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