetrik Şifreleme
   d) Kimlik Doğrulama Protokolü

5. **IPsec'in ana bileşenleri nelerdir?**
   a) SHA ve AES
   b) AH ve ESP
   c) SSL ve TLS
   d) DNS ve DHCP

6. **Site-to-Site VPN ne tür bir VPN bağlantısını tanımlar?**
   a) Uzaktan Erişim VPN
   b) Şirket İçi VPN
   c) Farklı şirket içi ağlar arasında güvenli bağlantı
   d) Mobil VPN

7. **SSL VPN hangi protokolleri kullanarak güvenli şifreleme ve kimlik doğrulama sağlar?**
   a) IPSec
   b) SSL/TLS
   c) HMAC
   d) RSA

8. **Hangisi VPN'in avantajlarından biridir?**
   a) Maliyet artışı
   b) Kullanıcıların gerçek IP adreslerini açığa çıkarır
   c) Açık WiFi ağlarında güvenliği azaltır
   d) Uzaktan erişim ve gizlilik sağlar

9. Bütünlük algoritmaları hangi amaçla kullanılır?

a) Verileri şifrelemek
b) Verilerin bütünlüğünü sağlamak
c) Kimlik doğrulamak
d) Ağ trafiğini yönlendirmek

10. Hangisi asimetrik şifreleme algoritmalarından biri değildir?

a) RSA
b) Diffie-Hellman Anahtar Değişimi
c) AES
d) Eliptik Eğri Kriptografisi (ECC)

Yanıt Anahtarı: 1-B, 2-C, 3-A, 4-A, 5-B, 6-C, 7-B, 8-D, 9-B, 10-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.

Dhall, H., Dhall, D., Batra, S., & Rani, P. (2012). Implementation of IPSec protocol. *2012 Second International Conference on Advanced Computing \& Communication Technologies*, 176–181.

Ezra, P. J., Misra, S., Agrawal, A., Oluranti, J., Maskeliunas, R., & Damasevicius, R. (2022). Secured communication using virtual private network (VPN). *Cyber Security and Digital Forensics: Proceedings of ICCSDF 2021*, 309–319.

Ferguson, N., & Schneier, B. (1999). *A cryptographic evaluation of IPsec*.

Ferguson, P., & Huston, G. (1998). *What is a VPN?*

Gupta, P., & Kumar, S. (2014). A comparative analysis of SHA and MD5 algorithm. *Architecture*, *1*(5).

Madson, C., & Glenn, R. (1998). *The use of HMAC-MD5-96 within ESP and AH*.

Miller, V. S. (1985). Use of elliptic curves in cryptography. *Conference on the Theory and Application of Cryptographic Techniques*, 417–426.

Mouha, N., Dworkin, M., & others. (2021). Review of the advanced encryption standard. *Technical Report, National Institute of Standards and Technology*.

Muttaqin, K., & Rahmadoni, J. (2020). Analysis and design of file security system AES (advanced encryption standard) cryptography based. *Journal of Applied Engineering and Technological Science (JAETS)*, *1*(2), 113–123.

Obaid, T. S. (2020). Study a public key in RSA algorithm. *European Journal of Engineering and Technology Research*, *5*(4), 395–398.

Purohit, K., Kumar, A., Upadhyay, M., & Kumar, K. (2020). Symmetric key generation and distribution using Diffie-Hellman algorithm. In *Soft Computing: Theories and Applications: Proceedings of SoCTA 2019* (pp. 135–141). Springer.

Rathore, M. S., Razzaq, A., Hidell, M., & Sjödin, P. (2009). *Site-to-Site VPN Technologies: A Survey*.

Santoso, B., Sani, A., Husain, T., & Hendri, N. (2021). VPN Site To Site Implementation Using Protocol L2TP And IPSec. *TEKNOKOM*, *4*(1), 30–36.

Shneyderman, A., & Casati, A. (2003). *Mobile VPN: delivering advanced services in next generation wireless systems*. John Wiley \& Sons.

Su, N., Zhang, Y., & Li, M. (2019). Research on data encryption standard based on aes algorithm in internet of things environment. *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, 2071–2075.

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

Okuma Listesi

Kaya ve İ. Türkoğlu , "Simetrik ve Asimetrik Şifreleme Algoritmalarının Performans Karşılaştırılması", *Fırat Üniversitesi Mühendislik Bilimleri Dergisi*, c. 35, sayı. 2, ss. 891-900, Eyl. 2023, doi:10.35234/fumbd.1296228

Yerlikaya, T. , Gençoğlu, H. , Emir, M. K. , Çankaya, M. & Buluş, E. (2011). RSA ŞİFRELEME ALGORİTMASI VE ARİTMETİK MODÜL UYGULAMASI . İstanbul Aydın Üniversitesi Dergisi , 3 (9) , 95-104 . Retrieved from https://dergipark.org.tr/tr/pub/iaud/issue/30054/324501

Beşkirli, A. , Özdemir, D. & Beşkirli, M. (2019). Şifreleme Yöntemleri ve RSA Algoritması Üzerine Bir İnceleme . Avrupa Bilim ve Teknoloji Dergisi , Özel Sayı 2019 , 284-291 . DOI: 10.31590/ejosat.638090

T. Yerlikaya ve N. İşçimen , "ASİMETRİK ŞİFRELEMEDE ASAL SAYILAR VE GÜVENLİK", Trakya Üniversitesi Mühendislik Bilimleri Dergisi, c. 24, sayı. 1, ss. 11-18, Tem. 2023, doi:10.59314/tujes.1303091

Çelik, S. (2021). Kuantum Kriptolojisi ve Siber Güvenlik . Bilişim Teknolojileri Dergisi , 14 (1) , 53-64 . DOI: 10.17671/gazibtd.733309

BÖLÜM 5

BİLGİ GÜVENLİĞİ

ANAHTAR KAVRAMLAR

Bilgi, Veri, Kişisel Veriler, Bilgi Sınıflandırma, Aktif Bilgi Toplama, Pasif Bilgi Toplama

ÖĞRENME HEDEFLERİ

1. Bilgi ve veri kavramlarını açıklar
2. Bilgiyi sınıflandırmanın getirdiği avantajları ifade eder
3. Çeşitli bakış açılarına göre verileri sınıflandırır
4. Özel nitelikli kişisel veriye örnekler verir
5. Çeşitli durumlarda yer alan verilerin güvenliğinin nasıl sağlanacağını açıklar
6. Aktif ve pasif bilgi toplama işlemleri yapar

BEŞİNCİ BÖLÜM

GİRİŞ

Organizasyonların veya bireylerin, bilgi varlıklarını (verileri, bilgisayarları, ağları, yazılımları, donanımları, vb.) yetkisiz erişim, kullanım, ifşa, bozulma, engellenme ve yok olmalara karşı koruma süreci olan bilgi güvenliği, birçok farklı alanı kapsar. Bu alanlar arasında siber güvenlik, fiziksel güvenlik, iş sürekliliği yönetimi, uygunluk yönetimi, risk yönetimi ve kullanıcı eğitimi bulunmaktadır. Alınan önlemler, veri sızıntıları, kimlik hırsızlığı, zararlı yazılımlar, fidye saldırıları ve diğer siber tehditler gibi potansiyel riskleri en aza indirmeyi amaçlar. Kısaca ifade etmek gerekirse bilgi güvenliği, gizlilik, bütünlük ve erişilebilirlik sağlayarak kuruluşun bilgi varlıklarının korunmasını amaçlar(İREN & CAN, 2017).

Bilgi güvenliği, organizasyonlar için kritik bir öneme sahiptir çünkü veri güvenliği ihlalleri, müşteri güvenini zedeler, itibarı olumsuz etkiler ve hukuki sonuçlar doğurabilir. Bu nedenle, bilgi güvenliği stratejileri oluşturmak ve uygulamak, organizasyonların başarılı bir şekilde faaliyet göstermeleri için önemli bir gerekliliktir. Bu süreç, teknoloji, süreçler ve insan davranışları üzerinde odaklanır. Güçlü şifreleme, güvenlik yazılımları, güncelleştirmeler, ağ güvenliği tedbirleri ve eğitim gibi çeşitli unsurları içerir. Ayrıca, bireylerin bilinçlendirilmesi ve güvenlik politikalarına uygun davranmaları da büyük önem taşır.

Bilgi güvenliği, sürekli değişen tehditlere karşı adapte olmak ve gelişen teknolojiyle birlikte güncellenmek zorundadır. Organizasyonlar ve bireyler, bilgi güvenliği konusunda bilinçli ve proaktif olmalı, sürekli olarak güvenlik önlemlerini gözden geçirmeli ve iyileştirmelidir.

Bu bölümde öncelikle veri ve bilgi kavramları ele alınacak, ardından iki farklı bakış açısından veriler sınıflandırılacaktır. Bölümün geri kalan kısmında siber güvenlik perspektifinden bilgi toplama yöntemleri ve stratejiler açıklanacaktır.

1. VERİ VE BİLGİ KAVRAMLARI

Veri, genellikle anlamlı bir bağlam içermeyen temel bilgi parçacıklarıdır. Sayılar, metinler, semboller veya gözlemler gibi çeşitli biçimlerde bulunabilirler. Yâni, işlenmemiş ve organize edilmemiş bilgilerdir. Örneğin, bir dosyadaki sayılar, bir veritabanındaki girişler veya bir ölçü aletinden alınan değerler veri örnekleridir. Bu değerlerin anlam taşıması için bir bağlama ve düzene oturtulması gerekir.

Bilgi ve veri kavramları genelde birbirinin yerine kullanılsa da bilgi; verinin işlenmesi, düzenlenmesi ve yorumlanması sonucu elde edilen ve anlam taşıyan bir yapıdır (CANBEK & SAĞIROĞLU, 2006). O halde bilgi, bir bağlam içinde anlam ifade eden veri koleksiyonudur. Örneğin, bir grup rakam (1, 15, 26 gibi) veri olarak kabul edilir. Ancak, bu rakamlar bir anlam ile ilişkilendirildiğinde bilgi haline gelir. 35 tek başına bir veri iken, ortamın sıcaklığı ile ilişkilendirildiğinde bilgi hâlini alır

Veriden bilgiye geçiş, verinin analiz edilip yorumlanmasıyla gerçekleşir. Örneğin, bir grafikteki sayılar, bir rapordaki istatistikler veya bir olayın neden-sonuç ilişkileri bilgi örnekleridir. Bilgi, insanlar veya sistemler tarafından kullanılarak anlam ve değer kazanır.

Bilgi güvenliği, bu veri ve bilgilerin yetkisiz erişim, kullanım, ifşa, bozulma, engellenme ve yok olmalara karşı korunmasını sağlamayı amaçlar. Bu çerçevede, veri ve bilgilerin gizliliği, bütünlüğü ve erişilebilirliği, bilgi güvenliği stratejilerinin temel odak noktalarını oluşturur.

2. BİLGİYİ SINIFLANDIRMA

Bilgiyi sınıflandırmak, bu bilgilerin önem düzeyine göre gruplandırılmasını ve korunmasını sağlayan bir stratejidir. Bu strateji bağlamında sınıflandırma, genel olarak bir organizasyonun bilgi güvenliğini artırmak ve potansiyel risklere karşı daha dirençli hale getirmek için önemli bir adımdır ve organizasyonlara ve bireylere bir dizi avantaj sağlar(DURNA & DEMİREL, 2008). Bu avantajlar aşağıda özetle ifade edilmiştir.

Gizliliği Sağlama: Bilgi veya verinin sınıflandırılması, gizliliğin korunmasına yardımcı olur. Hassas veya özel bilgiler, genel bilgilerden ayrılarak daha katı güvenlik önlemlerine tabi tutulabilir. Bu sayede yetkisiz erişim ve ifşanın önüne geçilebilir. Veri gizliliğinin sağlanması için genellikle şifreleme algoritmaları kullanılır (TOPALOĞLU v.d., 2016).

Risk Yönetimi: Sınıflandırma, organizasyonların risklerini daha etkili bir şekilde yönetmelerini sağlar. Örneğin, kritik iş bilgileri veya müşteri verileri daha fazla koruma gerektirebilirken, genel bilgiler için daha hafif güvenlik önlemleri yeterli olabilir.

Bütünlüğü Sağlama: Sınıflandırma, bilgi veya verinin bütünlüğünü korumak için önemlidir. Özellikle kritik bilgilerin doğruluğunu ve güvenilirliğini sağlamak adına sınıflandırma önemli bir rol oynar.

Düzenli Erişim Kontrolü: Belirli bilgilerin belirli kişiler veya roller tarafından erişilebilmesini sağlar (BULUT ve diğerleri., 2023). Böylece, güvenlik politikalarının ve erişim kontrollerinin etkili bir şekilde uygulanmasını kolaylaştırır.

Uyumluluğu Sağlama: Çeşitli düzenlemelere ve yasal gereksinimlere uyumu kolaylaştırabilir. Örneğin, kişisel verilerin korunması gerektiği durumlarda sınıflandırma, ilgili düzenlemelere uygunluk sağlar.

Kaynak Yönetimi: Sınıflandırma, organizasyonların kaynaklarını daha etkili bir şekilde yönetmelerini sağlar. Kritik bilgilerin üzerinde odaklanmak, güvenlik kaynaklarının optimal bir şekilde kullanılmasına yardımcı olabilir.

Eğitim ve Farkındalık: Sınıflandırma, çalışanlara hangi bilgilerin daha hassas olduğu konusunda rehberlik eder. Bu da çalışanların bilgi güvenliği politikalarına uymalarını ve daha bilinçli olmalarını sağlar.

2.1. Bilgi Türleri

Bilgi türleri ya da bilgiyi sınıflandırma, çok çeşitli kriterlere ve ihtiyaçlara göre yapılabilir. Burada keskin bir netlik yoktur ve bireye, organizasyona veya amaca göre çeşitli sınıflandırmalar yapılabilir. Aşağıda bu sınıflandırma için genel bazı başlıklar yer almaktadır.

Hassaslık Seviyesine Göre:

• *Kamusal Bilgi:* Genel olarak kamuya açık bilgileri ifade eder.

• *İçsel Bilgi:* Bir organizasyonun iç işleyişi ile ilgili bilgilerdir.

• *Gizli Bilgi:* Sınırlı bir grup insanın bilmesi gereken hassas bilgiler.

İşlevselliğe Göre:

• *Stratejik Bilgi:* Organizasyonun stratejik hedefleriyle ilgili bilgilerdir.

• *Operasyonel Bilgi:* Günlük işlemler ve faaliyetlerle ilgili bilgilerdir.

• *Taktiksel Bilgi:* Stratejik ve operasyonel arasındaki bağlantıyı sağlayan bilgilerdir.

Biçimine Göre:

• *Yazılı Bilgi:* Dokümanlar, raporlar, yazışmalar.

• *Sözlü Bilgi:* Toplantılar, konuşmalar, mülakatlar.

• *Görsel Bilgi:* Grafikler, tablolar, şemalar.

• *Elektronik Bilgi:* Dijital ortamlarda depolanan bilgiler.

İlgili Sektöre Göre:

• *Sağlık Bilgisi:* Tıbbi kayıtlar, hasta bilgileri.

• *Finansal Bilgi:* Mali tablolar, bütçeler, finansal raporlar.

• *Müşteri Bilgisi:* Müşteri verileri, satış bilgileri.

Zaman İçindeki Değişime Göre:

• *Statik Bilgi:* Değişmeyen, sabit bilgiler.

• *Dinamik Bilgi:* Zamanla değişen, güncellenen bilgiler.

Erişilebilirlik Düzeyine Göre:

• *Kamu Bilgisi:* Herkes tarafından erişilebilir bilgilerdir.

• *Sınırlı Erişim Bilgisi:* Belirli bir grup insanın erişebileceği bilgiler.

• *Özel Bilgi:* Sınırlı ve kontrol edilmiş erişime sahip bilgiler.

Öneme Göre:

• *Kritik Bilgi:* Organizasyonun temel faaliyetleri için kritik olan bilgiler.

• *Standart Bilgi:* Günlük operasyonlar için gerekli ancak kritik olmayan bilgiler.

Bu sınıflandırmalar, organizasyonun ihtiyaçlarına ve belirli bir bağlama göre değişebilir. Organizasyonlar genellikle kendi içinde benzersiz bir bilgi sınıflandırma sistemine sahip olabilir ve bu sistem, belirli güvenlik politikalarına ve düzenlemelere uyum sağlamak üzere tasarlanabilir.

2.2. Kişisel Bilgi

Bilgi güvenliği açısından önemli konularından biri de kişisel bilgilerdir. Kişisel bilgi, bir birey hakkında spesifik veya tanımlayıcı olan her türlü veriyi ifade eder. Bu bilgiler, doğrudan bir kişiyi tanımlayabilen veya tanımlamak için kullanılabilen verilerdir. Kişisel bilgiler, genellikle isim, adres, telefon numarası, e-posta adresi, doğum tarihi, kimlik numarası, biyometrik veriler (parmak izi, retinanın taranması gibi), finansal bilgiler (kredi kartı numarası, banka hesap numarası), sağlık bilgileri gibi verileri içerir.

Kişisel bilgiler, bir kişinin kimliğini belirlemek veya bu kişiyi belirli bir şekilde tanımlamak için kullanılabilecek her türlü veriyi içerir. Bu

bilgiler, gizlilik ve güvenlik açısından oldukça hassas olduğundan, genellikle özenle korunması gereken verilerdir. Bu tür bilgilerin yetkisiz kişilerin eline geçmesi, kimlik hırsızlığı, dolandırıcılık ve diğer güvenlik tehditlerine neden olabilir.

Bu nedenle, kişisel bilgilerin toplanması, saklanması ve işlenmesi genellikle yasal düzenlemelere tabidir. Kişisel veri koruma yasaları, bireylerin kişisel bilgilerinin nasıl toplanacağını, nasıl saklanacağını ve nasıl kullanılacağını düzenler. Bu yasalar, kişisel bilgilerin güvenliğini sağlamak ve bireylerin mahremiyetini korumak için önemli bir rol oynar. Aşağıda kişisel bilgilere ilişkin bazı örnekler verilmiştir:

Temel Kimlik Bilgileri:

- Ad
- Soyad
- Doğum tarihi
- Cinsiyet
- Medeni durum

İletişim Bilgileri:

- Adres (ev, iş)
- Telefon numarası (ev, iş, cep)
- E-posta adresi

Kimlik Doğrulama Bilgileri:

- Kimlik numarası
- Pasaport numarası
- Ehliyet numarası

Finansal Bilgiler:

- Banka hesap numarası
- Kredi kartı numarası
- Vergi numarası

Sağlık Bilgileri:

- Tıbbi geçmiş
- Hastalıklar ve tedavilerle ilgili bilgiler
- Reçete bilgileri

Biyometrik Bilgiler:

- Parmak izi verileri
- Retina tarama verileri
- Yüz tanıma verileri

İnternet Kimliği ve Aktivite Bilgileri:

- Kullanıcı adları
- Parolalar
- İnternet tarayıcı geçmişi
- IP adresleri

Aileye İlişkin Bilgiler:

- Çocukların adı
- Ebeveyn bilgileri
- Anne kızlık soyadı

Eğitim Bilgileri:

- Mezun olduğu okul
- Ders başarı puanları
- Aldığı sertifikalar

Bu bilgilerin haricinde kişiyi tanımlayabilecek diğer verilerin olduğunu unutmamak gerekir. Örneğin bireylerin özel hayatına, sağlığına, cinsel hayatına, ırkına, etnik kökenine, dini inançlarına veya siyasi görüşlerine dair bilgiler de kişisel bilgi kapsamına girer. Bu tür veriler *özel nitelikli veriler* olarak adlandırılır.

2.3. Durumlarına Göre Veriler

Verileri ya da bilgileri sınıflandırmanın diğer bir yöntemi de verinin durumlarına göre yapılan sınıflandırmadır. Buna göre veriler, *"hareket halindeki veriler", "depolanan / saklanan veriler" ve "işlenen veriler"* olarak sınıflandırmak mümkündür. Hangi durumda olursa olsunlar tüm verilerin güvenliğinin uygun şekilde korunması ve güvenliğinin sağlanması gerekir.

Hareket halindeki veriler, ağ veya internet ortamında protokoller tarafından (örneğin IP) taşınan verileri ifade eder. Bir kullanıcının bir web sayfasında girerken kullanmış olduğu kullanıcı adı, parola, ad, soyad veya e-posta gibi kişisel veriler ağ ortamında bir cihazdan diğerine taşınır. Hassas bilgileri içerebilen hareket hâlindeki veriler İnternet gibi güvensiz bir ortamdan hareket ettiği için ciddi güvenlik riskleri barındırabilir. Bu nedenle güvenliğinin sağlanması oldukça önemlidir. Sanal Özel Ağlar kullanılarak hareket halindeki verilerin güvenliği sağlanabilir.

Depolanan veriler, saklanmak amacıyla bilgisayar disklerinde veya çeşitli harici ortamlarda korunan verileri ifade eder. Bir veri tabanında yer alan kayıtlar, bilgisayar disklerinde resim veya video gibi dosya olarak saklanan veriler, metin tabanlı olarak saklanan veriler bunlara örnek olarak gösterilebilir. Bu tür verilere önem düzeyine göre çeşitli güvenlik yöntemleri uygulanabilir. Örneğin kritik öneme sahip veriler için yetkisiz erişimlerden korumak amacıyla şifreleme yöntemleri uygulamak faydalı olacaktır. Bu veriler erişilebilirlik düzeyine göre bilgiler barındırabileceklerinden kimlik doğrulama ile veri erişimi sağlamak iyi bir uygulamadır. Depolanan veriler için diğer bir iyi uygulama, belirli periyotlar dahilinde yedekleme almaktır. Örneğin sık güncellenen bir veri tabanı için yedekleme işleminin en azından günlük olarak yapılması önerilir.

İşlenen veriler, bilgi işlem cihazlarının belleğinde işlenmek amacıyla geçici olarak tutulan verilerdir. Genelde işletim sistemleri ya da uygulama yazılımları tarafından bu verilerin işlenmesi gerekir. Bu verilere yönelik yapılacak saldırılar diğer iki türe göre daha zor olsa da benzer şekilde korunması gereken verilerdir. Çeşitli antivirüs veya antimalware yazılımları kullanılarak güvenlik önlemleri almak mümkündür.

3. BİLGİ TOPLAMA

Siber güvenlik dünyasında gerek saldırı için olsun gerek savunma için olsun bilgi toplama ihtiyacı vardır. Bilgi toplama yöntemleri, *Pasif Bilgi Toplama* ve *Aktif Bilgi Toplama* olarak iki başlık altında ele alınabilir (Keusch v.d., 2020). Bu iki strateji, çeşitli durum ve ihtiyaçlara göre kullanılabilir. Aktif bilgi toplama genellikle spesifik ve hızlı yanıtlar gerektiren durumlar için daha uygundur. Örneğin, bir pazar araştırması yapmak, müşteri geri bildirimleri almak gibi durumlar bu kapsamda değerlendirilebilir. Pasif bilgi toplama ise genellikle sürekli izleme ve genel trendleri anlama amacıyla daha uygundur. Bu başlıkta bilgi güvenliği açısından aktif ve pasif bilgi toplama yöntemleri açıklanacaktır.

3.1. Pasif Bilgi Toplama

Siber güvenlikte pasif bilgi toplama, bir sistem veya ağ üzerinde gerçekleşen olayları, trafikleri veya diğer dijital izleri gözlemleme ve kaydetme sürecini ifade eder. Pasif bilgi toplama, genellikle güvenlik analizi ve tehdit istihbaratı elde etme amacı taşır. Ayrıca, bir sistemin normal davranışını anlama, olası güvenlik tehditlerini belirleme ve saldırı tespiti gibi güvenlik konularında kullanılır.

• **Gözlem ve İzleme:** Ağ trafiğini izlemek, sistemi gözlemlemek ve normal aktiviteleri belirlemek amacıyla yapılır. Örneğin günlük kayıtları (log), sistem olayları ve ağ trafiği analizleri üzerinden bilgi toplamak bunlara örnek olarak verilebilir.

• **Günlük Analizi:** Sistem günlükleri, güvenlik olay kayıtları ve diğer kaynaklardan gelen güvenlik bilgilerini değerlendirmek amacıyla yapılır. Buradaki önemli husus, sistemdeki olayları, hataları ve potansiyel tehditleri belirlemektir.

• **Zayıf Nokta Analizi:** Sistemdeki zayıf noktaları belirlemek ve bu noktalarda potansiyel güvenlik risklerini anlamak amacıyla gerçekleştirilir. Ağ altyapısında ve uygulamalarda mevcut güvenlik açıklarını değerlendirmek örnek olarak verilebilir.

• **Dijital Ayak İzi Analizi:** Hedef sistem veya organizasyon hakkında çevrimiçi olarak toplanan verileri analiz etmektir. Hedefin dijital varlıklarını, kullanılan teknolojileri, çalışanlarını ve potansiyel güvenlik risklerini belirlemek için kullanılır.

• **Sistem Araştırması:** Sistem bileşenlerini, bağlantıları ve konfigürasyonları anlamak için aktif olmayan bir yaklaşım kullanmaktır. Ağ topolojisini çıkarmak, güvenlik politikaları ve sistem konfigürasyonları üzerinden bilgi toplamak örnek olarak verilebilir.

• **Veri Madenciliği:** Büyük veri setlerini analiz ederek gizli veya anlamlı bilgileri keşfetme sürecidir. Kullanıcı davranışlarını belirleme, ağ etkileşimleri ve güvenlik olayları üzerinden örüntüleri ve anlamlı ilişkileri belirleme örnek olarak gösterilebilir.

Pasif bilgi toplama, bir sistemi savunma amacı güderken saldırganların faaliyetlerini anlamak ve tespit etmek için de kullanılır. Bu, siber güvenlik uzmanlarına ve analistlere, olası tehditlere karşı proaktif bir savunma sağlamak adına önemli bir araç ve süreç sunar.

3.2. Aktif Bilgi Toplama

Siber güvenlikte aktif bilgi toplama, bir sistem veya ağ üzerindeki güvenlik zayıflıklarını ve tehditleri değerlendirmek amacıyla bilinçli bir şekilde hedef sisteme etkileşimli bir şekilde müdahalede bulunma sürecini ifade eder. Aktif bilgi toplama, siber güvenlik uzmanları veya etik hackerlar tarafından kullanılan bir yöntemdir. Bu süreç, sistemin güvenlik seviyesini değerlendirmek, zayıf noktaları tespit etmek ve bu zayıflıkların nasıl kapatılacağını anlamak için kullanılır. Bu yöntem kötü niyetli saldırganlar (siyah şapkalı hacker) tarafından da sıklıkla saldırı öncesinde kullanılır. Bu nedenle güvenlik uzmanları tarafından da bilinmesi gerekir.

• **Ağ Taraması:** Hedef sistem veya ağdaki aktif cihazları tespit etmek için port tarama ve ağ tarama araçları kullanmaktır. Ağ üzerindeki açık portları, servisleri ve hedef sistemlerin durumlarını belirlemek bu amacın örneklerindendir.

• **Zaafiyet Taraması:** Hedef sistem veya uygulamalardaki bilinen güvenlik zayıflıklarını tespit etmek için otomatik zaafiyet tarama araçları kullanmaktır. Bu taramalar, sistemdeki güncellemelerin ve yamaların durumunu kontrol eder.

• **Sızma Testleri:** Hedef sistem veya ağa etik saldırılar gerçekleştirerek, sistemin güvenlik seviyesini test etmek işlemleridir. Güvenlik zafiyetleri ve açıkları sömürerek sistemdeki potansiyel tehditleri belirlemek sızma testlerinin amaçlarındandır.

• **Sosyal Mühendislik Saldırıları:** İnsan faktörünü kullanarak, hedef organizasyon içindeki çalışanlardan bilgi elde etmeye çalışmaktır. Kullanıcıları yanıltmak, bilgi çalmak veya yetkisiz erişim sağlamak amacıyla manipülasyonlar yapmak örnekler olarak gösterilebilir.

• **Fuzzing:** Uygulamalara belirli veya rasgele veri girişleri ile test yaparak potansiyel hataları tespit etmektir. Bu yöntemle uygulamaların beklenmedik tepkilerini inceleyerek güvenlik açıkları ortaya çıkarılabilir.

Aktif bilgi toplama yöntemleri, genellikle etik hackerlar, güvenlik uzmanları veya siber güvenlik ekipleri tarafından yasal ve kontrollü bir ortamda gerçekleştirilir. Bu tür testlerin organizasyon içinde veya bir etik hackleme etkinliği çerçevesinde yürütülmesi, güvenlik açıklarının kapatılmasına yardımcı olabilir ve sistemin savunma mekanizmalarını güçlendirebilir.

4. BİLGİ GÜVENLİĞİ STRATEJİLERİ

Bilgi güvenliğini sağlamak için çeşitli stratejiler bulunmaktadır. Bu stratejiler, bir kuruluşun bilgi varlıklarını korumak, yetkilendirilmemiş erişimleri engellemek ve olası güvenlik tehditleriyle başa çıkmak için tasarlanmıştır. Aşağıda bilgi güvenliğini sağlamak için kullanılabilecek temel bazı stratejiler yer almaktadır.

- **Risk Analizi ve Yönetimi:** Bilgi güvenliği risklerini belirlemek ve bu risklere karşı uygun önlemleri almak için düzenli olarak risk analizi yapmak gerekir. Müşteriler, çalışanlar, gibi ilgili tarafların risk toleranslarını anlamak ve buna göre stratejiler belirlemek bu kapsamda ele alınacak eylemlerdendir.

- **Politika ve Prosedürler:** Bilgi güvenliği politika ve prosedürlerini oluşturmak ve bu politika ve prosedürleri düzenli olarak güncellemek var olan ve olası tehditlere karşı koruma sağlar. Bu kapsamda yapılacak diğer bir eylem de personeli bilgi güvenliği konusunda eğitmek ve bu politika ve prosedürlere uyumu teşvik etmek.

- **Eğitim ve Farkındalık:** Personeli güvenlik politikaları konusunda eğitmek ve bilinçlendirmek, sosyal mühendislik saldırılarına karşı eğitim ve farkındalık programları düzenlemek kurumda bilgi güvenliğini sağlamada uygulanacak önemli stratejilerdendir.

- **Güvenlik Duvarları ve Ağ Güvenliği:** Güvenlik duvarları (firewall) ve ağ güvenliği önlemleri kullanarak yetkilendirilmemiş erişimleri engellemek bu kapsamda yapılacak olan stratejilerdendir. Ağ trafiğini izlemek ve anormal aktiviteleri tespit etmek amacıyla güvenlik önlemleri almak, özellikle hareket halindeki veriler için güvenlik sağlayacaktır.

- **Veri Şifreleme:** Hassas önem düzeyine sahip verileri şifreleyerek, yetkisiz erişimlere karşı korumak gerekir. Ayrıca veri iletimi sırasında şifreleme kullanarak güvenli iletişimi sağlamak da bu kapsamda ele alınmalıdır. Bu sayede hem hareket halindeki hem de depolanan verilerin güvenliği sağlanabilir.

- **Güvenlik Yazılımları ve Güncellemeler:** Antivirüs programları, güvenlik yamaları ve antimalware gibi diğer güvenlik yazılımlarını düzenli olarak güncellemek gerekir. Yazılımları ve sistemleri düzenli olarak güvenlik açıkları yönünden taramak güvenlik zaafiyetlerini azaltmak anlamına gelir.

- **Fiziksel Güvenlik**: Fiziksel olarak yetkisiz erişime açık olan cihazların güvenliğinde bahsedilemez. Bu nedenle özellikle büyük kurumsal ağlarda yer alan veri merkezleri, sunucu odaları ve diğer kritik altyapıları fiziksel güvenlik önlemleriyle korumak gerekir. Bunun için Erişim kontrol sistemleri, güvenlik kameraları ve biyometrik tanıma sistemleri gibi fiziksel güvenlik teknolojilerini kullanılabilir.

- **Olay Yanıtı ve İnceleme**: "Olay Yanıtı" genellikle bir kurumun güvenlik olaylarına nasıl tepki verdiğini ifade eder. Güvenlik olayları, bilgisayar ağlarında, sistemlerde veya diğer bilgi teknolojisi altyapılarında meydana gelen istenmeyen olayları içerir. Bu olaylar, kötü amaçlı yazılım saldırıları, veri sızıntıları, yetkilendirilmemiş erişim girişimleri gibi çeşitli tehditlerden kaynaklanabilir. Bu tür olası durumlar için olay yanıt planları oluşturmak ve uygulamak, saldırı öncesi saldırı sırası ve saldırı sonrasında yapılacakları açıkça tanımlar. Güvenlik olaylarını izlemek, analiz etmek ve bu olaylara hızlı bir şekilde müdahale etmeyi sağlar.

- **İzleme ve Denetim:** Güvenlik olaylarını izlemek ve güvenlik denetim loglarını düzenli olarak kontrol etmeyi gerektirir. Denetim süreçleri oluşturarak güvenlik politikalarının etkili bir şekilde uygulandığını doğrulamak bilgi güvenliğinin sürdürülebilirliği için önemlidir.

- **Yedekleme ve Felaket Kurtarma:** Düzenli yedekleme stratejileri oluşturmak ve bu yedekleri güvenli bir şekilde depolamayı ifade eder. Felaket kurtarma planları hazırlamak ve düzenli olarak test etmek gerekir.

Bu stratejilerin birleşimi, bir kuruluşun bütünlüğünü, gizliliğini ve sürekli erişilebilirliğini sağlamak adına etkili bir bilgi güvenliği programını oluşturabilir. Unutulmaması gereken önemli bir nokta, bilgi güvenliğinin sürekli bir çaba gerektiren bir süreç olduğudur; bu nedenle stratejilerin düzenli olarak gözden geçirilmesi ve güncellenmesi önemlidir.

BÖLÜM ÖZETİ

Bilgi ve veri kavramları birbirlerinin yerine kullanılan ancak gerçekte iki farklı kavramdır. Veri, genellikle anlamlı bir bağlam içermeyen temel bilgi parçacıkları ifade ederken bilgi, verinin bir kapsam çerçevesinde anlamlandırılmış halidir. Bilgi güvenliği açısından bilgiyi ve veriyi sınıflandırmak, geliştirilecek olan güvenlik uygulamalarına kolaylık sağlayacaktır. Çok çeşitli açılardan bilgiyi sınıflandırmak mümkündür. Örneği bilgiyi hassaslık seviyesine göre, işlevselliğine göre, biçimine göre, kullanıldığı sektöre göre, zaman içindeki değişimine göre, erişilebilirlik düzeyine göre ve önem düzeyine göre sınıflandırmak mümkündür. Bilginin dayandığı verileri de benzer şekilde sınıflandırmak mümkündür. Buna göre verileri; temel kimlik bilgileri, iletişim bilgileri, kimlik doğrulama bilgileri, finansal bilgiler, sağlık bilgileri, biyometrik bilgiler, internet kimliği ve aktivite bilgileri, aileye ilişkin bilgiler ve eğitim bilgileri içerecek şekilde sınıflandırmak mümkündür. Kişisel veriler veya kişisel bilgi güvenliğinde son derece önemli bir konudur. Kişisel bilgi, bir birey hakkında spesifik veya tanımlayıcı olan her türlü veriyi ifade eder. Bu bilgiler, doğrudan bir kişiyi tanımlayabilen veya tanımlamak için kullanılabilen verilerdir. Bireylerin özel hayatına, sağlığına, cinsel hayatına, ırkına, etnik kökenine, dini inançlarına veya siyasi görüşlerine dair bilgiler özel nitelikli kişisel verilerdir ve korunması son derece önemlidir. Siber uzayda bilgi önemlidir ve saldırganlar tarafından kötü amaçlı eylemlerde kullanılabilir. İnternet ortamında veya siber uzayda bilgi toplama için çeşitli araçlar ve yöntemler yer almaktadır. Bu yöntemler saldırganlar tarafından kötü amaçlı olarak kullanılsa da güvenlik uzmanları tarafından güvenlik açıklarının tespit edilip kapatılması gibi iyi amaçlar doğrultusunda kullanılabilir. Genelde bilgi toplamanın aktif ve pasif olmak üzere iki türü bulunmaktadır. Aktif bilgi toplamada bilgi alınmak istenen hedef ile etkileşim kurularak bilgi toplanır.

GÖZDEN GEÇİRELİM

1. Veri ile bilgi arasındaki temel fark nedir?

a) Veri, anlam taşıyan bir yapıdır, bilgi ise işlenmemiş bilgilerdir.

b) Bilgi, bir bağlam içinde anlam ifade eden veri koleksiyonudur, veri ise organize edilmemiş bilgilerdir.

c) Veri, genellikle anlamlı bir bağlam içerir, bilgi ise sayılar, metinler veya semboller gibi çeşitli biçimlerde bulunabilir.

d) Bilgi, işlenmemiş ve organize edilmemiş bilgilerdir, veri ise anlam taşıyan bir yapıdır.

2. Bilgiyi sınıflandırmanın aşağıdaki avantajlardan hangisine katkı sağlar?

a) Bilgi güvenliğini sağlamak

b) Bilginin anlamını kaybetmek

c) Erişim kontrolünü karmaşıklaştırmak

d) Risk yönetimini zorlaştırmak

3. Hangisi, bilgi türlerini sınıflandırmanın bir örneğidir?

a) Üretken Bilgi, Tüketilen Bilgi, Atılan Bilgi

b) Kamusal Bilgi, İçsel Bilgi, Gizli Bilgi

c) Yazılı Bilgi, Görsel Bilgi, Sözlü Bilgi

d) Statik Bilgi, Dinamik Bilgi, İlgili Bilgi

4. Bilgi güvenliği stratejilerinin amacı hangisinde doğru tanımlanmıştır?

a) Bilgi güvenliği, veri ve bilgilerin yetkisiz erişim, kullanım, ifşa, bozulma, engellenme ve yok olmalara karşı korunmasını amaçlar.

b) Bilgi güvenliği sadece veri gizliliğine odaklanır, bütünlük ve erişilebilirlik önemli değildir.

c) Bilgi güvenliği, bilgiyi herkese açık hale getirmeyi amaçlar.

d) Bilgi güvenliği, yalnızca veri analizi ile ilgilenir, yorumlama ve anlam taşıma önemli değildir.

5. Kişisel bilgiler, bir birey hakkında spesifik veya tanımlayıcı olan her türlü veriyi içerir. Bu bilgiler neden önemlidir?

a) Sadece özel sektörün ilgisini çeker.

b) Gizlilik ve güvenlik açısından hassas oldukları için.

c) İnternet üzerinde paylaşılabilir oldukları için.

d) Sadece iş yerinde kullanılır, kişisel hayatta etkisi yoktur.

6. Hangisi kişisel bilgi örneğidir?

a) Halka açık bir şirketin hisse senedi fiyatı.

b) Bir kitabın yayınlanma tarihi.

c) Bir bireyin adı ve soyadı.

d) Bir ülkenin başkenti.

7. **Kişisel bilgilerin yetkisiz kişilerin eline geçmesi, ne tür güvenlik tehditlerine neden olabilir?**

   a) İnternet hızının artmasına.

   b) Kimlik hırsızlığı, dolandırıcılık gibi risklere.

   c) Güvenli online alışveriş deneyimine.

   d) Sadece reklam şirketlerinin kar etmesine.

8. **Kişisel bilgi koruma yasaları neleri düzenler?**

   a) Sadece ülke sınırları içindeki bilgi paylaşımını.

   b) Bireylerin kişisel bilgilerinin nasıl toplanacağını, nasıl saklanacağını ve nasıl kullanılacağını.

   c) Sadece büyük şirketlerin güvenlik politikalarını.

   d) Yalnızca online alışveriş sitelerinin işlemlerini.

9. **Veri durumlarına göre sınıflandırmaya göre, depolanan veriler için uygulanan bir güvenlik yöntemi hangisidir?**

   a) Sanal Özel Ağlar kullanımı.

   b) IP adreslerinin izlenmesi.

   c) Hareket halindeki verilerin periyodik yedeklenmesi.

   d) İşletim sistemlerinde geçici olarak tutulan verilerin şifrelenmesi

Yanıt Anahtarı: 1-C, 2-A, 3-B, 4-A, 5-B, 6-C, 7-B, 8-B, 9-D

Kaynakça

Bulut, A., Aydın, M. A., & Zaim, A. H. (2023). Sıfır Güven Ağ Erişim Mimarisinde Kullanıcı Güvenliğinin Sağlanması. *İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi*, *22*(43), 215–232. https://doi.org/10.55071/ticaretfbd.1102276

Canbek, G., & Sağıroğlu, Ş. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. *Politeknik Dergisi*, *9*(3), 165–174.

Durna, Y. Doç. D. U., & Demirel, Y. D. D. Y. (2008). Bilgi Yönetiminde Bilgiyi Anlamak. *Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *30*, 129–156.

İren, E., & Can, Ö. (2017). Bilgi Sistemlerinde Güncel Güvenlik Problemleri Ve Önerilen Çözümler. *TÜBAV Bilim Dergisi*, *10*(2), 27–42.

Keusch, F., Struminskaya, B., Kreuter, F., & Weichbold, M. (2020). *Combining Active and Passive Mobile Data Collection* (pp. 657–682). https://doi.org/10.1002/9781118976357.ch22

Topaloğlu, N., Calp, M. H., & Türk, B. (2016). Bilgi Güvenliği Kapsamında Yeni Bir Veri Şifreleme Algoritması Tasarımı ve Gerçekleştirilmesi. *Bilişim Teknolojileri Dergisi*, *9*(3), 291. https://doi.org/10.17671/btd.36875

BÖLÜM 6

GÜVENLİK STRATEJİLERİ VE KORUNMA

ANAHTAR KAVRAMLAR

Bilgi Toplama, Temel Güvenlik, Güvenlik Yazılımları

ÖĞRENME HEDEFLERİ

1. Bilgi toplama araçlarını açıklar.
2. Temel güvenlik önlemlerini açıklar.
3. Zaafiyet derecelendirme sistemini tanımlar.
4. Güvenlik yazılımlarını tanımlar.
5. Güvenlik yönetim merkezinin işlevini açıklar.

ALTINCI BÖLÜM

GİRİŞ

Siber saldırılara, tehditlere ve zararlı yazılımlara karşı savunma yapabilmek ya da koruma stratejileri geliştirebilmek için, tehdit aktörlerinin yöntemlerini, tekniklerini, ağın işleyişini ve yapısını bilmeyi gerektirir. Saldırının ilk aşaması keşif aşamasıdır. Saldırgan bu aşamada hedefe ilişkin bilgi toplamaktadır. Siber güvenlik uzmanının da bu bilgi toplama yöntemlerini bilmesi, güvenlik stratejileri oluşturmada ve korunma aşamaları tasarlamalarında yararlı olacaktır. Bu bölümde, bilgi toplama yöntemleri, bilgi toplama araçları, temel güvenlik önlemleri ve stratejileri ele alınmıştır.

1. SİBER GÜVENLİKTE BİLGİ TOPLAMA ARAÇLARI

Siber güvenlik dünyasında gerek saldırı için olsun gerek savunma için olsun bilgi toplama ihtiyacı vardır. Bilgi toplama yöntemleri, Pasif Bilgi Toplama ve Aktif Bilgi Toplama olarak iki başlık altında ele alınabilir.

1.1. Pasif Bilgi Toplama Araçları

Pasif bilgi toplama sürecinde, bilgi alınmak istenen ağ ya da sistem ile doğrudan bir etkileşim bulunmaz. Elde edilen bilgi, doğrudan sistemden değil internet kaynaklarından elde edilir. Bu bilgi toplama yöntemlerinde şunlar yapılabilir.

- IP Adresleri Hakkında Bilgi Toplama Araçları
- Domainler Hakkında Bilgi Toplama Araçları
- Web Sayfalarında Bilgi Toplama Araçları

IP Adresleri Hakkında Bilgi Toplama

IP adreslerinin dünyadaki dağıtım merkezi ICANN (Internet Corporation for Assigned Names and Numbers)'dır. Bu kâr amacı gütmeyen kurum, İnternet adresi alanı tahsisi, protokol ataması ve ülke kodu (.tr, .de, .se gibi) internet alan adı yönetiminden sorumludur. Bir IP adresi sorgusunu en kısa yoldan Whois Sorgusu ile yapılmaktadır.

Whois Sorgusu

Whois sorgusu, sorgu yapılan alan adı ile bazı bilgilere ulaşmayı hedefler. Alan adı sahibi kişiye ait iletişim bilgileri ve alan adı ile ilgili teknik bilgiler yasal çerçevede (ICANN) listelenir. Whois sorgusunu herkes yapabilir yani herkes ulaşabilir. Ancak alan adı sahibi kendisine ait bilgilerin Whois sorgusu sırasında listelenmesini istemeyebilir. Bunun için Whois Gizleme servisinin aktif edilmesi gerekmektedir. Bu sayede, ICANN verileri gizleyip başka kişiler ile paylaşmayacaktır.

Şekil 1 Whois web sitesi ve arama işlemi

http://www.whois.com/ internet adresine bilgi edinmek istenilen alan adı yazıldığında (örnek: ankara.edu.tr) Şekil 2'deki ekran görünmektedir.

ankara.edu.tr

```
** Domain Name: ankara.edu.tr
Frozen Status: -
Transfer Status: The domain is LOCKED to transfer.

** Registrant:
   Ankara Üniversitesi
   Hidden upon user request
   Hidden upon user request
   Hidden upon user request
   Hidden upon user request

** Registrar:
NIC Handle              : tk1036
Organization Name       : TRABİS KK
Address                 : ANKARA
                          ANKARA
                          00000 Ankara Türkiye
Phone                   : 90-312-2100060
Fax                     : 90-312-2100060

** Domain Servers:
ns1.ankara.edu.tr 80.251.40.10
ns2.ankara.edu.tr 80.251.40.11

** Additional Info:
Created on..............: 1999-Apr-30.
Expires on..............: 2025-Apr-29.

** Whois Server:
Last Update Time: 2023-12-07T02:17:49+03:00
```

Şekil 2 Örnek Whois sorgusu

RIPE Üzerinden IP Sorgulama

Şekil 3 RIPE NCC sayfası

RIPE NCC, IANA kuruluşuna bağlı olan, Avrupa ve Ortadoğu bölgesi gibi bir bölgeye IP adresi dağıtımından sorumlu olan bir kuruluştur. Bu kuruluşa https://www.ripe.net/ internet adresinden erişilebilir. Belirtilen bölgede yer alan IP adreslerine ilişkin pasif bilgi sorgulaması yapılabilir. İlgili web sayfasında sorgulanmak istenen IP adresi yazılarak sorgulama yapılabilir. Şekil 4'te yer alan ekran görüntüsünde örnek bir sorgulama yapılmıştır.

Responsible organisation: Ankara University
Abuse contact info: abuse@ankara.edu.tr

inetnum:	5.23.120.0 - 5.23.123.255
netname:	TR-AU-NAT
descr:	Ankara University
country:	TR
admin-c:	AUID1-RIPE
tech-c:	AUID1-RIPE
status:	ASSIGNED PA
mnt-by:	ANKARA-NET-MNT
mnt-domains:	ANKARA-NET-MNT
created:	2012-05-15T14:03:02Z
last-modified:	2017-11-08T09:36:02Z
source:	RIPE

route:	5.23.120.0/21
descr:	ANKARA-NET
origin:	AS8678
mnt-by:	ANKARA-NET-MNT
created:	2012-05-15T12:43:50Z
last-modified:	2012-05-15T12:43:50Z
source:	RIPE

Şekil 4 Örnek Ripe NCC sorgulama

Site Durumunu öğrenme

https://ns.tools/ web sitesi, bir web sayfanın aktif mi yoksa pasif mi olduğunu öğrenmek için ping işlemi uygular. Bu yöntemle web sitesinin işlevsel ve aktif olup olmadığı öğrenebilir. Ayrıca bu web sitesi ile ilgili daha farklı bilgiler de toplanabilir.

Şekil 5 ns.tools sitesi

Alan Adları Hakkında Bilgi Toplama Araçları

Etki alan adları olarak da adlandırılan domain adları, genellikle web sitelerine IP numaraları yerine, hatırlaması daha kolay olan isim yazarak erişmek için kullanılan bir sistemdir. İnternet ortamında cihazların iletişiminde nümerik IP adresleri kullanılır. Ancak kullanıcılar erişmek istedikleri web sayfaları ya da herhangi bir kaynağın IP adresini akılda tutması güç olabilir. Bu nedenle belirli kurallar dâhilinde, benzersiz alan isimleri kullanılır.

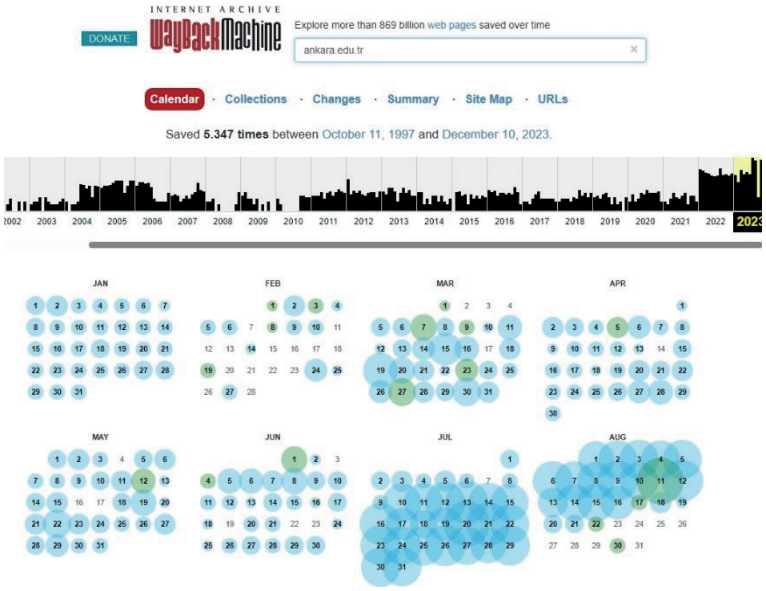
Alan adı isimlendirmesi, daha önce bahsedilen DNS sistemi ile ilişkilidir. Belirli bir web sitesine ilişkin bu benzersiz alan adları hakkında bilgi toplamak için isim sorgulaması yapılabilir. Alan adlarının kullanımda olup olmadığı ya da var olup olmadığına ilişkin bilgilere erişmek için domain sorgulama sistemleri kullanılabilir.

Web Sayfalarından Bilgi Toplama Araçları

- Archive.org
- Netcraft.com
- Pipl.com

Archive.org : İnternet ortamında yıllar boyunca devasa sayıda web sayfaları yayına girer ve bazen çeşitli nedenlerle kapanabilir. Archive.org sayfası, 1996 yılından itibaren web sitelerinin görüntülerini indeksleyen oldukça yararlı bir web sayfasıdır. Yayından kaldırılan ya da günümüzde var olmayanların yanı sıra, günümüzde var olan sitelerin de eski görüntülerine erişmek mümkündür.

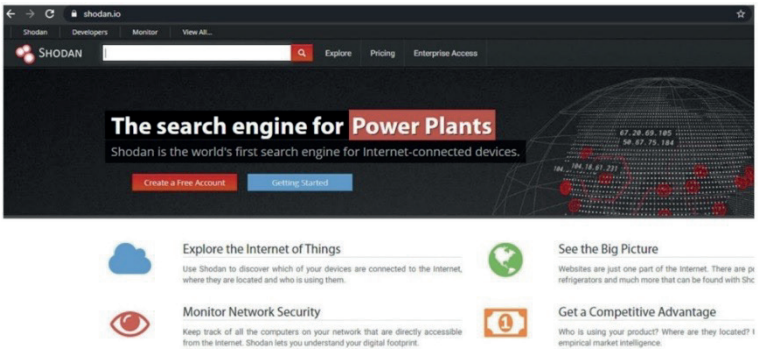
İlgili sayfada sorgulanmak istenen web sitenin adresi yazılır. Arama (“Search”) alanına sorgulanmak istenen site adresi yazılır ve “Go” tuşuna basılır.Şekil 6’da örnek bir ekran görüntüsü yer almaktadır.



Şekil 6 Örnek archive.org sorgusu

Açılan takvimden, (indekslenmişse) istenilen bir tarihe ait sayfanın görüntüsüne ulaşılabilir.

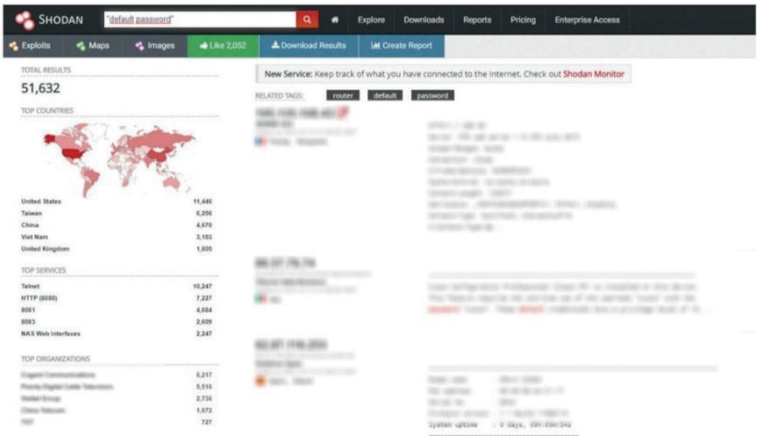
Shodan Kullanarak Bilgi Toplama: Shodan, çeşitli filtreler kullanarak internete bağlı bilgi işlem cihaz türlerini bulmayı sağlayan www.shodan.io sayfasından hizmet veren bir arama motorudur.



Şekil 7 shodan.io ana sayfası

Shodan, internete bağlı cihazları aramak için interneti sürekli olarak tarayan dünya çapına yayılmış sunuculara sahiptir. Web kameraları, varsayılan parola kullanan cihazlar, yönlendiriciler ve IoT cihazları gibi birçok cihazın bulunmasını sağlayabilir. Hangi cihazların bağlı olduğu, nereye bağlı oldukları ve hangi servislerin güvenlik açığı içerdiği ile ilgili olarak veri madenciliği yapmak amacıyla kullanılabilir.

Shodan ekranında görüntülenen tüm cihazlar, güvenlik açığı içeren sistemler değildir. Ancak bazı güvenlik açığı barındıran sistemlerin de tespit edilebilmesi mümkün olabilir. Örneğin, varsayılan parola kullanan sistemlerin tespit edilebilmesi için arama alanına "default password" yazınız.



Şekil 8 Örnek Shodan.io sorgusu

Şekil 8'deki Shodan ekran görüntüsünde varsayılan parolayı kullanan sistemlere ilişkin bilgiler gösterilmektedir. Shodan aramasında, filtreleme parametreleri de kullanılabilir. Shodan ile kullanılabilecek bazı filtreler şunlardır:

- city: Belirli bir şehirde arama yapar
- country: Belirli bir ülkede arama yapar
- os: işletim sistemine göre arama yapar
- port: Açık olan TCP/UDP portlarına göre arama yapar
- product: Belirli bir ürüne göre arama yapılır.

Örneğin, Amerika Birleşik Devletlerinde SNMP hizmeti açık olan Cisco 7200 yönlendiricileri görmek için arama kutusuna {country:US product:"Cisco 7200 Router" port:161} yazılabilir.

Siber güvenlik kapsamında yapılabilecek diğer bir Shodan araması da ileriki bölümlerde ele alınacak olan CVE güvenlik zafiyeti numarasına göre arama yapmaktır. Ancak bu tür bir arama sadece lisanslı ve akademik kullanıma açıktır.

DİKKAT EDELİM

Bu bölümde yapılan aramalar ve anlatılan konular eğitim amaçlıdır. Lütfen yasal olmayan durumlara karşı dikkatli olunuz.

1.2. Aktif Bilgi Toplama Araçları

Bu bilgi toplama yönteminde hedef sistem ile doğrudan iletişime geçirilir. Saldırgan açısından riskli bilgi toplama yöntemidir ve çok dikkatli olunması gerekmektedir. Yakalanma olasılığı her zaman mevcuttur. Bir siber güvenlik uzmanının da savunma amaçlı olarak bu aktif bilgi tekniklerini bilmesi gerekmektedir.

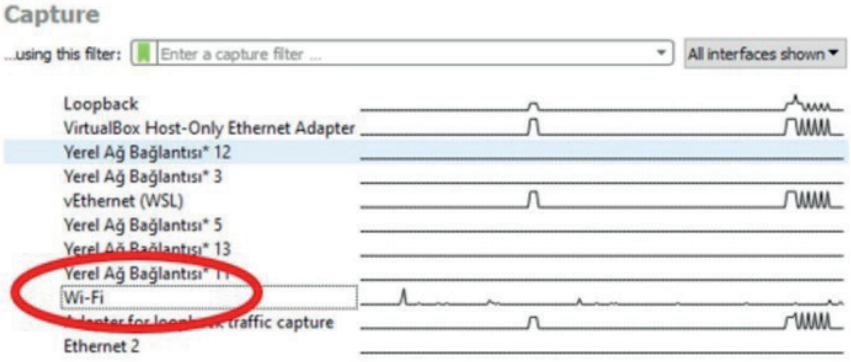
Network Maping

Network mapper, en yaygın bilinen şekliyle bilgisayarın açık olan bağlantı noktalarını, parmak izini, kullanılan servislerin isim ve versiyon numaralarını bulmaya yarayan bir araçtır. NMAP, daha önceki konularda ele alınan çeşitli ağ protokolleri aracılığıyla veri toplamayı sağlayan yararlı bir araçtır. Ağda yer alan konaklara ICMP gibi paketler gönderilerek sorgulamalar yapılır ve cihazlardan gelen cevaplar incelenir. Gelen cevaplardaki bilgilerdeki doğrudan bilgilere ya da ipuçlarına göre ağda keşif işlemleri yapılabilir, aktif olarak bilgi alınabilir.

Nmap, ağ haritalaması üzerine odaklanmış bir araçtır. Bu sayede incelenmek istenen bir ağda bulunan cihazların, kullanılan işletim sistemlerinin ve açık bulunan servis ve bağlantı noktası bilgileri tespit edilebilir. Bu bilgilerin elde edilebilmesi için sadece hedef bilgisayar sistemine ait web adresini veya IP adresini bilmek ve Nmap'i kullanmak yeterlidir. Örneğin bir IP'nin bulnduğu ağın haritasının çıkarılması için "nmap IP_adresi" yazmak yeterlidir. Bu komut ile o IP adresindeki bilgisayarın bilinen bağlantı noktalarına SYN taraması gerçekleştirir. Bağlantı noktaları, bir sistemde çalışan hizmetler ve uygulamalar ilişkili bir kavramdır. Hedefe ilişkin SYN taraması yapmak, TCP protokolünün SYN bayrağını kullanarak açık hizmetlerin bulunmasını sağlamaktadır.

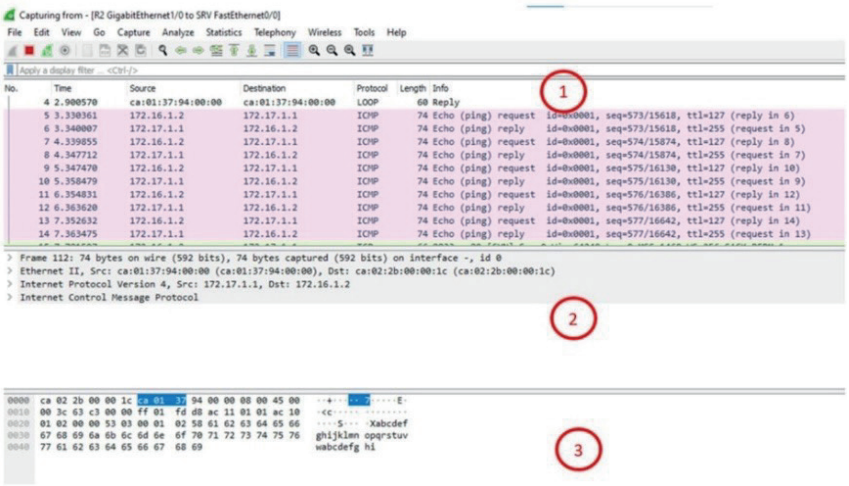
WireShark

WireShark, ağ ortamında paketlerin yakalanmasını ve analiz edimesini sağlayan ücretsiz ve en popüler protokol analiz ve paket yakalama aracıdır. Bu yararlı yazılım https://www.wireshark.org/ sayfasından indirilebilir.



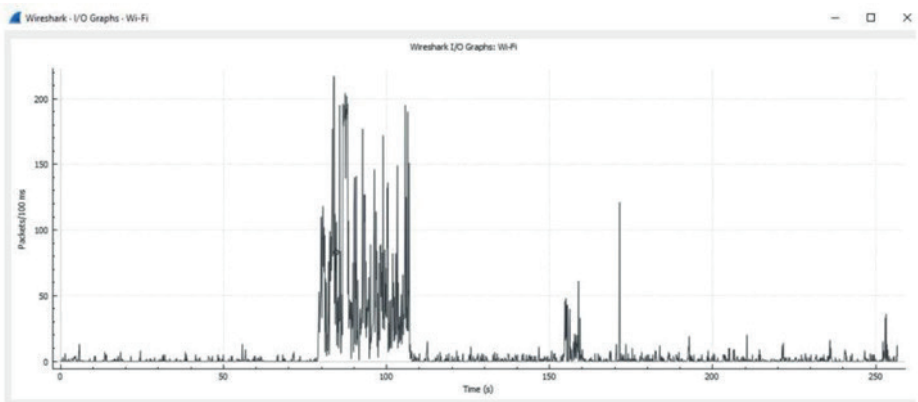
Şekil 9 Wireshark dinlenecek arayüz seçme

Yazılım çalıştırılırken ilk olarak paketin yakalanacağı arayüz (NIC) seçilir. Arayüz seçiminin ardından, Şekil 10'daki gibi bir ekran görüntüsü gelir.



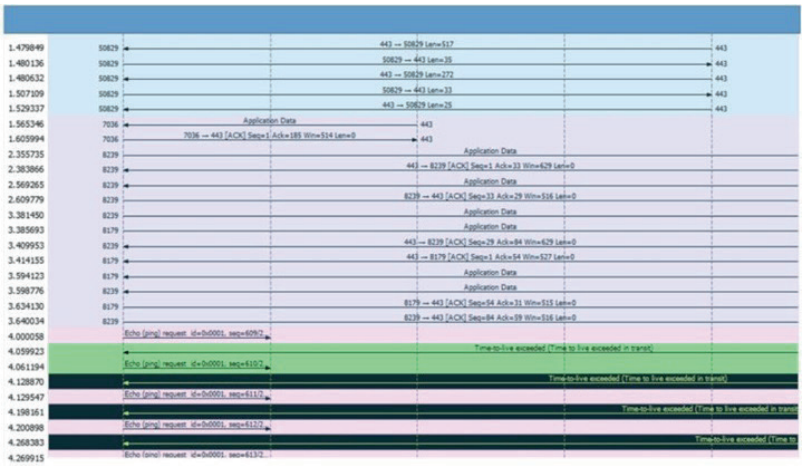
Şekil 10 Wireshark paket toplama ekranı

WireShark ekranı üç ana bölümden oluşur. İlk bölümde zamana göre yakalanan paketler yer almaktadır. İkinci bölümde yakalanan bu paketin katmanlı yapıdaki içerikleri, üçüncü bölümde ise paketin içerdiği veriler kodlanmış olarak görüntülenmektedir.



Şekil 11 Wireshark istatistiksel analiz ekranı

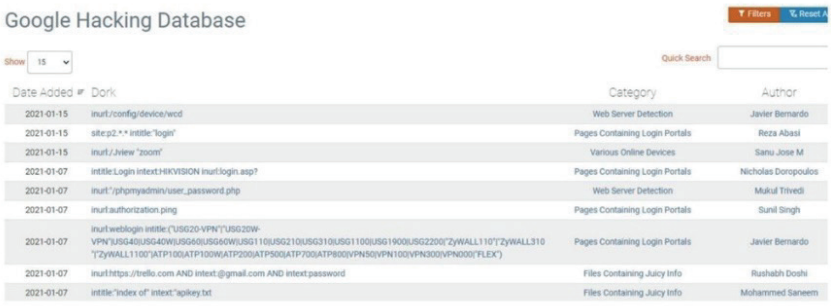
Yakalanan paketlerin tek tek incelenmesinin yanı sıra, ağ ortamı hakkında genel ağ kullanımı, en fazla iletişim kuran IP'ler, TCP veri akışı gibi istatistiksel ve görsel bilgiler de sunmaktadır.



Şekil 12 Wireshark iletişiminin görselleştirilmesi

Google Hack Veritabanı

Google internette en yaygın kullanılan arama motorudur. Siber güvenlik dünyasında bilgi toplamada, Google arama motorunun sağladığı anahtar kelimeler ile detaylı bilgi toplama yapılabilir. Arama motorunun indeksleme becerisi, zararlı olabilecek birçok kritik bilginin de indekslenmesine neden olmuştur. Google Hack Veritabanı, https://www.exploit-db.com/google-hacking-database bağlantısından erişilebilen Google sorgularının listesini içeren bir indeksleme veritabanıdır.



Şekil 13 Google Hack Veritabanı

Örneğin, bir web sunucusunun parmak izi, Google üzerinden Apache çevrimiçi dokümantasyonu veya IIS tarafından web kök dizinine eklenen özel bir klasör için sorgulama yapılaması mümkündür.

{intitle:"Apache HTTP Server" intitle:"documentation" site: hedefsite.abc}

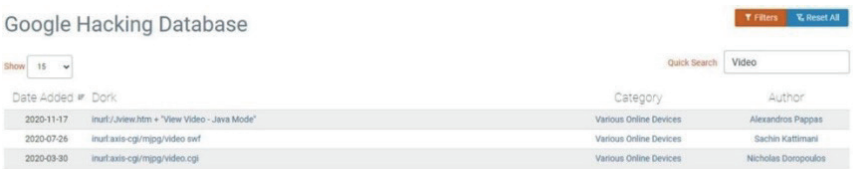
Bunun için belirli bir siteye yönelik (hedefsite.abc) yukarıdaki sorgulama cümlesi yazılarak, google'nin indekslediği verilerden özelleştirme yapılabilir.

Diğer bir örnek de dosya türüne göre belirli bir sitede arama yapmaktır. Buna göre hedefsite için bak dosyalarının tespitine yönelik olarak aşağıdaki gibi bir sorgulama yapılabilir.

{filetype:"bak" site:hedefsite.abc}

Görüleceği üzere, Google hack veritabanı kullanılarak, kullanıcı adı & parolalar, kritik bilgiler içeren hata mesajları ve güvenlik zafiyetleri bulunabilir. İlgili veritabanında yer alan güncel sorgular kullanılarak bilgiler toplanabilir.

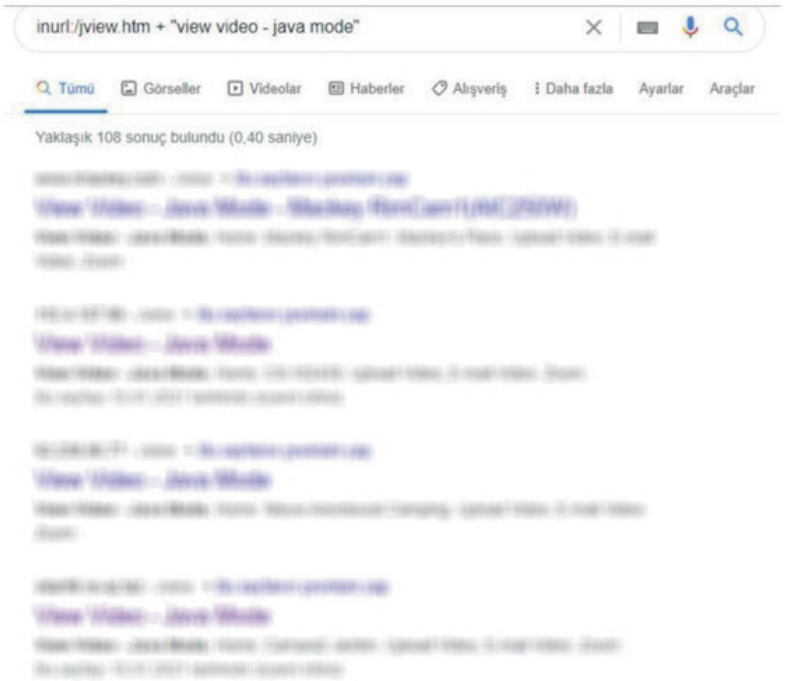
Örnek olarak, ilgili veritabanında yer alan arama kısmına "video" yazılarak, bununla ilgili sorgulara ulaşılabilir.



Şekil 14 Google Hack sorgulama sonucu

Gelen ilk ekrandaki ilk sorgu cümlesi Google arama motorunda yazılabilir. Bu durumda Şekil 15'teki gibi bir liste görüntülenecektir.

Bu sorguya cevap veren herhangi bir link açıldığında kamera video akışını gösteren cihaza erişim sağlanabilecektir.



Şekil 15 Örnek Google sorgusu

2. TEMEL GÜVENLİK ÖNLEMLERİ

Bir bilgisayarı güvenli hale getirmek, kişi veya kuruma göre farklı nedenlerden dolayı farklı türdeki eylemleri uygulamaya koymak amacıyla yapılması gereken işlemler ve kurallar bütünüdür. Bilgisayar güvenliği kuralları, bilgisayarı kullandığınız sürece devam eder. Bir bilgisayar sisteminin güvenliği ne kadar iyi tasarlanırsa tasarlansın, güvenlik ile ilgili işlemler kontrol edilmez ve zaman göre güncellenmezse, sisteminiz herhangi potansiyel bir bilgisayar korsanına karşı savunmasız bırakabilir.

Araştırmalara göre yeni bir bilgisayar kurulumu tamamlandıktan sonra ilk siber saldırı ortalama yedi dakika sonra gerçekleşmektedir. Bunun nedeni, bilgisayar saldırganlarının genellikle fırsat arayan ve sürekli araştıran otomatik tarama araçları kullanmasıdır. Bir istismar, genellikle bir kurulumu tamamladıktan sonra, güvenlik önlemleri alınmadan dakikalar içinde gerçekleşebilir. Bu araştırma bizlere, bilgisayar kurulumu yapıldıktan sonra internet bağlantısı kurulmadan tüm savunma ve koruma işlemlerini yerine getirmemiz gerektiği sonucunu ortaya çıkartmaktadır.

Bilgisayar kullanıcılarının sayısı arttıkça bilgisayar güvenliği konusuna yeterli önemi göstermeyen veya deneyimsiz bir kullanıcının kullandığı bilgisayar, belirlenmiş bir hedefe yönelik dağıtılmış bir hizmet reddi (DDoS) saldırısına dâhil edilebilir. Bu gibi sorunlara karşı üç konuda temel bilgisayar güvenliğini ele alabiliriz.

2.1. Fiziksel Güvenlik

Bilgisayar sisteminin fiziksel güvenliğidir. Bilgisayarın fiziksel olarak zarar görmemesi veya kötü niyetli kişilerce ele geçirilmemesi için gerekli önlemlerin alınmasıdır. Bununla beraber aşırı elektrik akımından korumak için kesintisiz güç kaynağı kullanmak bilgisayarın ve bilgisayar içinde saklanan verilerin güvenliği için oldukça önemlidir. Günümüzde kişisel bilgisayarlarda elektrik hatlarındaki problemler dolayısı ile veri kaybı oldukça sık görülmektedir. Modem, sabit sürücü veya ana kart arızaları nedenleri ile bilgisayarların bir süre kullanılamaması gibi problemlere karşı fiziksel güvenlik tedbirleri alınmalıdır.

Şekil 16 Fiziksel güvenlik

2.2. Veri Bütünlüğü

Verilerin yedeklenmesi ve bu şekilde veri kaybının önlenmesidir. Kurumlar veya kişisel kullanıcılar kendileri için değerli gördükleri verileri korumalıdır. Her yıl, bir şekilde kaybedilen değerli bilgileri yeniden üretmek için büyük bir miktarda iş gücü kaybı oluşmaktadır. Yedeklemeler flaş diskler, sürücüler, kâğıt çıktılar veya diğer bilgisayar sistemlerinde olabilir. Orijinal verinin kaybolmasını önlemek ve verileri yangın, su baskını gibi nedenlerle yedeklemek için bu yedeklemelerin kopyalarını düzenli olarak orijinal verinin tutulduğu yerden daha uzak fiziksel konumlara koymak önemlidir. Ayrıca önemli veriler için RAID sistemleri kullanılabilir çözümlerdir. RAID sistemleri bir verinin kopyasını aynı zamanda başka sürücülere de yazması anlamına gelir. Bir sürücünün arızalanması durumunda, içeriği diğer sürücülerdeki verilerden elde edilebilir.

2.3. Veri Güvenliği

Veri güvenliğine yönelik en önemli tehdit, yasa dışı bilgisayar korsanlarıdır. İçten veya dıştan gelebilecek her türlü güvenlik ihlaline karşı alınması gereken bazı önemli tedbirler bulunmaktadır. Bilgisayarlara parola koymak, önemli doya ve dizinlere erişim izinleri koymak, güvenlik duvarı gibi çözümleri kullanmak, kullanılan yazılımların güvenliğini yamalar ve güncelleştirmeler ile sağlamak, veri tabanlarını güvende tutmak, e-posta gibi güvensiz uygulamalar için gerekli önlemleri almak veri güvenliği için oldukça önemlidir.

Bilgisayarları daha güvenli hale getirmek için yapılması gereken temel işlemlerin listesi aşağıdaki gibidir.

• Bilgisayarın fiziksel güvenliği sağlanmalı

• Yedekleme alınmalı ve sisteminizin olduğundan uzak bir yerde saklanmalı

• Elektrik sorunların karşın kesintisiz güç kaynağı kullanılmalı

• Periyodik olarak virüs kontrolü yapılmalı

• Güvenlik duvarı gibi çözümler kullanılmalı

• İyi ve güvenli parola kullanılmalı

• Düzenli aralıklarla parolaların güncellenmesi

• Kullanılmayan hesapların kaldırılması

• Dosya ve dizin erişimlerinin yapılması

• Önemli dosyaların şifrelenmesi

• Şifrelenmiş e-posta yazılımları kullanılmalı

• İşletim sistemi ve yazılımlara ait yamaların ve güncelleştirmelerin yapılması

• Bilinmeyen yazılımların yüklenmemesi ve izinlerin verilmemesi

• Bilgisayarın kullanılmadığı zamanlarda kapatılması

• Bilgisayarı mümkün olduğunca yönetici (administrator) hesabı ile kullanılmaması

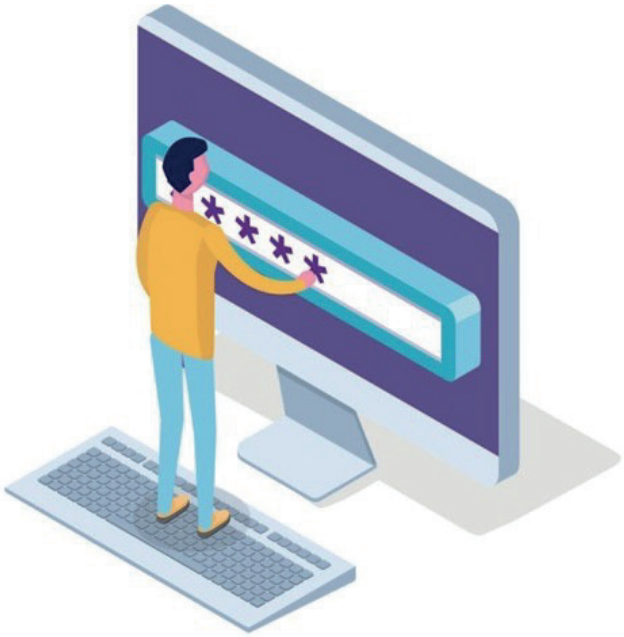
• E-posta adresinizi her web sitesine vermemelidir.

2.4. Parola Güvenliği

Parolalar günümüzde hayatımızda oldukça önemli yer tutmaktadır. Parolalar kimlik doğrulaması için kullanılan en etkili yöntemlerden birisidir. Bilişim teknolojilerinin gelişmesi ile hayatımıza gelen yeniliklerinin tamamına yakınında parolalar kullanılmaktadır. Banka kartlarımızda, internet hesaplarımızda, telefonlarımızda, ev güvenlik sistemlerinde vb. parolaları kullanmaktayız.

DİKKAT EDELİM

Parola ve şifre farklı kavramlar olsa da çoğu zaman birbirinin yerine kullanılır.



Şekil 17 Parola güvenliği

Parolaların kimlik doğrulamasında kullanılması beraberinde önemli bir sorunu meydana getirdiler. Bunların içinde en önemli olarak görünler sorunlar ise; kullanıcıların zayıf veya tahmin edilmesi kolay parolaları seçmeye ve aynı parolaları farklı yerlerde yeniden kullanmaya devam etmeleridir. Dünya üzerinde son on yılda yapılan araştırmalar kullanıcıların en sık tercih ettiği parolaları şu şekilde listelemektedir:

- 123456
- password
- qwerty
- 111111
- 123123
- 987654321
- 123456789
- asdfgh

Her yıl yapılan uyarılara rağmen bu liste pek değişmemiştir. Bunun için kullanıcılara bir takım parola belirleme kuralları tavsiye edilmektedir. Bu kurallar aşağıdaki listede belirtilmiştir.

- Minimum karakterin karşılanması gibi karmaşıklık gereksinimlerin belirlenmesi,
- Daha önceden kullanılan şifrelerin seçilmemesi,
- Parolaların periyodik olarak ve belki de sık sık değiştirilmesi,
- Kullanılan parolaların yukarıdaki listedeki gibi yaygın ve zayıf olarak kullanılan parolalardan seçilmemesi.

Parolaların belirlenmesi ve belirli standartların yakalanması için Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) parola ilkeleri sorununa çözüm getirmeyi amaçlamıştır. NIST parolalar ve bunların nasıl yönetilip saklanması gerektiği hakkında detayları ortaya koymaktadır. Buna göre, olası parolaların yaygın olarak kullanıldığı ve bilinen değerleri içeren bir listeye karşı kontrol edilmesi gerektiği belirtmiştir. Parolaların belirlenmesinde dikkat edilmesi gereken hususlar şunlardır:

- Kullanıcı tarafından sağlanan parolalar en az sekiz alfa numerik karakterden oluşmalıdır.
- Önceki ihlallerden elde edilen parolalar olmamalıdır.
- Sözlük kelimeleri olmamalıdır.
- Doğrum tarihleri gibi 1900-2020 arasındaki tarihler olmamalıdır.
- Tekrarlayan veya sıralı karakterler (örneğin aaaaaa veya 1234abcd) olmamalıdır.
- Hizmetin adı, kullanıcı adı ve bunların türevleri gibi kullanım amacına özgü kelimeler olmamalıdır.

Parolalar belirlenirken yukarıdaki kriterler dikkate alınmalı ve karmaşık yapıdaki parolaların oluşturulması sağlanmalıdır.

Parola Karmaşıklığı

Parola karmaşıklığı, parola belirleme ilklerine bağlı olarak, güçlü bir parola için biz dizi kuralı karşılaması anlamına gelmektedir. Parola karmaşıklığındaki temel kurallar şunlardır.

- Parola, hesap adını veya hesap adındaki varyasyonları içeremez.
- Parola hem büyük harf (A-Z) hem de küçük harf (a-z) içermelidir.
- Parola içinde özel karakterler (~! @ # $% ^ & * _- + = `| \ () {} [] :;” ‘<>,.?/) olmalıdır. (Genellikle ALT tuşu ile çıkan karakterlerdir. Ancak Euro gibi para birimi simgeleri, özel karakter olarak sayılmaz.).
- En az karakter sayısına uyulmalıdır. Bu değer sistemden sisteme, kullanıcıdan kullanıcıya değişebilir. En az parola uzunluğu 8 karakter olması gerekirken tavsiye edilen karakter sayısı 12’dir.

Parolalar yukarıda sıralanan kurallara göre en az 8 karakter ile oluşturulduğunda, tek bir parola için en az 218.340.105.584.896 farklı olasılık anlamına gelir. Oluşturulan parolanın olasılığı kaba kuvvet saldırısını oldukça zorlaştırır, ancak parolanın kırılması yine de imkânsız değildir. Kırılması neredeyse imkânsıza yakın bir parola için, parola karakter sayısını artırmak gereklidir. Minimum karakter sayısı artarsa, parolanın kırılma süresi de artar.

Parola karmaşıklığının sağladığı yararların yanı sıra bazı zorlukları da beraberinde getirmektedir. Bunların başında parolanın unutulması gelir. Daha uzun ve içinde özel karakterlerin bulunduğu bir parolayı hatırlamak zordur. Hele bir de tüm parolalar farklı farklı olduğunda hatırlamak ve diğerleri ile karıştırmamak oldukça zor bir olaydır. Bu nedenle parolalar oluşturulurken belirli bir mantık takip edilmelidir.

Örneğin;

Ben Dört Çocuklu Bir Ailenin 3. Bireyiyim!

gibi bir cümleyi kendi gerçek yaşamınızdan yazabilirsiniz. Cümlenin ilk karakterleri ve özel karakterleri alındığında Bdcba3.B! gibi bir parola elde etmiş olunur.

Bu Web Sitesine (eğitim ile ilgili) 20 Aralık günü üye oldum.

gibi bir cümleyi üye olduğunuz bir web sitesinin ilgi alanına ve üyelik tarihine göre özelleştirebilir ve unutmamanızı sağlayabilirsiniz. İlk karakterleri ile özel karakterleri alındığında BWS(eii)20Aguo. gibi bir parola elde etmiş olunur.

Güçlü parola oluşturmak için farklı teknikleri de kullanabilirsiniz. Bunlardan birkaçına dair örnekler aşağıda verilmiştir.

Cümleler olduğu gibi yazılarak güçlü parola oluşturulabilir. Örneğin;

Bu Web Sitesine 4.Nisanda Python Ogrenmek icin uye oldum.

Siber Guvenlik dersini 13:30'a koymuşlar.

Benzer rakam ve harfleri birbirinin yerine kullanarak güçlü parolalar oluşturulabilir. Örneğin;

O yerine 0, L yerine 1, Z yerine 2, E yerine 3, S yerine 5, G yerine 6, B yerine 8 yazılarak;

Leylek = 13y13k

MorMenekşe = M0rM3n3k53

Zonguldak = 20n6u1dak

Bazı kelime veya karakterlerin yerine özel karakter kullanarak güçlü parolalar oluşturulabilir. Örneğin;

Yağmur yerine "" işareti, yüz yerine %, ve yerine &, ş yerine $, ı-i yerine !, boşluk yerine * yazılarak;

Yarın Yağmur yağacakmış = Yar!n""ya6acakm!$

Yüzmeyi severim = %mey!*sever!m

Parola için oluşturduğunuz cümledeki sadece sesli veya sadece sessiz harfleri kullanarak güçlü parolalar oluşturabilirsiniz. Örneğin;

Bu vatan 1 bütündür. = Bvtn1btndr.

Atam 30 Agustos'da zaferi ilan etti. = Aa30auo'azeiiaei.

Parola Güvenliğini Sağlama

Günümüzün çevrimiçi ortamında, güvenliğe yönelik basit "kullanıcı adı ve parola" yaklaşımı, siber suçlular için kolay bir avdır. Birçok oturum açma işlemi dakikalar içinde tehlikeye atılabilir ve özel veriler kötü niyetli kişilerin ellerine geçebilir.

Parolaların tahmin edilerek veya daha farklı yöntemler kullanılarak başkaları tarafından ele geçirilmesini engellemek için parolaların güvenliğinin sağlanması gerekmektedir. Bunlar için yapılması gereken hususlar şunlardır.

1. Gizli sorular ile güvenceye alma

2. İki aşamalı doğrulama yöntemi kullanılması

3. Biometrik kimlik doğrulama kullanılması

Gizli Soru

Güvenlik soruları, bir kullanıcının parolasını unutması veya çok faktörlü kimlik doğrulama (MFA) gerektiğinde ikincil kimlik doğrulama faktörlerini kaybetmesi durumunda hesabına yeniden erişim sağlamasına olanak sağlamak için birçok web sitesi tarafından kullanılır. Bununla birlikte, genellikle parolalardan çok daha zayıf bir kimlik doğrulama biçimidir.

Yeni bir çevrimiçi hesap oluşturulduğunda, web siteleri genellikle kullanıcıdan güvenlik sorularını yanıtlamalarını ister, böylece bir kullanıcı kendi kimliğini doğrulaması istenirse parolayı girecek, hatırlamaması durumunda kendisini kanıtlaması için güvenlik sorularını soracaktır. Bu sorular arasında

"Annenizin kızlık soyadı nedir?" , "Hangi şehirde doğdunuz?" veya "Gittiğiniz ilkokulun adı nedir?" gibi sorular yer almaktadır.

Şekil 18 Güvenlik soru ve cevap arayüzü

Maalesef web sitelerine üyelik veya hizmet alımı sırasında buna benzer çevrimiçi güvenlik sorularını doğru olarak yanıtladığınızda bu işlemin yeterli bir güvenli durum olmadığını söylemek gerekir. Bunun nedeni, hesabınıza erişmek isteyen birinin yanıtları bulmak için kolayca İnternet araştırması yapabilmesidir. Sosyal medya hesaplarınızı inceleyen saldırgan bilgisayar korsanı dayınıza yazdığınız bir mesaja ulaşabilir ve dayınızın soy isminden annenizin kızlık soyadını bulabilir.

Bir kullanıcının kimliğini doğrulamak için tek bir mekanizma olarak güvenlik sorularına güvenilmemelidir. Bir öneri olarak, "hangi şehirde doğdunuz?" gibi bir parola hatırlatma sorusuna ilk kayıt esnasında şehir adı olmayan ancak hatırda kalınabilecek bir ifade yazılabilir.

İki Aşamalı (Faktörlü) Doğrulama

İki faktörlü kimlik doğrulama (2FA), bir sisteme erişmek için iki farklı tanımlama biçimi gerektiren bir güvenlik sistemidir. Çevrimiçi bir hesabın, akıllı telefonun veya bir kapının güvenliğini güçlendirmek için iki faktörlü kimlik doğrulama kullanılabilir. Bu doğrula sistemi güvenli olan veriye veya sisteme erişilmeden önce kullanıcıdan iki tür bilgi talep ederek yapar. Bu bilgiler bir parola veya kişisel kimlik numarası (PIN), kullanıcının akıllı telefonuna gönderilen bir kod (SMS gibi) olabilir.

Yeni bir cihazda ilk kez oturum açılmak istenildiğinde, şifre ile telefon numaranıza gönderilen 4-8 basamaklı doğrulama kodu olmak üzere iki bilgi sağlanması gerekir. Kodu girilerek yeni cihaza güvenildiği doğrulanmış olur.

İki faktörlü kimlik doğrulama, yetkisiz kullanıcıların çalıntı bir parola kullanarak bir hesaba erişim sağlamasını önlemek için tasarlanmıştır. Kullanıcılar, özellikle aynı parolayı birden fazla web sitesinde kullanırlarsa, parolaların ele geçirilmesi konusunda büyük bir risk altında olabilirler.

İki faktörlü kimlik doğrulama, aşağıda verilen iki tekniğin birleşimidir:

• Bildiğiniz parolanız

• Sahip olduğunuz bir bilgi veya akıllı telefonunuza veya başka bir cihaza gönderilen bir kod içeren bir metin (veya bir akıllı telefon kimlik doğrulama uygulaması gibi).

2FA güvenliği artırsa da parolanın güvenliği için kusursuz değildir. Bilgisayar korsanları yine de hesaplara yetkisiz erişim elde edebilir. Bunu yapmanın yaygın yolları arasında kimlik avı saldırıları, hesap kurtarma prosedürleri ve kötü amaçlı yazılımlardır.

Biometrik Kimlik Doğrulama

Biyometrik kimlik doğrulama, kişinin kendisini kanıtlaması ve doğru kişi olduğunu ispatlamak için bireyin eşsiz biyolojik özelliklerine dayanan bir güvenlik sürecidir. Biyometrik doğrulama sistemleri, elde edilen biyometrik veriyi veri tabanındaki kayıtlı, depolanmış ve daha önceden onaylanmış gerçek verilerle karşılaştırır. Elde edilen biyometrik veri örneği ile kayıtlı olan biyometrik veri eşleşirse, kimlik doğrulaması onaylanır. Kişiye özgü olan bu biyometrik veriler unutulamaz veya kaybedilemez, taklit edilemez olmaları, bu kimlik doğrulamayı diğer yöntemlerden ayırır. Ancak son derece özel olan biyometrik kişisel bilgilerin kullanılıyor olması, siber güvenlik açısından önem gösterilmesini gerektirir.

Biyometrik kimlik doğrulama yöntemleri, birden fazla biyometrik deseni birleştirerek veya biyometrik doğrulamayı tamamlayan geleneksel bir şifre veya ikincil cihazla birlikte iki faktörlü kimlik doğrulama (2FA) veya çok faktörlü kimlik doğrulama (MFA) biçimi olarak da kullanılabilir.

Günümüzde yaygın olarak kullanılan biyometrik kimlik doğrulama teknolojileri şunlardır:

Parmak izi tarama: Parmak ucunda yer alan izlerin modelinde belirli özellikleri arayarak kimlik doğrulama yapar. Harici bir özelliğe sahip bir görüntüyü yakalamanın dezavantajı, bu görüntünün kodlanmış biçimde saklansa bile kopyalanabilmesidir. Parmak izleri, taklit edilebilen bir kimlik doğrulama yöntemidir. Bazı parmak izi çizgi modelleri o kadar benzerdir ki pratikte bu yüksek bir yanlış kabul oranına neden olabilir.

Retina taramaları, bireyin iç gözünü kaplayan ışığa duyarlı yüzeyde kan damarı deseninin bir görüntüsünü üretir.

İris tanıma: İnsanın göz bebeğinin etrafında yer alan benzersiz halkadaki desene göre yapılan kimlik doğrulamadır. Bir iris taraması gerçekleştirildiğinde, tarayıcı bir irisin benzersiz özelliklerini okur ve bunlar daha sonra şifrelenmiş bir koda dönüştürülür. İris taraması, özellikle kızılötesi ışık kullanılarak yapıldığında çok iyi sonuçlar vermektedir.

Parmak damar kimliği ve avuç tanıma: Bir insanın parmağında yer alan ve benzersiz olan damar desenine göre yapılan bir kimlik doğrulamadır. Damar deseni tanıma durumunda, parmaktaki damarların bitiş noktaları ve çatallanmaları bir görüntü biçiminde yakalanır, sayısallaştırılır ve şifreli bir koda dönüştürülür.

Yüz tanıma sistemleri: Bu sistemler, bir eşleşme belirlemek için yüzün farklı bölümlerinin şeklini ve konumunu analiz ederler. Bununla

birlikte, yüz tanımanın bir takım önemli dezavantajları da vardır. Örneğin bir kişinin tanımasını mümkün kılmak için genellikle doğrudan kameraya bakması gerekir.

Ses tanıma sistemleri, daha değişken koşullardan ziyade konuşmacının ağzının ve boğazının şekli tarafından oluşturulan özelliklere dayanır.

Biyometrik sahtekârlık, başka bir kişi olarak tanımlanmak amacıyla sahte bir biyometrik özelliğin sunulmasıdır. Bu, kopyalanmış bir parmak izi veya tahrif edilmiş iris modeline sahip bir kontakt lens kullanmayı içerebilir.

2.5. Parola Kırma Teknikleri

Parola kullanımı, kimlik doğrulama sistemlerinde en sık kullanılan yöntemdir. Kullanıcı ya da bir ağ cihazı, doğru parolayı kimlik doğrulayıcıya sunabilirse, iddia ettiği kullanıcı ya da cihaz olduğunu ispat etmiş olur. Parola, kimliğin ispatı olduğundan güvenliği ve gizliliği son derece önemlidir. Ancak tehdit aktörleri, parolayı elde etmeye yönelik oltalama saldırılarından, tersine mühendislik yöntemlerine kadar çok çeşitli yöntemler kullanırlar. Temel olarak parolayı elde etme yöntemleri "parola kırma (password cracking)" olarak adlandırılır.

Parola tahmin etme

Saldırgan açısından, uygulaması en kolay olan parola kırma tekniğidir. Hedef kullanıcı hakkında bilgi toplandıktan sonra, doğum tarihi, memleketi, tuttuğu futbol takımı gibi kişisel bilgilerden yola çıkarak parola tahmini yapılır. Bu kategorideki diğer bir yöntem de, en sık kullanılan "qwerty" veya "123qwe" parolaların denenmesidir. Yine bu kısımda ele alınabilecek diğer bir husus olarak, aynı parolanın farklı yerler için de kullanılması ile ilgilidir. Eğer kullanıcı her yerde aynı parolayı kullanıyorsa ve bu kullanım alanlarından birinde parola kırılmışsa, saldırganın ilk yapacağı aynı parolayı farklı noktalar için denemek olacaktır.

Sözlük saldırıları

Brute force (kaba kuvvet ya da deneme yanılma) saldırılarında kullanılan yöntemdir. Bir yazılım tarafından belirli bir kelime listesinde (sözlük) yer alan parolaların sıralı olarak denenmesi mantığına dayanır. Bu sözlük, en sık kullanılan gerçek kelimeleri içerdiği gibi, "Ankara06" ve "Passw0rd1" gibi yine sık kullanılan parolalardan da oluşabilir. Tehdit aktörleri, bu listelere internet ortamından rahatlıkla ulaşabilmektedir. Sözlük saldırısı kategorisinde yer alabilecek diğer bir yöntem de, karakter üreteçleri kullanarak kendi özelleştirilmiş listelerini oluşturmak ve bu oluşturulan liste üzerinden deneme yanılma saldırısı yapmaktır. Bu yöntem hem parola üretmek hem de denemek olarak iki kısımdan oluştuğu için uzun zaman alabilir. Kullanıcılar unutmamak için genellikle kısa parolalar kullandıklarından, bu saldırılar oldukça başarılı saldırılardır.

Önceden hesaplanmış parola listeleri

Daha önce ifade edildiği gibi, parolalar veritabanlarında genellikle özetlenerek (hash) saklanır. Bir şekilde bu veritabanı eğer saldırgan tarafından eşe geçirilmişse, parola açık olarak veri tabanında yer almayacaktır. MD5 ve SHA gibi özetleme fonksiyonları tek yönlü matematiksel fonksiyon olduklarından, hash değerinden parolanın ham haline ulaşmak tersine mühendislik yöntemi ile mümkün değildir. Ancak, bu durumda saldırgan önceden hesaplanan hash değerlerinin yer aldığı listelerden yola çıkarak parolanın ham haline ulaşabilir (rainbow table attacks). Ancak bu yöntemin başarılı olabilmesi için, parolanın bu listede önceden yer alıp özetlenmiş olması gerekir. Sık kullanılan kelimeler (ya da parolalar)

bu listede çok büyük ihtimalle yer aldığından, kırılması muhtemeldir. Bu nedenle, parolanın tek başına özetlenmiş olarak veritabanında kaydedilmesi yeterli bir güvenlik önlemi değildir, parolanın seçimi de son derece önemlidir.

Parolaların şifrelenmesi, özetlenmesi ya da veritabanına çeşitli tekniklerle kaydedilerek güvenliğinin sağlanması önemli bir konudur. Ancak tüm bu parola güvenlik çabalarını riske atabilecek bir durum vardır, kullanıcının hafızasında yer alan bu parola bilgisini bilinçli ya da bilinçsiz olarak saldırgana vermesidir. Saldırganlar son derece etkili sosyal mühendislik teknikleri (senaryoları) ile bu parolaları elde etmek için uğraşabilirler. Oltalama saldırıları ile bu işlem yapılabildiği gibi, yetkili bir otorite gibi görünerek parolayı kullanıcıdan isteyebilirler. Kullanıcı, parola girdiği her yere dikkat etmeli ve parolayı kesinlikle hiç kimseye vermemelidir.

3. GÜVENLİK ZAAFİYETİ DERECELENDİRME

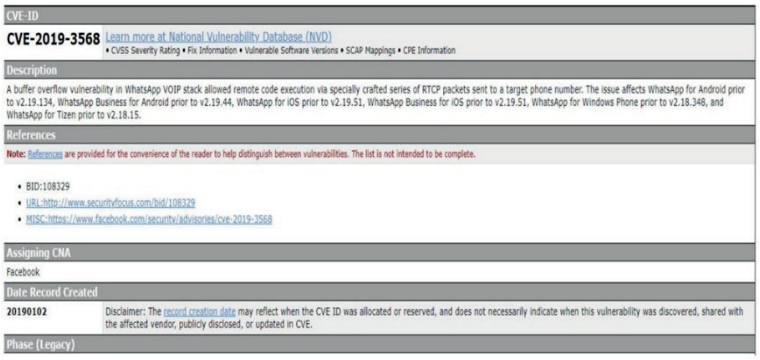
Siber güvenlikte amaç, sistemleri ve kullanıcıları tehdit aktörlerinin kötü amaçlı saldırılarına karşı korumaktır. Saldırılar, teknik, mantıksal veya fiziksel olabilen güvenlik açıklarını hedefler. Risk yönetimi gereği tüm potansiyel tehditler ele alınmalı ve güvenlik açısından riskleri tehdidin önemine göre ele alınmalıdır. Zararlı yazılımların resmi bir isimlendirme kural yapısı yoktur. Zararlı yazılımların bilinen isimleri, genellikle tehdidi tanımlayan araştırmacılar tarafından verilmiş isimlerdir. Bu başlıkta güvenlik tehditleri ve zafiyetlerin tanımlanmasında kullanılan isimlendirme ve zaafiyet derecelendirmesi ele alınacaktır.

3.1. CVE İsimlendirmesi

Siber güvenlik dünyasında bir güvenlik açığıyla ilişkili riski derecelendirmek ve bu güvenlik açığı hakkında iletişim kurmak için bir isimlendirme ve puanlama sistemi kullanılır. Bu sayede, siber güvenlik tarafları aynı güvenlik açığı hakkında herhangi bir kafa karışıklığı olmadan iletişim kurabileceklerdir.

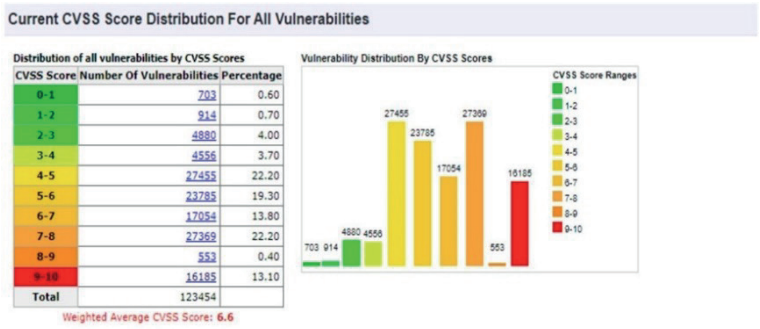
CVE (Common Vulnerabilities and Exposures), Ortak Güvenlik Açıkları ve Etkilenmeler sistemi, genel olarak bilinen bilgi güvenliği açıkları ve riskleri için bir referans yöntemi sağlar. Belirli tanımlamalara göre güvenlik zafiyetlerinin tutulmasını sağlayan bir isimlendirme veri tabanıdır. Bu veri tabanına https://cve.mitre.org/ sitesinden ulaşılabilir.

CVE yapısında, 1999 yılından itibaren tespit edilen güvenlik açıklarını listelemek için bir isimlendirme kuralı geliştirmiştir. Buna göre tespit edilen açık, CVE-YYYY-NNNN olarak isimlendiriliyordu. YYYY tespit edilen yılı, NNNN ise güvenlik açığına verilen numarayı gösterir. Ancak daha sonra bu isimlendirme geliştirildi. Aynı web sayfasından yeni isimlendirme kuralına bakılabilir. Örneğin Şekil 19'daki ekran görüntüsünde, CVE-2019-3568 numaralı WhatsApp uygulamasına yönelik bir güvenlik açığı listelenmektedir.



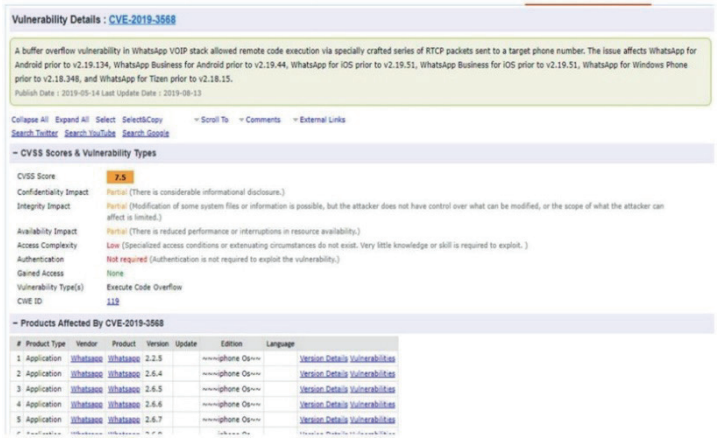
Şekil 19 Örnek CVE ekranı

Belirli bir CVE ile ilişkili daha fazla ayrıntılı bilgi için https://www.cvedetails.com/ sayfası ziyaret edilebilir.



Şekil 20 Zafiyete ilişkin CVE skor belgesi

CVE-2019-3568 numaralı güvenlik açığına ilişkin detaylı incelemenin ekran görüntüsü Şekil 3.21'de gösterildiği gibidir.



Şekil 21 CVE detay ekranı

Güvenlik açığına ilişkin detaylı bilgilerin sunulduğu bu sayfada, güvenlik açığının açıklaması, güvenlik açığı türü, etkilenen ürünler, zaafiyetin karmaşıklığı gibi bilgilerin yanı sıra, güvenlik açığının derecesini belirten CVSS skoru da yer almaktadır (Örnekte 7.5).

3.2. Zafiyet Derecelendirmesi (CVSS)

CVSS, Ortak Güvenlik Açığı Puanlama Sistemi (Common Vulnerability Scoring System) olarak adlandırılan ve bir güvenlik açığının (güvenlik zafiyetinin) derecelendirilmesi için kullanılan bir sistemdir. Sistemde güvenlik açığının önem düzeyine göre, kompozit metrikler kullanılarak 0 (en az tehlikeli) ile 10 (en çok tehlikeli) arasında puanlama yapılır.

Puanlama birden fazla parametreye bakılarak hesaplanır. CVSS puanlama yapısı birkaç kez değişmiştir. Günümüzde kullanılan en güncel puanlama sürümü, 2019 yılı haziran ayından beri kullanılan CVSSv3.1 sürümüdür.

CVSSv2 puanının hesaplanmasında temel puanlama (base), zamansal puanlama (temporal) ve çevresel (environmental) puanlama olmak üzere üç ölçüt (metric) kullanılmaktadır.

Şekil 22 CVSS Base Score Metrikleri

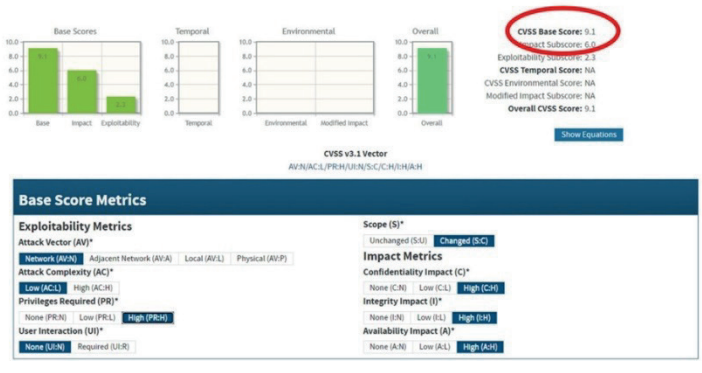
Temel puanlamada, siber güvenliğin temel bileşenleri (C-I-A) bir alt grupta, saldırı vektörü, erişim karmaşıklığı ve kimlik doğrulama da diğer bir alt grupta hesaplamaya katılır.

Erişim vektöründe yer alan "Lokal Erişim (Local)" istismarın ağ üzerinden yapılamayacağını, sadece yerel cihazdan yapılabildiğini belirtir. "Bitişik Ağ (Adjacent Network)" ifadesi saldırının aynı ortamda bulunan, aynı mantıksal ağdan yapılabildiğini belirtir. "Ağ (Network)" ifadesi ise, internet gibi farklı ağ üzerinden (ya da farklı VLAN üzerinden) yapılabildiğini belirtir. Bu durum, güvenlik açığı puanının daha yüksek olduğu anlamına gelir.

Zafiyetin erişim karmaşıklığı (access complexity) için düşük, orta ve yüksek ölçekler kullanılmaktadır. Karmaşıklık düzeyinin artması, zafiyetin puanını arttır.

Kimlik doğrulamada (Authentication) ise çoklu doğrulama (Multiple), tek doğrulama (Single) ve doğrulama yok (None) olmak üzere yine üç farklı ölçüt kullanılmaktadır. Çoklu kimlik doğrulamada, zafiyetin birden fazla kez kimlik denetiminden geçildikten sonra gerçekleşebileceği belirtilir. Her kimlik doğrulama bir güvenlik olduğundan, çoklu kimlik doğrulamaya sahip bir zafiyet düşük puanlı olmasını sağlar. Tek kimlik doğrulama ise, zafiyetin gerçekleşmesi için sadece bir kez kimlik doğrulamadan geçilmesinin yeterli olduğu anlamına gelir. Kimlik doğrulamanın olmaması, bu alt metrik için en tehlikeli olanıdır.

Aynı şekilde derecelendirmede gizlilik (confidentiality), bütünlük (integrity) ve kullanılabilirlik (availability) parametrelerinin her biri için üç düzey belirlenmiştir. CVSSv3.1 için güncellenmiş puanlama ölçütleri https://nvd.nist.gov/vuln-metrics/cvss/v3- calculator adresinde yer almaktadır.



Şekil 23 CVSS skor hesaplama

CVSSv3.1 için yukarıdaki bağlantıda yer alan hesaplama aracı kullanılarak, parametrelerin değişiminin CVSS skoruna etkisi görülebilir. Şekil 23'deki ekran görüntüsünde, CVSS temel metrik skoru 9,1 olarak belirlenen bir güvenlik zafiyetinin özellikleri görüntülenmektedir. Aynı araç kullanılarak, zamansal puanlama (temporal) ve çevresel (environmental) puanlama hesaplanabilir.

4. GÜVENLİK YAZILIMLARI

Önceki bölümlerde ele alındığı gibi ağlar siber saldırıların hedefidir. Ağları korumak için ağ düzeyinde koruma sağlayan IPS, IDS, güvenlik duvarları gibi sistemler kullanılır. Aynı şekilde son kullanıcı cihazlarında da kullanılabilecek güvenlik yazılımları vardır. Bazı güvenlik çözümleri birden fazla bileşen de içerebilir. Örneğin hem antivirüs hem de anti-malware aynı yazılımda sunulabilir.

4.1. Antivirüs

Virüsleri tespit etmek ve sistemden kaldırmak için bir hoşta yüklenen programlardır. Windows Defender, Norton Security, McAfee, Trend Micro gibi birçok antivirüs yazılımı bulunmaktadır. Antivirüsler genellikle daha önceden antivirüs üreticileri tarafından tespit edilen ve zararlı yazılımın karakteristik özelliklerini (imzaları) kaydeden veri tabanı yapısını kullanırlar. İmza veri tabanının sürekli olarak güncel tutulması bu nedenle önemlidir. Birçok antivirüs programı, verileri analiz ederek gerçek zamanlı koruma da sağlayabilir. Bu programlar aynı zamanda sisteme gerçek zamanlı olarak tanınmadan önce girmiş olabilecek mevcut zararlı yazılımları da tarar.

Yazılım olarak kullanılan konak tabanlı antivirüs koruması, ajan tabanlı antivirüs olarak da bilinir. Ajan tabanlı antivirüs, korunan her makinede çalışır ve merkezi bir sistemden tarama gerçekleştirir. Aracısız sistemler, aynı anda bir bilgisayarda birden çok işletim sistemi örneğinin çalıştığı sanallaştırılmış ortamlar için popüler hale gelmiştir. Sanallaştırılmış her sistemde çalışan ajan tabanlı antivirüs, sistem kaynakları üzerinde ciddi bir yük oluşturabilir.

4.2. AntiMalware

Günümüzde anti-virüs yazılımları ile birlikte entegre olarak çalışan yazılımlardır. Bu programlar, üç farklı yaklaşım kullanarak virüsleri algılayabilir. İmza tabanlı yaklaşımda, bilinen zararlı yazılım dosyalarının çeşitli özelliklerini (imzalarını) tanır. Sezgisel tabanlı yaklaşımda, çeşitli zararlı yazılım türleri tarafından paylaşılan genel özellikleri tanır. Davranış temelli yaklaşımda ise şüpheli davranışların analizini kullanır.

4.3. Konak Tabanlı Güvenlik Duvarı

Yazılımsal güvenlik duvarı, sistemi kötü amaçlı yazılımlardan, solucanlardan, virüslerden ve e-posta eklerinden korumayı amaçlayan konak tabanlı güvenlik duvarı programlardır. Genellikle konak bilgisayardan çıkan ve konak bilgisayara giren belirli protokollerin filtrelenmesini sağlamak üzere geliştirilmişlerdir.

4.4. Diğer Yazılımlar

Gelişmiş Kötü Amaçlı Yazılım Koruması (AMP)- Virüslere ve kötü amaçlı yazılımlara karşı uç nokta koruması sağlar.

E-posta Güvenlik Aracı (ESA)- SPAM ve potansiyel olarak kötü niyetli e-postaların uç noktaya ulaşmadan önce filtrelenmesini sağlar.

Web Güvenlik Aracı (WSA)- Konakların web üzerindeki tehlikeli konumlara ulaşmasını önlemek için web sitelerinin filtrelenmesini ve kara listeye alınmasını sağlar. Kullanıcıların internete nasıl eriştiğini kontrol eder ve kabul edilebilir kullanım politikalarını uygulayabilir, belirli sitelere ve hizmetlere erişimi kontrol edebilir ve zararlı yazılım taraması yapabilir.

Ağ Kabul Kontrolü (NAC)- Yalnızca yetkili ve belirli kriterlerin sağlandığı (örneği işletim sisteminin güncel olması) sistemlerin ağa bağlanmasına izin verir.

5. GÜVENLİK OPERASYONLARI MERKEZİ

Güvenlik operasyonları merkezi (Security Operations Center – SOC), kurumsal ve teknik düzeyde güvenlik sorunlarıyla ilgilenen merkezi bir birimdir (digitalguardian.com, 2023). Güvenlik Operasyon Merkezi, siber tehditleri önlerken, saldırıları tespit eder, ağı analiz eder ve olası tehditlere yanıt verir. Daha genel bir ifade ile bir kuruluşun güvenlik duruşunu sürekli olarak izlemek ve iyileştirmek için insanları, süreçleri ve teknolojiyi kullanan kuruluş içindeki merkezi bir işlevdir.

SOC, birbiri ile uyum içinde çalışan birimlerden ve teknolojilerden oluşan bir merkezi nokta olarak ele alınabilir. Bir kurumda SOC yapısının bulunması, ağın daha geniş bir ifade ile kurumdaki varlıkların sürekli izlenmesini sağlayarak, saldırı öncesi, saldırı anı ve saldırı sonrası eylemlerin gerçekleştirilerek potansiyel (veya devam eden) tehditlerin ortadan kaldırılmasını sağlar. SOC yapısının varlığı sadece kurumun fiziksel varlıklarını değil, iş döngüsünü, süreci ve yapıyı da korur.

Şekil 24 SOC bileşenleri

5.1. SOC Fonksiyonları

Güvenlik Operasyonları Merkezi, her biri son derece önemli olan ile ilişkili birçok fonksiyonlardan oluşur. Bu fonksiyonların yürütülmesi, ağın daha fazla güvenli olmasını sağlayacaktır. Aşağıda bu fonksiyonlardan bazıları ele alınmıştır (mcafee.com, 2023).

1. Mevcut Kaynakların Listesini Alma: SOC, farkında olmadığı ya da varlığından habersiz olduğu kaynakları koruyamaz. Bu nedenle kurumda korunması gereken kaynakları ve varlıkların belirlenmesi ile bu kaynakların nasıl korunacağının belirlenmesi gerekir. Bu aşama aynı zamanda saldırı yüzeyinin ve saldırı vektörlerinin de tanımlanmasını sağlar. Savunma esasında kullanılabilecek donanımların, yazılımların ve araçların varlığının tespiti bu fonksiyon içerisinde ele alınır.

2. Hazırlık ve Önleyici Bakım: Ağlar için en tehlikeleri saldırılardan birisi, sıfırıncı gün olarak bilinen saldırılardır. Bu tür saldırılardan korunmanın en önemli yöntemlerinden biri, hazırlık yapma ve önleyici bakım yapmaktır. SOC ekibinin, güncel saldırıları takip etmesi gerektiği gibi en güncel güvenlik gelişmelerini de takip etmesi gerekir. Ancak yine de saldırı gerçekleşebilir. Bu nedenle olası bir saldırı durumunda, felaket kurtarma planının bulunması gerekir. Önleyici bakım olarak, tüm sistemlerin güncel olduğu sağlanmalıdır. Yine sistemdeki beyaz liste (kabul edilebilir) ya da kara listenin de (kabul edilemez) bu doğrultuda güncellenmesi gerekebilir. Aynı şekilde personelin de periyodik olarak eğitimler ile bilgilendirilmesi gerekir.

3. Sürekli Proaktif İzleme: Saldırının ne zaman gerçekleşeceği bilinmez. Bu nedenle anormal bir durum oluşup oluşmadığının belirlenmesi için varlıkların sürekli olarak izlenmesi gerekir. Ağdaki günlük dosyalarının, mesajların ve olayların izlenmesini sağlayan SIEM yazılımları bu amaç doğrultusunda kullanılır.

4. Uyarı Sıralaması ve Yönetimi: Ağın izlenmesi sırasında çok farklı düzeyde ve önemde tehditler yakalanabilir. SOC analistinin görevi, uyarılara göre tehditleri önem sırasına dizmek ve acil eylem gerekenler ile diğerlerini birbirinden ayırt edebilmektir.

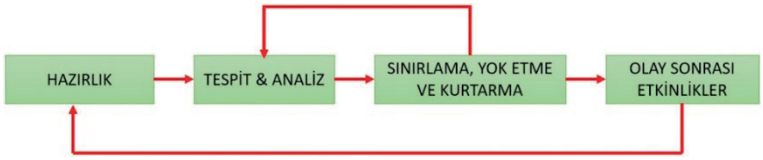
5. Olay Müdahale: Tehdit ya da saldırının gerçekleştiği anlaşıldığı anda yapılması gerekenleri ifade eder. Genellikle ilk verilen tepki, saldırının yayılmasını önlemek amacıyla izolasyon sağlamaktır. Zararlı yazılımın tespit edilip silinmesi, zararlı işlemin durdurulması ve zararlı dosyanın silinmesi bu aşamada gerçekleşir. Hedef izole edildikten sonra tüm ağ tekrar analiz edilir.

6. Kurtarma ve İyileştirme: Saldırı gerçekleştikten sonra mümkün olan en kısa sürede sistemin tekrar devreye alınması gerekir. Geciken her süre, itibar ve parasal kayıp olarak yorumlanabilir. Sistem yapılandırmalarının düzenlenmesi, yedeklerin yüklenmesi gibi işlemler bu fonksiyonun sorumluluğundadır.

7. Log Yönetimi: SOC için belki de en önemli işlemlerdendir. Sistemdeki tüm kaynaklardan gelen loğların ve olayların SIEM yazılımları ile yönetimini ifade eder. Hem saldırı öncesi hem de saldırı sonrası ayrı ayrı incelenmesi gereken bir durumdur. Saldırı öncesinde anomali tespiti yapılması bir örnek olarak verilebilir. Aynı şekilde saldırı sonrasında, saldırının nasıl gerçekleştiğinin ve etkisinin analizi de yine bu fonksiyonun sorumluluğundadır.

5.2. Olay Müdahale Yaşam Döngüsü

Bir saldırıya hazırlıklı ve planlı olmak önemlidir. Olay müdahalesi bir kez gerçekleşen bir durum değil, her zaman gelişen bir döngüdür. Bu yöntemlerden biri de Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından belirlenen, olay müdahale yaşam döngüsüdür.



Şekil 25 .Olay Müdahale Yaşam Döngüsü

Hazırlık, olay müdahale ekibinin bir olaya nasıl müdahale edecekleri konusunda eğitimi aşamasıdır.

Tespit ve Analiz- Sürekli izleme yaparak, bir olayı hızla tanımlar, analiz eder ve doğrular.

Sınırlama, Yok Etme ve Kurtarma- Tehdidi kontrol altına almak, kurumsal varlıklar üzerindeki etkiyi ortadan kaldırmak, verileri ve yazılımı geri yüklemek için yedekleri kullanmak gibi işlemleri uygular. Daha fazla bilgi toplamak veya araştırmanın kapsamını genişletmek için tespit ve analize geri dönebilir.

Olay Sonrası Aktiviteler- Daha sonra olayın nasıl ele alındığının belgelenmesidir. Gelecekteki müdahale için güncellemeler önerir ve bir tekrar oluşmasının nasıl önleneceğini belirtir.

BÖLÜM ÖZETİ

Saldırı ve savunma için bilgi toplama yöntemleri, pasif ve aktif olmak üzere iki kategoriye ayrılır. Pasif Bilgi Toplama, doğrudan etkileşim olmadan, internet kaynaklarından bilgi toplanmasıdır. Örnekler arasında IP adresleri, domainler ve web sayfaları hakkında bilgi toplama yer alır. Aktif Bilgi Toplamada ise hedef sistemle doğrudan iletişime geçilerek yapılan, riskli bilgi toplama yöntemidir. Network mapping ve WireShark gibi araçlarla ağ haritalaması ve paket analizi yapılabilir. Ayrıca fiziksel güvenlik, veri bütünlüğü ve veri güvenliği gibi temel güvenlik önlemleri ve parola güvenliği hakkında bilgiler sunulmuştur. Parola karmaşıklığı ve güvenliğini sağlama yöntemleri detaylandırılmıştır. Bunun yanında siber güvenlikte zafiyetlerin derecelendirilmesi açıklanmıştır. Bu derecelendirme tehditlerin ciddiyetini ve aciliyetini belirlemek için kullanılır. Zafiyetlerin etkisini değerlendirmek için kullanırlar. Kritik Zafiyet Skorlama Sistemi (CVSS) açıklanmıştır. Bu sistem, zafiyetlerin teknik özelliklerine ve potansiyel etkilerine göre puanlama yapar. Zafiyetlerin tespiti, değerlendirilmesi ve giderilmesi süreçlerini içeren Zafiyet Yönetimi süreci de açıklanmıştır. Bu süreç, organizasyonların güvenlik duruşunu güçlendirmek için kritik öneme sahiptir.

GÖZDEN GEÇİRELİM

1. **Siber güvenlikte pasif bilgi toplama sürecinde hangi bilgiler toplanabilir?**
   a) Yalnızca IP adresleri
   b) Domain bilgileri ve web sayfaları
   c) Yalnızca Whois sorgusu sonuçları
   d) IP adresleri, domain bilgileri ve web sayfaları

2. **Whois sorgusu ne amaçla kullanılır?**
   a) Web sayfasının aktif olup olmadığını öğrenmek
   b) Alan adı sahibinin iletişim bilgilerine ulaşmak
   c) IP adreslerinin dağıtımını yapmak
   d) Ağ güvenliği analizi yapmak

3. **RIPE NCC ne iş yapar?**
   a) Alan adı sorgulama
   b) Avrupa ve Ortadoğu bölgesine IP adresi dağıtımı
   c) Güvenlik duvarı hizmetleri
   d) Parola güvenliği sağlama

4. **Bir web sayfasının aktif olup olmadığını öğrenmek için hangi araç kullanılır?**
   a) Whois sorgusu
   b) RIPE NCC
   c) ns.tools
   d) Shodan

5. **Shodan arama motoru ne için kullanılır?**
   a) Domain bilgilerini sorgulamak
   b) İnternete bağlı cihazları bulmak
   c) Parola güvenliği test etmek
   d) Veri bütünlüğünü sağlamak

6. **Nmap aracı ne işe yarar?**
   a) Paket analizi yapmak
   b) Ağ haritalaması yapmak
   c) Güvenlik duvarı oluşturmak
   d) Veri yedeklemek

7. **WireShark ile ne tür bilgiler toplanabilir?**
   a) Parola güvenliği bilgileri
   b) Ağ paketlerinin analizi
   c) Güvenlik zafiyeti derecelendirmesi
   d) Domain sorgulama sonuçları

8. **Google Hack Veritabanı ne için kullanılır?**
   a) Güvenlik zafiyetleri bulmak
   b) Parola karmaşıklığını test etmek
   c) Ağ güvenliği analizi yapmak
   d) IP adresi sorgulama

9. **Bilgisayar sistemlerinin fiziksel güvenliği için hangi önlem alınmalıdır?**
   a) Parola güvenliği sağlamak
   b) Kesintisiz güç kaynağı kullanmak
   c) Virüs taraması yapmak
   d) Güvenlik duvarı kurmak

10. **Parola karmaşıklığı sağlamak için hangi kural uygulanmalıdır?**
    a) Parola içinde sadece rakamlar kullanılmalıdır
    b) Parola, hesap adını içermemelidir
    c) Parola, en az 4 karakter olmalıdır
    d) Parola, yalnızca özel karakterler içermelidir

Yanıt Anahtarı: 1-D, 2-B, 3-B, 4-C, 5-B, 6-B, 7-B, 8-A, 9-B, 10-B

Kaynakça

digitalguardian.com. (2023, 8 4). https://digitalguardian.com/blog/what-security-operations-center-soc adresinden alındı

mcafee.com. (2023, 8 10). mcafee.com: https://www.mcafee.com/enterprise/en-us/security-awareness/%20operations/%20what-is-soc.html adresinden alındı

BÖLÜM 7

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ

ANAHTAR KAVRAMLAR

Bilgi Güvenliği Yönetim Sistemi,
Kapsam Belirleme, Risk Değerlendirmesi

ÖĞRENME HEDEFLERİ

1. Bilgi Güvenliği Yönetim Sistemini (BGYS) açıklar.
2. BGYS uygulanacak kuruluşun kapsamını açıklar.
3. BGYS'nin uygulanmasında üst yönetimin rolünü açıklar.

YEDİNCİ BÖLÜM

GİRİŞ

Bilgi Güvenliği Yönetim Sistemi, bir bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için gereklilikleri açıklamak amacıyla International Standardization Organization (ISO) tarafından hazırlanmış, ISO/IEC 27001 olarak da anılan, standarttır. Orijinal adı "ISO/IEC 27001 Information security, cybersecurity and privacy protection — Information security management systems — Requirements" şeklinde geçmektedir (ISO, 2023). Bu bölüm ilgili standardın orijinal metnine sadık kalarak oluşturulmaya çalışılmıştır.

Bilgi güvenliği yönetim sisteminin benimsenmesi, kuruluş için stratejik bir karardır. Bir kuruluşta bilgi güvenliği yönetim sisteminin kurulması ve uygulanması, kuruluşun ihtiyaç ve hedeflerine, güvenlik gereksinimlerine, kullanılan organizasyonel süreçlere, kuruluşun büyüklüğüne ve yapısına bağlı olarak farklılık gösterir. Tüm bu faktörlerin zaman içinde de değişmesi beklenir.

Bilgi güvenliği yönetim sistemi, bir risk yönetimi süreci uygulayarak bilginin gizliliğini, bütünlüğünü ve kullanılabilirliğini korur ve ilgili taraflara risklerin yeterince yönetildiğine dair güven verir. Bilgi güvenliği yönetim sisteminin, kuruluşun süreçlerinin ve genel yönetim yapısının bir parçası olarak entegre olması ve süreçlerin, bilgi sistemlerinin ve kontrollerin tasarımında bilgi güvenliğinin dikkate alınması önemlidir. Bir bilgi güvenliği yönetim sistemi uygulamasının, kuruluşun ihtiyaçlarına uygun olarak ölçeklendirilmesi beklenmektedir.

1. KURULUŞUN KAPSAMI

Bu standart kapsamında, kuruluş bağlamında bir bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için gereksinimleri belirtir. Aynı zamanda kuruluşun ihtiyaçlarına göre uyarlanmış bilgi güvenliği risklerinin değerlendirilmesi ve ele alınmasına yönelik gereksinimleri de içermektedir. Standart içerisinde belirtilen gereksinimler geneldir ve türü, boyutu veya niteliği ne olursa olsun tüm kuruluşlar için geçerli olması amaçlanmıştır.

Kuruluşu ve kapsamını tanımak

Kuruluş, amacı ile ilgili olan ve bilgi güvenliği yönetim sisteminin amaçlanan sonuçlarına ulaşma yeteneğini etkileyen dış ve iç bağlamını belirlemelidir. Bu bağlamların belirlenmesi, ISO 31000:2018 Risk Yönetimi Standardında açıklanmıştır (ISO, 2023).

Kuruluşun dış bağlamının incelenmesi aşağıdakileri içerebilir, ancak bunlarla sınırlı değildir:

• Uluslararası, ulusal, bölgesel veya yerel olsun, sosyal, kültürel, politik, yasal, düzenleyici, mali, teknolojik, ekonomik ve çevresel faktörler;

• Kuruluşun hedeflerini etkileyen temel itici güçler ve eğilimler;

• Dış paydaşların ilişkileri, algıları, değerleri, ihtiyaçları ve beklentileri;

• Sözleşmeye dayalı ilişkiler ve taahhütler;

• Ağların ve bağımlılıkların karmaşıklığı

Kuruluşun iç bağlamının incelenmesi aşağıdakileri içerebilir ancak bunlarla sınırlı değildir:

• Vizyon, misyon ve değerler;

• Yönetişim, organizasyon yapısı, roller ve sorumluluklar;

• Strateji, hedefler ve politikalar;

• Kuruluşun kültürü;

• Kuruluş tarafından benimsenen standartlar, kılavuzlar ve modeller;

• Kaynaklar ve bilgi açısından anlaşılan yetenekler (örneğin sermaye, zaman, insanlar, fikri mülkiyet, süreçler, sistemler ve teknolojiler);

• Veriler, bilgi sistemleri ve bilgi akışları;

Algılarını ve değerlerini dikkate alarak iç payd
• aşlarla ilişkiler;

• Sözleşmeye dayalı ilişkiler ve taahhütler;

• Karşılıklı bağımlılıklar ve ara bağlantılar.

İlgili tarafların ihtiyaç ve beklentilerini göz önünde bulundurmak

Kuruluş şunları belirlemelidir:

Bilgi Güvenliği Yönetim Sistemi ile ilgili ilgili taraflar;

a) Bu ilgili tarafların ilgili gereklilikleri;

b) Bu gerekliliklerden hangileri Bilgi Güvenliği Yönetim Sistemi aracılığıyla ele alınacaktır.

c) İlgili tarafların gereklilikleri, yasal ve düzenleyici gereklilikleri ve sözleşmeden doğan yükümlülükleri içerebilir.

Bilgi güvenliği yönetim sisteminin kapsamını genişletmek

Kuruluş, kapsamını oluşturmak için bilgi güvenliği yönetim sisteminin sınırlarını ve uygulanabilirliğini belirlemelidir. Bu kapsamı belirlerken, kuruluş şunları dikkate almalıdır:

a) Kuruluşu ve kapsamını tanımak başlığında verilen dış ve iç bağlamları;

b) İlgili tarafların ihtiyaç ve beklentilerini göz önünde bulundurmak başlığında bulunulan gereklilikler;

c) Kuruluş tarafından gerçekleştirilen faaliyetler ile diğer kuruluşlar tarafından gerçekleştirilen etkinlikler arasındaki arabirimler ve bağımlılıklar.

Kapsam, yazılı belge olarak sunulmalıdır. Kuruluş, bu belgenin gerekliliklerine uygun olarak, ihtiyaç duyulan süreçleri ve bunların etkileşimlerini de içeren bir bilgi güvenliği yönetim sistemi kurmalı, uygulamalı, sürdürmeli ve sürekli iyileştirmelidir.

2. LİDERLİK

Liderlik ve Bağlılık

Üst yönetim, bilgi güvenliği yönetim sistemi ile ilgili olarak liderlik ve bağlılığı şu şekilde göstermelidir:

a) Bilgi güvenliği politikasının ve bilgi güvenliği hedeflerinin oluşturulmasını ve kuruluşun stratejik yönü ile uyumlu olmasını sağlamak;

b) Bilgi Güvenliği Yönetim Sistemi gereksinimlerinin kuruluşun süreçlerine entegrasyonunu sağlamak;

c) Bilgi Güvenliği Yönetim Sistemi için ihtiyaç duyulan kaynakların mevcut olmasını sağlamak;

d) Etkin bilgi güvenliği yönetiminin ve bilgi güvenliği yönetim sistemi gerekliliklerine uyumun önemini iletmek;

e) Bilgi Güvenliği Yönetim Sistemi'nin amaçlanan sonuç(lar)a ulaşmasını sağlamak;

f) Bilgi Güvenliği Yönetim Sistemi'nin etkinliğine katkıda bulunmaları için kişileri yönlendirmek ve desteklemek;

g) Sürekli iyileştirmeyi teşvik etmek; ve

h) Sorumluluk alanlarına uygulandığı için liderliklerini göstermek amacıyla diğer ilgili yönetim rollerini desteklemek.

Politika

Üst yönetim, aşağıdakileri içeren bir bilgi güvenliği politikası oluşturmalıdır:

a) Kuruluşun amacına uygun;

b) Bilgi güvenliği hedeflerini içeren veya bilgi güvenliği hedeflerinin belirlenmesi için çerçeve sağlayan;

c) Bilgi güvenliği ile ilgili uygulanabilir gerekliliklerı yerine getirme taahhüdünü içeren;

d) Bilgi Güvenliği Yönetim Sisteminin sürekli iyileştirilmesi taahhüdünü içeren.

Bilgi güvenliği politikası yazılı doküman olarak mevcut olmalıdır. Bunun yanında kuruluş içinde iletişim kurularak, uygun şekilde ilgili taraflara açık bir şekilde oluşturulmalıdır.

Yönetimsel roller, sorumluluklar ve yetkiler

Üst yönetim, bilgi güvenliği ile ilgili rollere ilişkin sorumluluk ve yetkilerin kurum içinde atanmasını ve iletilmesini sağlamalıdır. Üst yönetim, aşağıdakiler için sorumluluk ve yetki verir:

a) Bilgi Güvenliği Yönetim Sistemi'nin 27001 standardının gerekliliklerine uygun olması;

b) Bilgi Güvenliği Yönetim Sistemi'nin performansının üst yönetime raporlanması.

Üst yönetim, kuruluş içinde bilgi güvenliği yönetim sisteminin performansının raporlanması için sorumlu ve yetkililer de atayabilir.

3. PLANLAMA

Riskleri ve fırsatları ele almak için yaptırımlar

Kuruluş, bilgi güvenliği yönetim sistemini planlarken, kapsamını ve ihtiyaçlarını göz önünde bulundurmalı ve ele alınması gereken riskleri ve fırsatları belirlemelidir:

a) Bilgi Güvenliği Yönetim Sisteminin amaçlanan sonuç(lar)ına ulaşabilmesini sağlamak;

b) İstenmeyen etkileri önlemek veya azaltmak;

c) Sürekli iyileştirme elde etmek.

Kuruluş şunları planlamalıdır:

a) Bu riskleri ve fırsatları ele almak için eylemler;

b) Eylemleri bilgi güvenliği yönetim sistemi süreçlerine entegre etmek ve uygulamak;

c) Bu eylemlerin etkinliğini değerlendirmek.

Bilgi güvenliği risk değerlendirmesi

Kuruluş, aşağıdakileri içeren bir bilgi güvenliği risk değerlendirme süreci tanımlamalı ve uygulamalıdır:

1) Aşağıdakileri içeren bilgi güvenliği risk kriterlerini belirler ve sürdürür:

a) Risk kabul kriterleri;

b) Bilgi güvenliği risk değerlendirmeleri gerçekleştirme kriterleri;

2) Tekrarlanan bilgi güvenliği risk değerlendirmelerinin tutarlı, geçerli ve karşılaştırılabilir sonuçlar üretmesini sağlar;

3) Bilgi güvenliği risklerini tanımlar:

a) Bilgi Güvenliği Yönetim Sistemi kapsamında bilginin gizlilik, bütünlük ve kullanılabilirlik kaybı ile ilişkili riskleri belirlemek için bilgi güvenliği risk değerlendirme sürecini uygulamasını;

b) Risk sahiplerini belirlemek;

4) Bilgi güvenliği risklerini analiz eder:

a) Tanımlanan bilgi güvenliği risklerinin gerçekleşmesi durumunda ortaya çıkabilecek olası sonuçları değerlendirmek;

b) Tanımlanan bilgi güvenliği risklerin gerçekçi bir şekilde ortaya çıkma olasılığını değerlendirmek;

c) Risk seviyelerini belirlemek;

5) Bilgi güvenliği risklerini değerlendirir:

a) Risk analizi sonuçlarını;

b) Analiz edilen risklerin giderilmesi için önceliklendirilme yapılması.

Kuruluş, bilgi güvenliği risk değerlendirme süreci hakkında yazılı belge halindeki bilgileri muhafaza etmelidir.

Bilgi güvenliği risklerinin giderilmesi

Kuruluş, aşağıdakiler için bir bilgi güvenliği risk işleme süreci tanımlamalı ve uygulamalıdır:

a) Risk değerlendirme sonuçlarını dikkate alarak uygun bilgi güvenliği risk giderme seçeneklerini seçmek;

b) Seçilen bilgi güvenliği risk işleme seçeneğini/seçeneklerini uygulamak için gerekli tüm kontrolleri belirlemek;

c) Gerekli kontrollerin ihmal edilmediğini doğrulamak;

d) Aşağıdakileri içeren bir Uygulanabilirlik Beyanı oluşturmak:

1) Gerekli kontroller;

2) Dahil edilmeleri için gerekçeler;

3) Gerekli kontrollerin uygulanıp uygulanmadığı;

4) Kontrollerinden herhangi birinin hariç tutulmasının gerekçesi.

e) Bir bilgi güvenliği risk giderme planı formüle etmek;

f) Risk sahiplerinin bilgi güvenliği risk giderme planının onayını ve kalan bilgi güvenliği risklerinin kabul edilmesini sağlamak.

Kuruluş, bilgi güvenliği riskinin ele alınma süreci hakkında yazılı belge haline getirilmiş bilgileri muhafaza etmelidir.

Güvenlik hedefleri ve planları

Kuruluş, ilgili fonksiyon ve seviyelerde bilgi güvenliği hedefleri oluşturmalıdır.

Bilgi güvenliği hedefleri:

a) Bilgi güvenliği politikası ile tutarlı olmalı;

b) Ölçülebilir olmalı (uygulanabilirse);

c) Uygulanabilir bilgi güvenliği gereksinimlerini ve risk değerlendirmesi ve risk giderme adımlarından elde edilen sonuçları dikkate almalı;

d) İzlenmeli;

e) İlgili paydaşlarla iletişim kurulmalı;

f) Uygun şekilde güncellenmeli;

g) Yazılı belge halinde mevcut olmalıdır.

Kuruluş, bilgi güvenliği hedefleri hakkında yazılı belgeleri muhafaza etmelidir. Kuruluş, bilgi güvenliği hedeflerine nasıl ulaşılacağını planlarken şunları belirlemelidir:

a) Ne yapılacak;

b) Hangi kaynaklara ihtiyaç duyulacak;

c) Kim sorumlu olacak;

d) Ne zaman tamamlanacak;

e) Sonuçlar nasıl değerlendirilecek.

Kuruluş, bilgi güvenliği yönetim sisteminde değişiklik yapılması gerektiğini belirlediğinde, değişiklikler de planlı bir şekilde gerçekleştirilmelidir.

4. DESTEK

Kuruluş, bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için ihtiyaç duyulan kaynakları belirlemeli ve sağlamalıdır. Bu amaçla kuruluş:

a) Kontrolü altında iş yapan kişinin/kişilerin bilgi güvenliği performansını etkileyen gerekli yeterliliklerini belirlemeli;

b) Bu kişilerin uygun eğitim, öğretim veya deneyim temelinde yetkin olmalarını sağlamalı;

c) Uygulanabilir olduğunda, gerekli yetkinliği elde etmek için önlemler almak ve alınan önlemlerin etkinliğini değerlendirmeli;

d) Yetkinlik kanıtı olarak uygun belgelenmiş bilgileri saklamalıdır.

Bu kısımda yapılabilecek uygulamalar arasında mevcut çalışanlara eğitim verilmesi, mentorluk yapılması veya yeniden atanması veya yetkili kişilerin işe alınması veya sözleşme yapılması sayılabilir. Kuruluşun kontrolü altında iş yapan kişilerin; Bilgi Güvenliği Politikasının, gelişmiş bilgi güvenliği performansının faydaları da dahil olmak üzere bilgi güvenliği yönetim sisteminin kuruluş etkinliğine katkılarının ve Bilgi Güvenliği Yönetim Sistemi gerekliliklerine uymamanın sonuçlarının farkında olmaları gerekmektedir. Bunun yanında kuruluş, bilgi güvenliği yönetim sistemi ile ilgili ne konuda, ne zaman, kiminle ve nasıl iletişim kurulacağına dair iç ve dış iletişim ihtiyacını da belirlemelidir.

Dokümantasyon

Kuruluşun bilgi güvenliği yönetim sistemi bu standardın gerektirdiği bilgileri yazılı olarak muhafaza etmeli ve Bilgi Güvenliği Yönetim Sistemi'nin etkinliği için gerekli olduğu belirlenen

her şeyi yazılı olarak belgelemelidir. Bir bilgi güvenliği yönetim sistemi için dokümante edilen bilgilerin kapsamı, aşağıdaki nedenlerden dolayı bir kuruluştan diğerine farklılık gösterebilir:

a) Organizasyonun büyüklüğü ve faaliyetleri, süreçleri, ürünleri ve hizmetleri;

b) Süreçlerin karmaşıklığı ve etkileşimleri;

c) Kişilerin yeterliliği.

Yazılı bilgileri oluştururken ve güncellerken, kuruluş kendi sistemine uygun bir şekilde aşağıdaki özellikleri kullanmalıdır:

a) Kimlik ve açıklama (örn. başlık, tarih, yazar veya referans numarası);

b) Biçim (ör. dil, yazılım sürümü, grafikler) ve ortam (ör. kağıt, elektronik);

c) Uygunluk ve yeterlilik için gözden geçirme ve onaylama.

Bilgi güvenliği yönetim sistemi ve bu doküman tarafından gerekli görülen dokümante edilmiş bilgilerin, ihtiyaç duyulan yerde/zamanda kullanıma hazır olması ve uygunluğu ile yeterince korunup kurunmadığı (örn. gizlilik kaybından, uygunsuz kullanımdan veya bütünlük kaybından) kontrol edilmelidir.

Dokümante edilmiş bilgilerin kontrolü için, kuruluş, uygun olduğu şekilde, aşağıdaki faaliyetleri ele almalıdır:

a) Dağıtım, erişim, erişim ve kullanım;

b) Okunabilirliğin korunması da dahil olmak üzere saklama ve koruma;

c) Değişikliklerin kontrolü (örn. sürüm kontrolü);

d) Alıkoyma ve elden çıkarma.

Bilgi güvenliği yönetim sisteminin planlanması ve işletilmesi için gerekli olduğu kuruluş tarafından belirlenen dokümante edilmiş dış kaynaklı bilgiler, uygun olarak tanımlanmalı ve kontrol edilmelidir. Erişim, yalnızca belgelenmiş bilgileri görüntüleme izni veya belgelenmiş bilgileri görüntüleme ve değiştirme izni ve yetkisi vb. ile ilgili bir karar anlamına da gelebilir.

5. İŞLETİM

Kuruluş, gereksinimleri karşılamak için gerekli süreçleri planlamalı, uygulamalı ve kontrol etmeli ve Planlama başlığında belirlenen eylemleri uygulamak için gerekli kriterleri belirlemeli ve kriterlere uygun olarak süreçlerin kontrolünü sağlamalıdır. Kuruluş, planlanan değişiklikleri kontrol etmeli ve istenmeyen değişikliklerin sonuçlarını gözden geçirmeli, gerektiğinde olumsuz etkileri azaltmak için harekete geçmelidir. Kuruluş, bilgi güvenliği yönetim sistemi ile ilgili olarak dışarıdan sağlanan süreçlerin, ürünlerin veya hizmetlerin kontrol edilmesini de sağlamalıdır.

Kuruluş, planlama adımındaki risk değerlendirmesinde belirlenen kriterleri dikkate alarak, planlanan aralıklarla veya önemli değişiklikler önerildiğinde/meydana geldiğinde bilgi güvenliği risk değerlendirmeleri yapmalıdır. Kuruluş, bilgi güvenliği risk değerlendirmelerinin sonuçlarına ilişkin dokümante edilmiş bilgileri muhafaza etmelidir.

Kuruluş, bilgi güvenliği risk giderme planını uygulamalıdır. Kuruluş, bilgi güvenliği risk giderme işlemlerinin sonuçlarına ilişkin belgelenmiş bilgileri muhafaza etmelidir.

6. PERFORMANS DEĞERLENDİRME

Kuruluş izleme, ölçme, analiz ve değerlendirme amacıyla şunları belirlemelidir:

a) Bilgi güvenliği süreçleri ve kontrolleri de dahil olmak üzere izlenmesi ve ölçülmesi gerekenler;

b) Geçerli sonuçları sağlamak için uygun olduğu şekilde izleme, ölçme, analiz ve değerlendirme yöntemleri. Seçilen yöntemlerin geçerli sayılabilmesi için karşılaştırılabilir ve tekrarlanabilir sonuçlar üretmesi gerekir;

c) İzleme ve ölçmenin ne zaman yapılacağı;

d) Kimin izleyip ölçeceği;

e) İzleme ve ölçme sonuçlarının analiz ve değerlendirmeye tabi tutulacağı zaman;

f) Sonuçların analiz edilmesi ve değerlendirilmesi.

Dokümante edilmiş bilgiler, sonuçların kanıtı olarak tutulmalıdır. Kuruluş, bilgi güvenliği performansını ve bilgi güvenliği yönetim sisteminin etkinliğini de değerlendirmelidir.

İç denetim

Kuruluş, bilgi güvenliği yönetim sisteminin aşağıdakileri yapıp yapmadığı konusunda bilgi sağlamak için planlanan aralıklarla iç denetimler yapmalıdır:

a) Gereksinimlere uygunluk

1) Kuruluşun bilgi güvenliği yönetim sistemi için kendi gereksinimleri;

2) Bu standardın gereklilikleri;

b) Etkin bir şekilde uygulanıyor ve sürdürülüyor mu.

Kuruluş, sıklığı, yöntemleri, sorumlulukları, planlama gereklilikleri ve raporlama dahil olmak üzere bir denetim programı planlamalı, oluşturmalı, uygulamalı ve sürdürmelidir. Kuruluş, iç denetim program(lar)ını oluştururken, ilgili süreçlerin önemini ve önceki denetimlerin sonuçlarını göz önünde bulundurmalıdır. Kuruluş:

a) her denetim için denetim kriterlerini ve kapsamını tanımlamalı;

b) denetçileri seçmeli ve denetim sürecinin tarafsızlığını ve tarafsızlığını sağlayan denetimler yapmalı;

c) Denetim sonuçlarının ilgili yönetime raporlanmasını sağlamalıdır.

Belgelendirilmiş bilgiler, denetim program(lar)ının ve denetim sonuçlarının uygulandığına dair kanıt olarak sunulmalıdır.

Yönetimin Değerlendirmesi

Üst yönetim, kuruluşun bilgi güvenliği yönetim sistemini, uygunluğunun, yeterliliğinin ve etkinliğinin sürekliliğini sağlamak için planlı aralıklarla değerlendirme yapar. Yönetimin değerlendirmesi aşağıdakilerin dikkate alınmasını içermelidir:

a) Önceki yönetim incelemelerinden elde edilen eylemlerin durumu;

b) Bilgi güvenliği yönetim sistemi ile ilgili dış ve iç konulardaki değişiklikler;

c) Bilgi Güvenliği Yönetim Sistemi ile ilgili ilgili tarafların ihtiyaç ve beklentilerindeki değişiklikler;

d) Eğilimler de dahil olmak üzere bilgi güvenliği performansı hakkında geri bildirim:

1) Uygunsuzluklar ve düzeltici faaliyetler;

2) İzleme ve ölçüm sonuçları;

3) Denetim sonuçları;

4) Bilgi güvenliği hedeflerinin yerine getirilmesi;

e) İlgili taraflardan geri bildirim;

f) Risk değerlendirme sonuçları ve risk tedavi planının durumu;

g) Sürekli iyileştirme fırsatları.

Yönetimin değerlendirme sonuçları, sürekli iyileştirme fırsatları ve bilgi güvenliği yönetim sisteminde herhangi bir değişiklik ihtiyacı ile ilgili kararları içermelidir. Dokümante edilmiş bilgiler, yönetimin değerlendirme sonuçlarının kanıtı olarak sunulmalıdır.

7. GELİŞTİRME

Kuruluş, bilgi güvenliği yönetim sisteminin uygunluğunu, yeterliliğini ve etkinliğini sürekli iyileştirmelidir. Bir uygunsuzluk meydana geldiğinde, kuruluş uygunsuzluğa tepki vermeli ve bu uygunsuzluğu gidermek için gerekli kontrolleri yapmalı, düzeltmek için harekete geçmeli ve ortaya çıkan sonuçlarla başa çıkabilmelidir. Uygunsuzluğun nedenlerini ortadan kaldırmak için harekete geçerken, başka bir yerde tekrarlanmaması veya ortaya çıkmaması için uygunsuzluk gözden geçirilmeli, nedenleri belirlenmeli ve benzer uygunsuzlukların mevcut olup olmadığı veya potansiyel olarak ortaya çıkıp çıkamayacağı belirlenmelidir.

Bunun yanında gerekli herhangi bir eylemi uygulamaktan geri durulmamalı, alınan herhangi bir düzeltici faaliyetin etkinliğini gözden geçirmeli ve gerekirse bilgi güvenliği yönetim sisteminde değişiklikler yapılmalıdır. Düzeltici faaliyetler, karşılaşılan uygunsuzlukların etkilerine uygun olacaktır. Yapılan işlemlere dair belgelenmiş bilgiler uygunsuzlukların niteliği ve daha sonra alınan önlemler ile herhangi bir düzeltici eylemin sonuçlarının kanıtı olarak sunulmalıdır.

BÖLÜM ÖZETİ

Bilgi Güvenliği Yönetim Sistemi (BGYS), kuruluşların bilgi güvenliğini sağlamak için ISO/IEC 27001 standardına dayanan bir çerçevedir. BGYS, bir bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için gereklilikleri belirler.

BGYS, bir kuruluşun iç ve dış bağlamlarını, ilgili taraflarını ve bilgi güvenliği risklerini belirleyerek başlar. Üst yönetim, BGYS ile ilgili liderlik ve bağlılığını göstererek politikaların oluşturulması, kaynak sağlanması ve sürekli iyileştirmeyi teşvik etme sorumluluğunu üstlenir. Bilgi güvenliği politikalarının oluşturulması ve sürdürülmesi, yönetim tarafından yürütülmelidir. Ayrıca, bilgi güvenliği ile ilgili rollerin ve sorumlulukların atanması ve iletilmesi gerekmektedir.

Planlama aşamasında, bilgi güvenliği risklerinin belirlenmesi, analizi ve değerlendirilmesi yapılır. Belirlenen risklere yönelik uygun önlemler seçilir ve uygulanır. Bilgi güvenliği hedefleri belirlenerek bu hedeflere ulaşmak için planlar oluşturulur.

BGYS'nin destek mekanizmaları arasında dokümantasyon süreci yer alır. Gereklilikler belgelendirilmeli ve dokümantasyon kontrol edilmelidir. Ayrıca, çalışanların bilgi güvenliği performansını artırmak amacıyla gerekli eğitim ve farkındalık çalışmaları sağlanmalıdır.

İşletim aşamasında, bilgi güvenliği süreçleri ve kontrolleri izlenmeli, ölçülmeli, analiz edilmeli ve değerlendirilmelidir. Planlanan aralıklarla iç denetimler gerçekleştirilerek sonuçları raporlanmalıdır.

Performans değerlendirmesi kapsamında, üst yönetim tarafından BGYS'nin uygunluğu, yeterliliği ve etkinliği değerlendirilmelidir. Bu değerlendirme, sürekli iyileştirme fırsatlarını belirlemek açısından önemlidir.

Geliştirme sürecinde, BGYS'nin sürekli iyileştirilmesi için kuruluş tarafından belirlenen fırsatlar uygulanmalıdır. BGYS'nin temel amacı, kuruluşların bilgi varlıklarını korumasını sağlamak ve bu alanda sürekli iyileştirmeler yapmasına rehberlik etmektir. Kuruluşların bu unsurları nasıl uygulayacağı, büyüklüklerine, yapılarına ve faaliyet gösterdikleri sektöre bağlı olarak değişiklik gösterebilir.

GÖZDEN GEÇİRELİM

1. **Bilgi Güvenliği Yönetim Sistemi (BGYS) nedir?**
   a) Bir kuruluşun bilgi güvenliğini sağlamak için rehberlik eden bir çerçeve
   b) Bir bilgisayar güvenlik yazılımı
   c) Bir ağ güvenlik protokolü
   d) Bir şifreleme algoritması
   e) Bir veri tabanı yönetim sistemi

2. **ISO/IEC 27001 standardı neyi açıklar?**
   a) Bilgi güvenliği politikalarının oluşturulması
   b) Bir bilgi güvenliği yönetim sistemi kurma, uygulama, sürdürme ve sürekli iyileştirme için gereklilikleri
   c) Risk değerlendirme süreçleri
   d) Bilgi güvenliği hedeflerinin belirlenmesi
   e) Bilgi güvenliği risklerinin giderilmesi

3. **BGYS'nin temel amacı nedir?**
   a) Veri tabanlarını yönetmek
   b) Ağ güvenliğini sağlamak
   c) Bir kuruluşun bilgi varlıklarını korumasını ve bu alanda sürekli iyileştirmeler yapmasını sağlamak
   d) Kullanıcı kimlik doğrulaması yapmak
   e) İnternet trafiğini izlemek

4. **BGYS'nin kuruluşun hangi yönlerini dikkate alması beklenir?**
   a) Yalnızca teknolojik yönler
   b) Yalnızca finansal yönler
   c) İç ve dış bağlamlar, ilgili taraflar ve bilgi güvenliği riskleri
   d) Yalnızca yasal yönler
   e) Yalnızca operasyonel yönler

5. **Bilgi güvenliği yönetim sistemi kapsamında, bilginin gizliliği, bütünlüğü ve kullanılabilirliği ile ilişkili riskler nasıl belirlenir ve değerlendirilir?**

6. **Bilgi güvenliği yönetim sisteminin sürekli iyileştirilmesi için hangi adımlar izlenmelidir ve bu süreçte liderliğin rolü nedir?**

Yanıt Anahtarı: 1-A, 2-B, 3-C, 4-C

Kaynakça

ISO. (2023, 8). Retrieved from https://www.iso.org/standard/27001

ISO. (2023, 9). Retrieved from https://www.iso.org/standard/65694.html

BÖLÜM 8

BİLİŞİM HUKUKU VE KİŞİSEL VERİLERİN KORUNMASI

ANAHTAR KAVRAMLAR

Bilişim Sistemleri, Kişisel Veri, Bilişim Suç ve Cezaları, Kişisel Verilerin Korunması, Kişisel Veri Suç ve Cezaları

ÖĞRENME HEDEFLERİ

1. Kişisel verilerin işlenmesinde veri sorumluları

2. Veri sorumlularının yükümlülükleri

3. Kişisel verilerin hukuka aykırı şekilde işlenmesi halinde mevzuatın düzenlediği idari yaptırımların öğrenilmesi hedeflenmiştir.

4. Bilişim ve bilişim sistemi kavramlarının mevzuatımızda tanımı ile bilişim hukukunun, hukuk dalları arasındaki yeri

5. Bilişim hukukunun kapsadığı alan ve faaliyetler, bilişim hukukunun kapsamı.

SEKİZİNCİ BÖLÜM

GİRİŞ

Bir canlı türü olarak insanın binlerce yıldır süren tarihsel gelişimi ve değişiminde ateşin, yazının, sayma sisteminin, takvimin, tekerleğin ve daha birçok keşfin önemli yeri vardır. Tarımsal üretimin keşfi, avcı-toplayıcılıktan yerleşik hayata geçişe, dolayısıyla insanların toplu olarak bir arada yaşamaya başlamasına yol açmıştır. Yerleşik olarak bir arada yaşamaya başlayan insanlar arasında yeni ilişkiler ve anlaşmazlıklar doğmuş, daha önce var olmayan ve günümüzde insanın insan olmaktan doğan temel haklarına yenileri eklenmiştir. Yine insanlar arasında işbölümü zamanla yaygınlaşmış, bir arada yaşayan insanların oluşturduğu toplumda bireyler ve topluluklar arasındaki ilişkilerin, mülkiyete dayalı üretim ilişkilerinin, iktidar (devlet/ yöneten) ile yönetilen arasındaki ilişkinin ve toplum düzeninin korunmasına ihtiyaç duyulmuştur. Hukuk düzeni bu ihtiyaçlardan ortaya çıkmış ve insanlığın gelişimine paralel olarak gelişen dinamik bir alan olarak varlığını sürdürmektedir.

İnternet ve bilişim sistemlerinin kamusal ve özel alanda yaygınlaşarak, çok çeşitli biçimdeki kullanım alanı dolayısıyla, bu alanda ortaya çıkacak hukuka aykırılıkların önüne geçecek hukuki düzenlemeler yapılmasına ihtiyaç duyulmuştur. Bu nedenle, bilişim sistemlerinin kendi güvenliğine yönelik olarak ve bilişim sistemlerinin araç olarak kötüye kullanılması yoluyla işlenebilecek suçlara yönelik düzenlemeler yapılmıştır. Bununla birlikte yine bilişim ve ağ sistemleri yoluyla elde edilen, saklanan, iletilen kişisel verilerin de korunmasına yönelik veri sorumlularının uyması gereken kurallar düzenlenmiştir. Diğer yandan elektronik ortamda ticarete ilişkin olarak düzenlemeler yapılmış, yine elektronik ortamda üretilen veya kullanılan fikir ve sanat eserlerine ilişkin olarak düzenlemeler yapılmıştır.

1. BİLİŞİM HUKUKUNUN KAPSAMI

Teknolojideki gelişmelerle bilgi elektronik ortama taşınmıştır. Bununla birlikte iletişim, ekonomik faaliyetler, devletin bireyle olan ilişkilerindeki bürokratik faaliyetler de elektronik ortamda sürdürülmeye başlanmıştır. İnsanlık tarihinde tarım devrimi ve sanayi devriminden sonra mikroelektroniğin ve iletişim olanaklarının artan gelişme hızıyla ivme kazanan, bilgisayar gücünün evlerimizde gündelik yaşamamıza değin girmesiyle, bilişim toplumu olarak adlandırılan yeni bir yaşam ve toplum düzeni ortaya çıkmıştır (KÖKSAL, 2003). Bilişim teriminin birçok tanımı yapılmaktadır. Bilişim, elektronik sistemlerin tamamını içeren bir üst terimdir. Bilişim, kısaca, bilgi ve teknolojinin birlikte kullanılarak üretilen sonuçlar olarak tarif edilebilir. Ya da daha geniş ve farklı olarak; teknik, ekonomik ve toplumsal alanlardaki iletişimde kullanılan ve özellikle elektronik aletler aracılığıyla düzenli bir biçimde işlenmeyi öngören bir bilimdir. Bir diğer tabirle, her türlü bilgi ve verinin elektronik bilgi işlem araçlarıyla işlenmesini ve değerlendirme tekniklerini konu alan bilim şeklinde de tanımlanabilmektedir (Bilgi Tekonojileri ve İletişim Kurumu, 2019).

Bir başka tanıma göre bilişim; insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimidir (Türk Dil Kurumu , 2023) .

Bu tanımlardan yola çıkarak, bilişimin elektronik makineler aracılığıyla ekonomik ve toplumsal alanda iletişimle ve bilginin işlenmesiyle ilgili bilim dalı olarak kabul edildiği söylenebilir. Bilişimi sağlayan her türlü elektronik araç, bilişim aracı olarak kabul edilir.

Yürürlükteki kanunlarda bilişim kavramına rastlamış değiliz. Buna karşın bilişim sistemi kanunda olmasa da ikincil mevzuat niteliğinde olan yönetmelikte tanımlanmış durumdadır. Bunun anlamı, bilişim sistemine yönelik veya bilişim sisteminin araç olarak kullanılması yoluyla işlenebilecek suçlarda, bilişim sisteminden ne anlaşılması gerektiğini göstermektedir. Bu anlamda bilişim sistemi kavramı mevzuatta tanımlanmış durumdadır. Bu tanıma göre "bilişim sistemi"; bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistemdir (Ceza Muhakemesinde Ses Ve Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmelik, 2011).

Kitabın bu bölümünde bilişim sistemi kavramı dijital ortamı kapsayan tüm unsurları kapsayacak şekilde kullanılacaktır. Bilişim hukuku terimi de esasen bilişimin tüm unsurlarını içeren genel bir kavramdır. Böylece okuyucu için daha anlaşılır bir şekilde konu aktarılmaya çalışılacaktır.

Bilişim hukuku terimi önceleri bilişim suç ve cezalarıyla sınırlı olarak, kamu hukukunun alt dalı olan ceza hukukunun bir dalı olarak görünmekteydi. Sonradan elektronik ticaret, elektronik imza, elektronik haberleşme, elektronik paralar, yapay zekâ gibi konular da bilişim hukukunun alt başlıkları olarak incelenmeye başlanmış ve özel hukuk dalı olarak konumlanmıştır. Artık günümüzde bilgisayar, cep telefonları, internet yayıncılığı, sosyal medya, elektronik ticaret, elektronik haberleşme, elektronik imza, yapay zekâ, elektronik paralar ve bilişim suçları başta olmak üzere, bilişim sistemleri aracılığıyla yürütülen her türlü legal ve illegal faaliyet bilişim hukukunun konusunu oluşturmaktadır (EKİCİ, 2023).

2. KİŞİSEL VERİLER HUKUKU

Veri, bir araştırmanın, bir tartışmanın, bir muhakemenin temeli olan ana öge; muta (I), data, done olarak tanımlanmaktadır (Türk Dil Kurumu , 2023). Veri sözcüğünün içerdiği en önemli özellik, bir bilgi içeriyor olmasıdır (EKİCİ, 2023). Bilişim hukuku açısından ise veri; bilişim sistemlerinin üzerinde işlem yapabildiği, bu işlemlere dayalı sonuçlar üretebildiği, saklayabildiği, sakladıklarını sonradan tekrar okuyup işleyebildiği ve diğer bilişim sistemlerine iletebildiği her türlü bilgi olarak tanımlanabilir (DÜLGER, 2023). Bilişim hukuku açısından veri olarak kabul edilecek bilgilerin bilişim sistemleri tarafından bir işleme tabi tutulabilir olması, ondan sonuç çıkarılabilir olması ve saklanabilir olması gerekmektedir (EKİCİ, 2023).

Bilişim hukuku kapsamında son yıllarda "kişisel veri" ve büyük veri" veri hukukunun önemli kısımları olmuştur (EKİCİ, 2023). Büyük veri, geleneksel ya da klasik veri işleme yöntemleri ile değerlendirilemeyecek kadar çok büyük hacimli, oldukça kompleks, hızlı değişebilen ve çok zayıf yapılandırılmış büyük miktardaki veriyi ifade etmektedir (TURAN, 2023, s. 295).

Kişisel Verilerin Korunması

Kişisel veri normlar hiyerarşisine göre en üst norm olan ve ülkemizin de taraf olduğu İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme (Avrupa İnsan Hakları Sözleşmesi)'nin 8. Maddesi ile koruma altına alınmıştır. Bu maddeye göre;

Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir. " (İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme, 1950)

Bu düzenleme uyarınca kişisel veriler, özel hayata saygı hakkı kapsamında sayılmaktadır. Bu nedenle de temel insan hakları arasındadır.

Kişisel veriler, 1982 Anayasasının 20'nci maddesinin 3'üncü fıkrası ile "*Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir*" hükmü ile koruma altına alınmıştır. Anayasanın bu düzenlemesi uyarınca 2016 yılında Kişisel Verilerin Korunması Kanunu (KVKK) TBMM'de kabul edilmiş ve Resmî Gazetede yayınlanarak yürürlüğe girmiştir.

Kişisel veri kavramı, bizzat kanun koyucu tarafından 6698 sayılı KVKK'nun 3'üncü maddesinin 1'inci fıkrasının (d) bendinde; *kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi* olarak tanımlanmıştır. (6698 Sayılı Kişisel Verilerin Korunması Kanunu , 2016) Bu tanım uyarınca, bilginin kişisel veri sayılabilmesi için gereken ilk koşul, bir bilginin gerçek kişiye ait olmasıdır. Bu nedenle tüzel kişilere ait bilgiler KVKK anlamında kişisel veri sayılmayacaktır. Kanuni tanımından yola çıkılarak bilginin kişisel veri sayılması için aranan diğer koşul, bilginin; kimliği belirli veya belirlenebilir bir gerçek kişiye ait olmasıdır. İkinci unsur, kimliği belirli veya belirlenebilir olmadıkça, yani anonim hale getirildiğinde, bu bilginin kişisel veri olmadığı anlamını taşımaktadır. Anonim hale getirme yine kanun tarafından tanımlanmıştır. Buna göre, kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette

kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi, kişisel verilerin anonim hale getirilmesidir (6698 Sayılı Kişisel Verilerin Korunması Kanunu , 2016).

Bir bilginin kişisel veri olabilmesi ve KVKK kapsamında sayılması için gereken ilk koşul olan bilginin bir gerçek kişiye ait olması unsuru, gerçek kişinin hukuki tanımının aktarılmasını da zorunlu kılmaktadır. Kişiler hukuku, Türk Medeni Kanunu'nda düzenlenmiştir (Türk Medeni Kanunu , 2001). Kanun'un 28. Maddesine göre; kişilik, çocuğun sağ olarak tamamıyla doğduğu anda başlar ve ölümle sona erer. Çocuk hak ehliyetini, sağ doğmak koşuluyla, ana rahmine düştüğü andan başlayarak elde eder. Hak ehliyeti kavramı da yine aynı kanunda, haklara ve borçlara sahip olmak olarak tanımlanmıştır. Bu nedenle, çocuğun sağ olarak tamamıyla doğma koşulu gerçekleştiğinde, kişisel verinin çocuğun ana rahmine düştüğü andan itibaren koruma altında olduğu söylenebilir. Böylece bir bilginin kişisel veri olarak KVKK'nun kapsamında olması, çocuğun ana rahmine düştüğü andan itibaren başlayarak, kişiliğin sona erdiği ölümle sona erer.

Kişisel Verilerin Korunması Kanunu ile, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere, kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek amaçlanmıştır (6698 Sayılı Kişisel Verilerin Korunması Kanunu , 2016). Kişisel verilerin korunmasının mahremiyetten daha geniş bir anlamı ve koruma alanı olduğu söylenmektedir. Buna göre, verilerin korunması ile mahremiyetin, yani özel hayatın gizliliğinin yanında, ifade özgürlüğü, din ve vicdan özgürlüğü, bilginin serbest akımı, birey özgürlüğü, kendi kaderini tayin etme gibi hakların da korunduğu belirtilmektedir (TURAN, Karşılaştırmalı Hukukta Kişisel Verilerin Korunması, 2021). Bu haklar, tıpkı özel hayatın gizliliği hakkı gibi, temel insan hakları arasındadır. Bu nedenle, kişisel verilerin korunması, sadece bireyin özel hayatının gizliliği hakkını değil, bundan daha geniş olarak ifade özgürlüğü başta olmak üzere bazı başka temel hakların korunmasını da sağlar.

Bu açıklamalardan sonra KVKK'nun amaçları kısaca;

• Kişisel verilerin işlenmesinde, kişilerin temel hak ve özgürlüklerini korumak,

• Kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek (disiplin altına almak),

• Kişilerin mahremiyetini korumak (özel hayatın gizliliği),

• Kişisel veri güvenliğini sağlamak olarak sayılabilir (Kişisel Verileri Koruma Kurumu, 2019).

Kanunun kapsamında ise, verileri işlenen gerçek kişiler ile verileri işleyenler bulunmaktadır. Kanunda tüzel kişilere ait verilerin kişisel veri olarak kabul edilmediğine bir kez daha vurgu yapmak gerekir. Verileri işleyenler ise ya gerçek kişilerdir ya da tüzel kişilerdir. Veri Verilerin işlenmesi otomatik olabileceği gibi, veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yolla işleyen tüzel kişiler bulunmaktadır. Veri kayıt sistemi Kanunda, *kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi* olarak tanımlanmıştır. Bu bakımdan, verilerin kurumsal ve kişisel veri olarak sınıflandırıldığında, kanunun kişisel verilerin korunmasına yönelik düzenlemeler içerdiği söylenebilir. Ancak, kurumlar nezdinde bulunan kişisel verilerin de olduğu tüm veriler, kurumlar açısından kurumsal veri olarak nitelendirilmekte olduğundan, kurumsal verilerin de kişisel veriler gibi korunması kurumsal yapılar açısından önem taşımaktadır (TURAN, Karşılaştırmalı Hukukta Kişisel Verilerin Korunması, 2021).

Verilerin kurumsal veri/kişisel veri olarak sınıflandırılmasının yanında, kişisel veriler de kendi içinde kişisel veriler/ özel nitelikli kişisel veriler olarak sınıflandırılabilir. Bu ayrıma göre,

bazı kişisel veriler, diğerlerine göre daha özel niteliktedir ve farklı bir koruma ihtiyacı içindedir. Kanun da kişisel veriler içinde bazı verileri özel nitelikli kişisel veri sayarak, bu verilerin işlenmesini diğerlerine göre başka koşullara tabi tutmuştur. KVKK'nun 6'ncı maddesinin 1'inci fıkrasında kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veri olarak sayılmıştır.

Kanun, kişisel verilerin KVKK ya da başka kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceğini düzenlemiştir. Bu anlamda kişisel verilerin işlenmesi; "kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem" olarak tanımlanmıştır (6698 Sayılı Kişisel Verilerin Korunması Kanunu , 2016). Bu tanımdan yol çıkarak, kişisel verilerin işlenmesinin, bir kişisel veriyi elde etmekle başlayıp bu veri üzerindeki her türlü işlemi kapsadığı söylenebilir. Bu nedenle, kişisel verilerin elde edilmesinde mevzuatın aradığı yükümlülükleri yerine getirmek, veri işleyenin sorumluluğunu sona erdirmez. Veri elde edildiği andan itibaren üzerinde gerçekleşen her türlü işlemde de KVKK'nun düzenlediği şartların gerçekleşmesi sağlanmalıdır.

Kişisel verilerin hangi şartlarda işlenebileceği ve kişisel verilerin işlenmesine ilişkin genel ilkeler de yine KVKK tarafından düzenlenmiştir. Buna göre, genel kural olarak kişisel verilerin ilgili kişilerin açık rızası olmadan işlenemeyeceği düzenlenmiştir. Kanun, açık rızayı *belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza* olarak tanımlamıştır (6698 Sayılı Kişisel Verilerin Korunması Kanunu , 2016). Açık rıza, 6698 sayılı Kanun'da hem özel nitelikli kişisel veriler hem de özel nitelikli olmayan kişisel veriler bakımından hukuka uygunluk sebebi olarak öngörülmüştür (https://www.kvkk.gov.tr/). Kanunda ayrıca, kişisel verilerin ilgili kişinin açık rızası olmadan işlenemeyeceği ve aktarılamayacağı, özel nitelikli kişisel verilerin ilgili kişinin açık rızası olmadan işlenemeyeceği düzenlenmiştir. Açık rıza; ilgili kişinin kendisiyle ilgili veri işlenmesine, özgürce, konuyla ilgili yeterli bilgi sahibi olarak, tereddüde yer bırakmayacak açıklıkta ve sadece o işlemle sınırlı olarak verdiği onay beyanı şeklinde anlaşılmalıdır. Açık rızanın yazılı olarak alınması şart olmayıp elektronik ortamda alınması da mümkündür (https://www.kvkk.gov.tr/).

Kişisel verilerin işlenmesinde ilgili kişinin açık rızasının aranmayacağı istisnalar da düzenlenmiştir. Buna göre;

a) Kanunlarda açıkça öngörülmesi,

b) Fiili imkânsızlık/rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması zorunluluğu,

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,

d) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,

e) İlgili kişinin kendisi tarafından alenileştirilmiş olması,

f) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,

g) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun

meşru menfaatleri için veri işlenmesinin zorunlu olması,

durumlarından her biri için ilgili kişinin açık rızası olmadan kişisel verilerin işlenmesi mümkündür. Bu istisnalar dışında ise, kişisel verilerin işlenmesinde ilgili kişinin açık rızasının alınması zorunludur.

Özel nitelikli kişisel verilerin işlenmesinde açık rıza aranmayacak durumlar ise şunlardır: Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Kanunlarda öngörülen haller dışında, yine bu veriler de açık rıza olmaksızın işlenemez.

Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir (6698 Sayılı Kişisel Verilerin Korunması Kanunu , 2016).

Özel nitelikli kişisel verilerin işlenmesiyle ilgili olarak kanun, Kişisel Verileri Koruma Kurulu (Kurul) tarafından belirlenen önlemlerin alınması şartını düzenlemiştir. Kurul'un 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı ile özel nitelikli kişisel verilerin işlenmesinde verileri işleyen veri sorumlusuna ek yükümlülükler getirmiştir. Bu yükümlülükler arasında özel nitelikli kişisel verilerin işlendiği elektronik ortamların;

a) Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi,

b) Kriptografik anahtarların güvenli ve farklı ortamlarda tutulması,

c) Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak loglanması,

d) Verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,

e) Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,

f) Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin sağlanması gerekmektedir.

Kişisel Verileri Koruma Kurumu tarafından tüm kişisel verilere yönelik olarak ayrıca, Kişisel Veri Güvenliği Rehberinde kişisel verilerin korunmasına yönelik alınması gereken idari ve teknik önlemler yer almaktadır (https://www.kvkk.gov.tr/).

KVKK'nda kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi veri sorumlusu olarak tanımlanmıştır. Veri sorumlusu, kişisel verilerin işlenme amaç ve araçlarını belirleyen gerçek ya da tüzel kişidir. Bunun dışında Kanun'un öngördüğü veri kayıt sisteminin kurulması ve yönetilmesi sorumluluğu da veri sorumlusuna aittir.

Kişisel veriler; ancak açık ve meşru amaçlar için, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olarak, işlendikleri amaç için gerekli olan süre kadar muhafaza edilmek şartlarıyla, hukuka ve dürüstlük kuralına uygun olarak, doğru ve gerektiğinde güncel olarak işlenebilir. Bu ilkeler, kişisel verilerin işlenebilmesinde veri sorumluların uyması gereken ilkelerdir.

Kanun tarafından gerçek kişilere, veri sorumlusuna karşı bazı başvuru hakları tanınmıştır.

Buna göre ilgili kişi kişisel verisinin işlenip işlenmediğini öğrenme, işlenmişse buna ilişkin bilgi talep etme hakkına sahiptir. Bunun dışında ilgili kişi, veri sorumlusuna kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, yurt içi ve yurt dışında kişisel verilerinin aktarıldığı üçüncü kişileri öğrenme, kişisel verileri yanlış veya eksik işlenmiş ise bunların düzeltilmesini isteme haklarına sahiptir.

İlgili kişi, KVKK'na uygun olarak kişisel verilerinin işlenmiş olması halinde dahi, işlenmesini gerektiren sebeplerin ortadan kalkması halinde veri sorumlusuna işlenen kişisel verilerinin silinmesi, yok edilmesi ya da anonim hale getirilmesi için başvuruda bulunma hakkına sahiptir. İşlenme sebepleri ortadan kalktığında, verileri işleyen veri sorumlusu da herhangi bir talep beklemeksizin bu verileri silmeli, yok etmeli ya da anonim hale getirmelidir (6698 Sayılı Kişisel Verilerin Korunması Kanunu , 2016).

3. VERİ SORUMLULARININ YÜKÜMLÜLÜKLERİ VE İDARİ YAPTIRIMLAR

Kişisel verilerin korunmasıyla ilgili kanuni düzenleme olan 6098 sayılı Kanun, ilgili kişisel verilerin elde edilmesiyle başlayan verilerin işlenmesi sürecine yönelik kuralları düzenlediği gibi, verilerin muhafazasını, işlenme amacı ortadan kalktığında silinme, yok edilme ya da anonim hale getirilmesini, ilgili kişisel verinin doğru ve güncel bilgiler içermemesi halinde bunların düzeltilmesine yönelik kuralları da koymuştur. Bu anlamda, veri sorumlusuna yönelik olarak öngörülen yükümlülüklerin ihlali halinde bazı idari para cezaları da düzenlemiştir.

Kabahat kavramı, 5326 sayılı 30.03.2005 tarihli Kabahatler Kanunu'nun 2'nci maddesinde; *kanunun, karşılığında idarî yaptırım uygulanmasını öngördüğü haksızlık* şeklinde tanımlanmıştır. Bu tanıma göre KVKK'nda aykırılıklar ve karşılığında idari para cezaları düzenlenmiştir. Bu nedenle, özellikle Türk Ceza Kanunu'nda düzenlenen bilişim suç ve cezalarına ilişkin bilişim suçlarından ayrı olarak, KVKK'na aykırılıklar kabahat şeklinde düzenlenmiştir. KVKK'nun ihlali bu anlamda kabahat fiilini oluştururken, kabahatin cezalandırılması ise idari para cezaları şeklinde düzenlenmiştir.

KVKK'nun 10'uncu maddesine göre veri sorumlusu ya da yetkilendirdiği kişi tarafından, kişisel verileri işlenecek olan ilgili kişiye, kişisel verilerin elde edilmesi sırasında veri sorumlusunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, kimlere hangi amaçla işlenen kişisel verilerin aktarılabileceği, kişisel verilerin hangi yolla toplanacağı ve kişisel verilerin işlenmesinin hukuki sebebini ve ilgili kişinin veri sorumlusuna başvurma hakkı olduğu konusunda aydınlatılması gerekmektedir. Söz konusu aydınlatma yükümlülüğünü yerine getirmeyen veri sorumlusu hakkında idari para cezası uygulanır.

Her şeyden önce veri sorumlusu, kişisel verilerin hukuka aykırı olarak işlenmesini önlemekle yükümlü tutulmuştur (6698 Sayılı Kişisel Verilerin Korunması Kanunu , 2016). Kanun, kişisel verilerin işlenmesinde özellikle "hukuka aykırı" terimini tercih etmiştir. Bu kavram yerine doğrudan KVKK'na atıf yaparak "kanuna aykırı" terimini de kullanabilirdi. Bu durumda hukuka aykırılık ile kanuna aykırılık kavramlarının aynı şeyi ifade etmediğini belirtmek isteriz.

Hukuka aykırılık kavramı, kanunla ya da herhangi bir mevzuat düzenlemesiyle sınırlı olmayan, hukukun genel ve evrensel ilkelerini de kapsayan en geniş anlamdadır. Bunun anlamı kanunda öngörülen işleme şartları sağlanmış olsa dahi, işlenmek istenen amacın sınırlarını aşacak şekilde ve ölçüsüz olarak amacı aşan verilerin işlenmemesi gerektiğidir. Örneğin, bir spor salonu müşterilerinin giriş-çıkış kontrolünü biyometrik veri olan parmak izi taranması yoluyla yapılması,

amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılmasını gerektirdiği, ölçülülük ilkesi gereği veri işlemenin amacı gerçekleştirecek ölçüde olması gerektiği, amacı aşan ölçüde çok veri elde etmenin, ilgili kişi aydınlatılsa ve açık rızası olsa dahi meşru bir amaca hizmet etmeyeceği sebebiyle hukuka aykırıdır.

Veri sorumlusunun ikinci yükümlülüğü, kişisel verilere hukuka aykırı olarak erişilmesini önlemektir. Bu nedenle veri sorumlusu, hukuka uygun şekilde işlediği kişisel verileri hem kurum içinde hem de dışarıdan gelebilecek olası siber saldırılara karşı korumakla yükümlüdür. Yine veri sorumlusunun bir diğer yükümlülüğü kişisel verilerin muhafazasını sağlamaktadır. Veri sorumlusu bu yükümlülüklerini yerine getirmek için her türlü teknik ve idari tedbirleri almak zorundadır.

Veri sorumlusu ile veri sorumlusu tarafından görevlendirilen, veri sorumlu adına veri işleyen gerçek ya da tüzel kişiler, görevlerinden ayrıldıktan sonra dahi işlenen verileri kanun amacı dışında kullanamaz ve başkasına açıklayamazlar. Veri sorumlusu, yukarıda açıklanan verilerin güvenliğine ilişkin tedbirleri almaması halinde idari para cezası ile cezalandırılır.

Kişisel verisinin işlenip işlenmediği, işlendiyse bunun kanuna uygun olup olmadığı, üçüncü kişilere aktarılıp aktarılmadığı, verilerin işlenmesi amacının gerekliliği ortadan kalktıktan sonra silinip silinmediği (veya anonim hale getirilip getirilmediği ya da yok edilip edilmediği) gibi hususlarda ilgili kişi, veri sorumlusuna başvuru hakkına sahiptir. Veri sorumlusu bu talebi en geç otuz gün içinde cevaplandırmakla yükümlüdür. Başvuru konusu bir talep niteliğindeyse, veri sorumlusu tarafından başvurunun reddi, verilen yanıtın yetersiz bulunması veya süresinde cevap verilmemesi hallerinde Kişisel Verileri Koruma Kuruluna şikâyet hakkına sahiptir. Kişisel verilerin hukuka aykırı olarak işlenmesi nedeniyle ilgili kişiler, şikâyet hakkının yanında ayrıca uğradıkları zarara karşılık tazminat talep etme hakları da mevcuttur (6698 Sayılı Kişisel Verilerin Korunması Kanunu , 2016). Şikâyet sonucunda Kurul tarafından ihlal tespit edildiğinde, veri sorumlusu tarafından en geç otuz gün içinde ihlalin ve hukuka aykırılığın giderilmesine karar verilir. Bu süre içinde hukuka aykırılık giderilmediği takdirde, veri sorumlusu idari para cezası ile cezalandırılır.

Kanun tarafından veri sorumlusu hakkında düzenlenen yükümlülüklere uyulmaması halinde düzenlenen idari para cezasının yanında, aydınlatma, veri güvenliği, Kurul tarafından verilen hukuka aykırılık nedeniyle ihlal kararının yerine getirilmemesi eylemlerinin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi hâlinde, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre disiplin soruşturması açılacağı düzenlenmiştir. Ayrıca bu kamu görevlilerinin, görevi ihmal veya görevi kötüye kullanma suçlarından sorumluluğu doğabilecektir.

Yukarıda açıklandığı üzere, veri hukukunun idari ve birazdan görüleceği üzere cezai yaptırımlar öngörerek Anayasal düzeyde koruma sağladığı kişisel verilerin korunması, pozitif hukuk kurallarıyla veri işleyen gerçek ve tüzel kişiler için uyulması gereken kuralları belirlemiştir. Ancak, kişisel verilerin hukuka aykırı olarak işlenmesi, veri güvenliğinin sağlanması, işlendikleri amaç ortadan kalktıktan sonra silinmesi ya da anonim hale getirilmesi ile verilerin üçüncü kişilere hukuka aykırı olarak aktarılması yükümlülükleri, veri sorumlusunun yetkilendirdiği veri işleyen kişiler için de geçerlidir. Bu anlamda, özellikle bilgi işlem alanında çalışan kişilerin, kişisel verilerin korunmasıyla ilgili yükümlülükleri bilmesi ve gerektiğinde veri sorumlusunun alması gereken önlemler hakkında farkındalık yaratması faydalı olacaktır.

4. BİLİŞİM SUÇLARI

Bilişim suçu kavramının mevzuatta tanımı yapılmamıştır. Buna karşın öğretide üzerinde fikir birliğine varılmayan birçok tanım bulunmaktadır (DÜLGER, 2023). Öğretide bilişim suçlarının dar ve geniş anlamda iki tanımı bulunmaktadır. Bu tanımlara göre, geniş anlamda bilişim suçu, bilişim sistemlerinin ve/veya verilerin kullanıldığı ya da bu sistem ya da verilere karşı işlenen her tür suç olarak tanımlanmıştır (DÜLGER, 2023).

Bu tanımın ifade ettiği husus, dar anlamda bilişim suçunun yanında, bir suçun bilişim sistemlerinin araç olarak kullanılarak işlenmesi halinde, bu suçun bilişim suçu olarak kabul edildiğidir. Örneğin Türk Ceza Kanunu 'nun (TCK) 157. Maddesinde "Hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlayan kişiye bir yıldan beş yıla kadar hapis ve beşbin güne kadar adlî para cezası verilir." şeklinde düzenlenen dolandırıcılık suçunun hareket unsuru yani eylem, hileli davranışlarla bir kimseyi aldatmaktır. Hilenin şekli önemli değildir. Bu yönüyle suçun serbest hareketli bir suç olduğu söylenebilir (Veli Özer ÖZBEK, Koray DOĞAN, Pınar BACAKSIZ, 2022). Suçun hareket unsuru olan hileli davranışların şekli önemli olmadığından, bilişim sistemleri yoluyla işlenmesi zorunluluğu yoktur. Ancak TCK'nın 158'inci maddesinin 1'inci fıkrasının (f) bendinde dolandırıcılık suçunun bilişim sistemlerinin araç olarak kullanılması suretiyle işlenmesi halinde üç yıldan on yıla kadar hapis ve beşbin güne kadar adlî para cezası verileceği düzenlenmiştir (5237 Sayılı Türk Ceza Kanunu, 2004). Görüldüğü gibi dolandırıcılık suçu esasında bilişim suçu olmamakla birlikte, bilişim sistemlerinin araç olarak kullanılması yoluyla işlenmesi halinde geniş anlamda bilişim suçu sayılabilir.

Türk Ceza Kanunu'nda düzenlenen hırsızlık, dolandırıcılık, kumar oynanması için yer ve imkân sağlama suçları bilişim sistemlerinin araç olarak kullanılması yoluyla işlenmesi halinde daha fazla ceza verilmesini gerektiren nitelikli hal kapsamındadır. Israrlı takip suçu açısından ise, bilişim sistemlerinin kullanılması yoluyla ısrarlı şekilde tema kurmaya çalışma suçun kanuni unsuru arasında sayılmıştır. Bütün bu suçlarla birlikte, hakaret, tehdit, şantaj gibi birçok suç bilişim araçları kullanılarak işlenebilir. Sayılan tüm bu suçlar, geniş anlamda bilişim suçları arasındadır.

Dar anlamda bilişim suçu ise verilere, bilişim sistemlerine, işleyişine, güvenliğine ya da bütünlüğüne karşı işlenen suçlardır. Dar anlamda bilişim suçları Türk Ceza Kanunu'nun "bilişim alanında suçlar" ve "özel hayata ve hayatın gizli alanına karşı suçlar" bölümünde düzenlenmiştir (DÜLGER, 2023).

4.1. Bilişim Sistemine Girme Suçu (TCK m. 243)

Maddenin birinci fıkrasında "*Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.*" düzenlemesi mevcuttur.

Kanuni düzenleme uyarınca, bilişim sistemine kasten hukuka aykırı olarak girilmesi ya da sisteme hukuka uygun girilmiş olmasına rağmen bu hukuka uygunluk durumu sona erdikten sonra kasten sistemde kalınması suç olarak düzenlenmiştir. Suçun oluşması için hukuka aykırı şekilde girilen veya hukuka aykırı olarak kalınan bilişim sisteminden verilerin ele geçirilmesi gerekmez. Öğretide bu suç tipinin bu tür eylemlerin önüne geçilmesinde tek başına yeterli olmadığı, bilişim sistemlerine yönelik yetkisiz girişlerin önüne geçilmesi için bilişim sistemlerinin korunmasının yanında, sisteme yetkisiz giriş ve veri ele geçirmeyi sağlayan yazılımların üretilmesi ve yayılmasının suç olarak düzenlenmesi gerektiği savunulmaktadır (DÜLGER, 2023).

Maddenin üçüncü fıkrasında "*Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur*" düzenlemesi mevcuttur. Bu hükme göre, sistemin içerdiği verilerin silinmesi ya da değiştirilmesi kastı olmadığı halde, sırf hukuka aykırı olarak bilişim sistemine girme ya da hukuka aykırı olarak sistemde kalma eylemi nedeniyle verilerin silinmesi ya da değişmesi durumu halinde daha fazla cezaya hükmolunacağı düzenlenmiştir. Öğretide failin bu fıkra nedeniyle sorumlu tutulması için verilerin silinmesi ya da yok edilmesinde en azından taksirle hareket etmiş olması gerektiği ifade edilmektedir.

Maddenin dördüncü fıkrasında ise "*Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.*" hükmü düzenlenmiştir. Buna göre, bilişim sistemine hukuka aykırı olarak girilmemesine rağmen, bilişim sisteminin kendisi ya da birden fazla bilişim sistem arasındaki veri alışverişini teknik araçla hukuka aykırı olarak izlemek suç olarak düzenlenmiştir. Burada esasında bilişim sistemine girme başlığı altında olsa da farklı bir suç olan, İngilizcesi "interface" olan "araya girme" eyleminin suç olarak düzenlendiği ifade edilmektedir (DÜLGER, 2023).

4.1. Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu (TCK m. 244)

Maddenin ilk fıkrası *"Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır."* şeklinde düzenlenerek, bilişim sisteminin çok geniş ve önemli alanlarda kullanıldığı gözetilerek işleyişin kasten engellenmesi ya da bozulması suç olarak düzenlenmiştir. Örneğin, kişiye ait sosyal medya hesabının şifresinin bir başkası tarafından değiştirilmesi halinde burada tanımlanan bilişim sisteminin işleyişinin engellenmesi suçunun oluştuğu söylenebilir. Söz konusu suçun teknik destek sorumlusunun kasten bir virüs saldırısına karşı sistemi savunmasız bırakması halinde ihmali davranışla işlenmesi de mümkündür (DÜLGER, 2023). Ancak aynı durumda, aşağıda görüleceği üzere, hesap sahibinin kendi sosyal medya hesabına şifresi başkası tarafından değiştirildiği için girememesi nedeniyle bilişim sistemindeki verilerin erişilmez kılınması da söz konusu olabilir.

Maddenin ikinci fıkrasında "*Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.*" düzenlemesi ile bilişim sistemi içerisindeki verilerin kasten bozulması, yok edilmesi, erişilmez kılınması, sisteme hukuka aykırı ve yetkisiz şekilde veri yerleştirilmesi eylemlerinin yanında sistemde var olan verilerin başka bir yere nakledilmesi eylemleri suç olarak düzenlenmiştir. Bu suçun da teknik destek sorumlusunun ihmali hareketiyle işlenmesi mümkündür. Bu nedenlerle, kurum ve kuruluşlarda bilişim güvenliğinden sorumlu çalışanların bilişim sistemlerinin siber saldırılara karşı görev tanımları dâhilindeki işlerini kasten yapmayarak bilişim sistemlerinin güvenliğini sağlamamaları halinde söz konusu suçları ihmalen işledikleri ve bu nedenle sorumlu oldukları kabul edilebilir.

Maddenin üçüncü fıkrasında ilk iki fıkrada tanımlanan eylemlerin işlendiği bilişim sistemlerinin banka, kredi kurumu, kamu kurum veya kuruluşuna ait olmasının daha fazla cezaya hükmedileceği "*Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır*" şeklinde düzenlenmiştir.

Maddenin son fıkrasında ise, ilk üç fıkrada tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlaması halinde, failin iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılacağı düzenlenmiştir.

4.2. Banka veya Kredi Kartlarının Kötüye Kullanılması (TCK m. 245)

Kanun koyucu banka ve kredi kartlarıyla işlenebilecek bilişim sistemleri alanındaki suçları ayrı bir madde ile düzenlemiştir. Buna düzenlemeye göre, kanun koyucu, başkasına ait banka veya kredi kartının ele geçirilip, sahibinin rızası olmadan kullanılması yoluyla yarar sağlanması eylemini üç yıldan altı yıla kadar hapis cezası ve beşbin gün adli para cezası ile yaptırıma tabi tutmuştur. Aynı maddenin diğer fıkralarında, başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretilmesi, satılması, devredilmesi, satın alınması veya kabul edilmesi eylemleri üç yıldan yedi yıla kadar hapis ve onbin güne kadar adlî para cezası ile yaptırıma tabi tutulmuş, sahte kartların kullanarak yarar sağlanması eylemi ise dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adlî para cezası yaptırımına tabi tutulmuştur.

4.3. Yasak Cihaz veya Programlar (TCK m. 245/A)

"*Bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bu bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişi, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.*"

Kanunun bu maddesinde, bir cihazın, yazılımın, programın, şifre ya da her türlü güvenlik kodunun bilişim alanında düzenlenen suçlar ile bilişim sistemlerinin araç olarak kullanılarak işlenebilen diğer suçların işlenmesi amacıyla yapılması veya oluşturulması durumunda maddede sayılan eylemleri yaptırıma tabi tutulmuştur.

5. KİŞİSEL VERİLERE İLİŞKİN SUÇLAR

Kişisel Verilerin Korunması Kanununun 17'nci maddesinde kişisel verilere ilişkin suçlar bakımından TCK'nın 135 ila 140'ıncı maddelerinde düzenlenen hükümlerin uygulanacağını düzenlemiştir. Buna göre, kişisel verilerin hukuka aykırı olarak kaydedilmesi, verilerin hukuka aykırı olarak ele geçirilmesi, yayılması, başkasına verilmesi; verilerin saklanması gereken süreden sonra yok edilmemesi suçları mevcuttur. Kişisel veriler, gelişen teknoloji ile yaygın biçimde bilişim sistemleri aracılığıyla işlenmekte olduğundan, bu alanda düzenlenen suçlar ve cezalar hakkında okuyucuya bilgi verilmesi yararlı görülmüştür. Ancak unutulmamalıdır ki, kişisel veriler yalnızca bilişim sistemleri aracılığı ile işlenmez. Bu durumda artık bilişim hukukunun kapsamı dışına çıkılmış olur. Bilişim sistemi aracılığı ile işlenmese de kişisel verilerin işlenmesine dair KVKK'ndaki uygunluk unsurları geçerli olacaktır. Aynı zamanda TCK'nın 135-140 maddelerinden failin sorumlu olması için, verinin bilişim sistemleri aracılığı ile işlenmesi şart değildir.

5.1. Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135)

"Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir. Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır."

KVKK'nda düzenlenen hukuka uygunluk şartları oluşmadan kişisel verilerin kaydedilmesi hapis cezası ile yaptırıma tabi tutulmuştur. Madde-

nin ikinci fıkrasında sayılan ve KVKK'nda da özel nitelikli kişisel veri olarak sayılan kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin kişisel verilerin hukuka aykırı olarak işlenmesi halinde birinci fıkradaki ceza miktarının yarı oranında artırılacağı düzenlenmiştir.

5.2. Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme (TCK m. 136)

"Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır.

Suçun konusunun, Ceza Muhakemesi Kanununun 236'ncı maddesinin beşinci ve altıncı fıkraları uyarınca kayda alınan beyan ve görüntüler olması durumunda verilecek ceza bir kat artırılır."

Bu maddenin birinci fıkrasında kişisel verilerin hukuka aykırı olarak bir başkasına aktarılması ya da bir başkasının kişisel verileri hukuka aykırı olarak ele geçirmesi suçu düzenlenmiştir. Maddenin ikinci fıkrasında ise, maddede sayılan eylemlerin cinsel saldırı ve cinsel istismar mağdurlarının ceza soruşturması evresindeki kayda alınan beyan ve görüntüleri hakkında işlenmesi halinde, daha fazla cezaya hükmolunacağı düzenlenmiştir.

TCK'nun 135 ve 136'ncı maddelerinde düzenlenen suçların kamu görevlisi tarafından görevinin verdiği yetki kötüye kullanılmak suretiyle veya belirli bir meslek ve sanatın sağladığı kolaylıktan faydalanmak suretiyle işlenmesi halinde daha fazla cezaya hükmolunacağı ise 137'nci maddede ayrıca düzenlenmiştir.

5.3. Verileri Yok Etmeme (TCK m 138)

"Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir.

Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır."

Maddenin ilk fıkrası, hukuka uygun olarak işlenen verilerin ya doğrudan kanunun silinme zamanını düzenlemesi ya da işlenme amacının ortadan kalkması halinde verilerinin silinmesiyle yükümlü olanların bu yükümlülüklerini yerine getirmemesini suç olarak düzenlemiştir. Buradaki amaç daha önce hukuka uygun olarak ve meşru bir amaçla işlenen kişisel verilerin sonsuza kadar saklanmasının kişisel verilerin ve özel hayatın gizliliğinin ihlal olasılığının artmasıdır.

KVKK'nun 17'nci maddesinde KVKK'nun 7'nci maddesine aykırı olarak kişisel verileri silmeyen ya da anonim hale getirmeyenlerin ise TCK'nun 138'inci maddesine göre cezalandırılacağı hükmü düzenlenmiştir.

Öğretide yok etme kavramının, imha kavramı kapsamında, yok etme, silme ve anonim hale getirme unsurlarından oluştuğu ifade edilmektedir (Rıza SAKA, Ramazan ÇAĞLAYAN, Mahmut KOCA, 2022). Buna göre, silime veya yok etme yerine, verinin anonim hale getirmesi durumunda suçun oluşmayacağı kabul edilmelidir.

Kanundaki düzenleme uyarınca suçun, ya ilgili kanunlarda verilerin kim tarafından silineceği düzenlenmişse bu kişi ya da KVKK'da düzenlenen veri sorumlusu tarafından işlenebileceği ifade edilmektedir (Rıza SAKA, Ramazan ÇAĞLAYAN, Mahmut KOCA, 2022).

Maddenin ikinci fıkrasında ise bir suç soruşturması ya da kovuşturması sırasında Ceza Muhakemesi Kanununa göre mağdur ya da sanıktan elde edilen bazı kişisel verilerin imha edilmeme-

si halinde cezanın daha ağır şekilde uygulanacağı düzenlenmiştir. Örneğin genetik inceleme verilerinin, iletişimin, gizli soruşturmacının elde ettiği suçla ilgili olmayan kişisel verilerin, teknik araçla izleme ses ve görüntü kaydı ile oluşan verilerden suçla ilgili olmayanların imha edilmesi gerekirken bunun yapılmaması halinde maddenin ikinci fıkrası uygulanacaktır. Bu durumlarda suçun faili, verilerin imhasıyla ilgili yükümlü kılınan kamu görevlisi olup, Ceza Muhakemesi Kanununa göre genellikle cumhuriyet savcısı olacaktır (Rıza SAKA, Ramazan ÇAĞLAYAN, Mahmut KOCA, 2022).

Kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve verileri yok etmeme hariç olmak üzere bu bölümdeki diğer suçların soruşturması ve kovuşturmasının mağdurun şikâyetine bağlıdır.

6. SONUÇ

Bilişim sistemlerinin gelişmesi, bilginin bilişim sistemlerinde işlenmesinin yaygın hale gelmesi sonucunda bilişim hukuku alanı doğmuş ve bu alan gelişmeye devam etmektedir. Bilişim sistemlerinin güvenliğini sağlamak, içerdiği çok sayıda kişisel verinin yanında kullanıldığı alana göre özel hayatın gizli mahrem kalması gereken bilgilerle beraber, ekonomik alanda örneğin bankacılık bilgilerini de içermektedir. İşte bu geniş kapsamlı ve korunmadığı zaman kötüye kullanımı çok olumsuz sonuçlar doğurması olası verilerin işlendiği bilişim sistemlerinin güvenliğini koruma gerekliliği, mevzuatımızda da bu alanın hem idari yaptırımla hem de adli ceza ile yaptırıma tabi tutulmasına sebep olmuştur.

Veri güvenliğinden sorumlu kişilerin yanında, bilişim sistemlerine yasal olmayan erişimlerin de engellenmesi gerekmekte olduğundan, bilişim sistemlerine ilişkin alanlarda faaliyet gösteren bireylerin ve kurumların hangi hallerde sorumlu olacağı giriş seviyesinde anlatılmaya çalışılmıştır. Giriş bölümünde ifade edildiği üzere internet yayıncılığı, sosyal medya, elektronik ticaret, elektronik haberleşme, elektronik imza, yapay zekâ, elektronik paralarla ilgili faaliyetler de bilişim hukukunun kapsamı içinde kalmakta ancak bu çalışmanın konusunu oluşturmamaktadır. Bu anlamda ön lisans seviyesinde temel bilgiler içeren bu çalışmanın öğrencilere faydalı olacağını umarım.

BÖLÜM ÖZETİ

Teknolojik gelişmeler sayesinde günümüz dünyasında bilişim araçları ve internet çok yaygın kullanım alanına sahiptir. Bu yapı iletişimden ekonomik faaliyetlere, veri üretme-saklama-yaymadan elektronik resmî belge oluşturmaya kadar, bununla da sınırlı olmayan ve daha birçok alanı etkileyen, değiştiren ve dönüştüren büyük etkilere sahiptir. Bilişimde yaşanan gelişmeler, geniş etki alanında yarattığı faydanın yanında riskler de barındırmaktadır. Bu riskler iki başlık altında incelenebilir. Bunlardan ilki, doğrudan bilişim araçlarının taşıdığı risklerdir. Diğer bir anlatımla bilişim sistemlerine yetkisiz ve kötü niyetli girilmesiyle başlayan ve çeşitlenen risklerdir. Diğeri ise, bir takım hukuka aykırı fiillerin, bilişim sistemlerinin araç olarak kullanılması yoluyla işlenmesi sonucunda ortaya çıkması olası risklerdir. Bu durumda ya hukuka aykırı fiilin işlenebilmesinin kolaylaşmış olabileceği ya da failin kimliğini daha kolay gizleyebileceği gibi durumlar bilişim sistemleri ve internet ağının taşıdığı kendine özgü risklerdir. Bilişim hukuku kavramı, önceleri bu gibi suç ve cezaların belirlendiği, ceza hukukuyla ilgili olarak kamu hukuku alanında anılmıştır. Bilişim sistemleri, bilişim araçları ve internetin kullanım alanı hem kamu kurum ve kuruluşlarını hem de gerçek ya da tüzel kişiler arasındaki hukuki iş ve işlemleri geniş anlamda etkilemiştir. Bilişim sistemleri, araçları ve internet yoluyla örneğin bankacılık işlemleri yapılabilmekte, nüfus kayıtlarına erişilebilmekte, ıslak imza ile aynı anlama gelen elektronik imzalı belge oluşturulabilmekte, sağlık verileri işlenmekte, kamu kurumlarına idari başvurular yapılabilmekte, dava açılabilmekte, kamu kurumları yetki alanı içindeki tüm bilgi ve belgeleri üretip saklayabilmektedir. Ayrıca yapay zekâ, kripto varlıklar gibi unsurlar bilişim hukukunun özel hukuk alanında da anılmasına ve gelişmesine sebep olmuştur. Bilişim hukukunun geniş kapsamı karşısında, kitabın bu bölümünde özellikle bilişim hukukunun bir alt dalı olarak sayılabilecek olan “veri hukuku” konusuna değinilecek, bilişim hukukunun diğer alt dalları hakkında genel bilgiler verilecek, bilişim suç ve cezaları ile kişisel verilere ilişkin suç ve cezalar hakkında açıklamalar yapılacaktır.

GÖZDEN GEÇİRELİM

1. Bilişim sistemlerinin yaygın olarak kullanımının beraberinde getirdiği riskleri düşünelim.

2. Kişisel verilerin hukuk düzeni tarafından hangi yollarla korunduğunu düşünelim.

3. Kişisel verilerin hukuka uygun olarak işlenme koşullarını biliyor musunuz?

4. Ağ ve veri güvenliğinin önemini bilişim suçları kapsamında düşünelim.

5. Kişisel verilerin korunmasında, veri sorumlusunun yükümlülüklerini gözden geçirelim.

6. Bilişim sistemine girme, sistemi engelleme, verileri yok etme ve değiştirmenin suç olduğunu, bu nedenle veri ve ağ güvenliğinin önemini kavrayalım.

Kaynakça

5237 Sayılı Türk Ceza Kanunu. (2004).

6698 Sayılı Kişisel Verilerin Korunması Kanunu . (2016, Nisan 7). *Kabul Tarihi: 24.03.2016*. Resmi Gazete, S.29677.

Bilgi Tekonojileri ve İletişim Kurumu. (2019). *Bilişim Hukuku ve Bilişim Suçu.* Ekim 15, 2023 tarihinde Bilgi Tekonojileri ve İletişim Kurumu Resmi Web Sayfası: https://internet.btk.gov.tr/bilisim-hukuku-ve-bilisim-sucu adresinden alındı.

Ceza Muhakemesinde Ses Ve Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmelik. (2011, Eylül 20). Sayı: 28060: Resmi Gazete.

DÜLGER, M. V. (2023). *Bilişim Suçları ve İnternet İletişim Hukuku.* Ankara: Seçkin Yayıncılık.

EKİCİ, Ş. (2023). *Bilişim ve Tekonoloji Hukuku.* Ankara: Seçkin.

https://www.kvkk.gov.tr/. (tarih yok). Ekim 22, 2023 tarihinde Kişisel Verileri Koruma Kurumu Resmi Web Sitesi: https://kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf adresinden alındı

İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme. (1950, Kasım 4). Roma.

Kişisel Verileri Koruma Kurumu. (2019). *Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi.* Ekim 22, 2023 tarihinde Kişisel Verileri Koruma Kurumu Resmi Web Sitesi: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/41784a70-2bac-4e4a-830f-35c628468646.PDF adresinden alındı

KÖKSAL, A. (2003). *Bilişim Devrimi, Küreselleşme ve Uygarlıklar Çatışması Ortamında Kimliğini Arayan Türkiye.* Ekim 15, 2023 tarihinde Prof. Dr. Aydın KÖKSAL Kişisel Web Sitesi: https://www.aydinkoksal.gen.tr/shared/dosyalar/yayinlar/yayin-194-2003.pdf adresinden alındı

Rıza SAKA, Ramazan ÇAĞLAYAN, Mahmut KOCA. (2022). *Avrupa Birliği Hukuku, İdare Hukuku ve Ceza Hukuku Açısından Kişisel Verilerin İmhası.* Seçkin Yayıncılık .

TURAN, M. (2021). *Karşılaştırmalı Hukukta Kişisel Verilerin Korunması.* Seçkin .

TURAN, M. (2023). *Bilişim Hukuku.* Seçkin.

Türk Dil Kurumu . (2023). *Türk Dil Kurumu Sözlükleri.* Ekim 15, 2023 tarihinde Güncel Türkçe Sözlük: https://sozluk.gov.tr/ adresinden alındı

Türk Medeni Kanunu . (2001). Resmi Gazete .

Veli Özer ÖZBEK, Koray DOĞAN, Pınar BACAKSIZ. (2022). *Türk Ceza Hukuku Özel Hükümler.* Seçkin Yayıncılık.