BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ

Ebu Yusuf Güven - Melike Başer - Muhammed Ali Aydın

Öz

Bilgi teknolojileri ve dijital hizmetler yaygınlaştıkça siber tehditler de çoğalmakta ve bilgi güvenliğinin önemi her geçen gün artmaktadır. İletişim altyapılarının ve bilgi işlem çözümlerinin sorunsuz çalışması hayati önem kazanmaktadır. Bilgi güvenliği, bilgi sistemlerinin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamaktan sorumludur ve birçok teknik veya teknik olmayan faktör bilgi güvenliği ihlallerine neden olabilir. Bu nedenle, bilgi güvenliği uyumluluğunu sağlamak için çalışanın davranışı kontrol edilmeli ve bilgilere erişimi kısıtlanmalıdır. Bilgi güvenliğini sağlamak için en temel araç, bir kuruluşun bilgi güvenliği politikasıdır. Etkili bir bilgi güvenliği politikası, uluslararası güvenlik standartları ve uygulamalar doğrultusunda oluşturulur. Bilgi güvenliği politikası, çalışanların beklenen ve beklenmeyen davranışlarını özetleyerek bir kuruluşun bilgi güvenliği standartlarını karşılama taahhüdünü belirtir. Ayrıca, bilgi güvenliği politikasının ihlali durumunda verilecek cezaları da belirler. Ancak herhangi bir kuruluşun güvenliğini sağlamak için bilgi güvenliği politikası tek başına yeterli değildir. Kuruluş aynı zamanda, etkili bir bilgi güvenliği politikası uyumluluğu sağlamalıdır. Bu çalışma kapsamında bilgi güvenliği kavramı anlatılmakta ve geçmişten günümüze bilgi güvenliğinin gelişim aşamaları gösterilmektedir. Özellikle Bilgi Güvenliği Yönetim Sistemleri ve Bilgi Güvenliği Politikasının uygulanabilirliği dünyaca kabul görmüş ISO 27001 standardı çerçevesinde açıklanmıştır. Siber tehditler kapsamında Bilgi Güvenliği Politikasına göre alınması gereken tedbirler aktarılmıştır.

Anahtar Kelimeler: Siber Güvenlik, Siber Dayanıklılık, Bilgi Güvenliği Yönetim Sistemi (BGYS), Bilgi Güvenliği Politikası, Bilgi Güvenliği Standardı

1. Giriş

Teknolojinin gelişmesiyle birlikte, kurum ve kuruluşlar İnternet üzerinden iş yapmak için çeşitli mekanizmalara sahip olmuştur. İnternet, ticarette rekabet edebilmek için önemli bir araç hâline gelmiştir. İş ve çalışma hayatının

büyümesiyle birlikte, kişisel İnternet kullanımı da artmaktadır. TÜİK verilerine göre, hane halkının büyük çoğunluğu İnternet'e erişim sağlamakta ve düzenli olarak İnternet'i kullanmaktadır (TÜİK, 2022).

Bilgi sistemleri, bilgi ekonomisi çağında kuruluşlar için kritik bir yardımcı hâline gelmiştir (Rehak, 2020). Veri yönetimi rolleri nedeniyle, işletmeler için önemli bir değere sahiptir. Ancak bilgi sistemlerinde herhangi bir aksaklık veya güvenlik ihlali ciddi finansal kayıplara ve itibar kaybına yol açabilir. Bu nedenle, rakipler için hedef hâline gelebilirler (Ali, 2021). Araştırmalar, bilgi güvenliği ihlallerinin sıklıkla teknik olmayan faktörlerden kaynaklandığını, örneğin çalışan ihmali gibi etkenlerin etkili olduğunu göstermektedir (Chen, 2020).

Kurum ve kuruluşlar, bilgi güvenliği yönetim sistemleri aracılığıyla bu riskleri etkin bir şekilde yönetmeli, bilgi güvenliği politikalarını belirlemeli ve kontrolleri uygulamalıdır. Bu sayede, bilgi güvenliği ihlallerine karşı daha dirençli olabilir, müşteri ve paydaşların güvenini sağlayabilir ve iş sürekliliğini koruyabilirler. Bilgi Güvenliği Yönetim Sistemleri (BGYS), bilgi varlıklarını korumak amacıyla uygulanan kapsamlı bir çerçeve sunar. BGYS'nin temel amacı, kuruluş içinde bilgi güvenliği risklerini tanımlamak, değerlendirmek ve iyileştirmek için sistematik bir yaklaşım sağlamaktır.

BGYS'nin uygulanması, risk değerlendirmesi, güvenlik politikalarının belirlenmesi, kontrollerin uygulanması, performans izleme ve sürekli iyileştirme gibi adımları içerir. Hassas bilgileri korumak için gerekli kontrolleri ve önlemleri ana hatlarıyla belirleyen politikaların, prosedürlerin ve kılavuzların geliştirilmesini içerir. Bu kontroller fiziksel güvenlik, erişim kontrolleri, ağ güvenliği, olaylara müdahale ve çalışanların farkındalığı gibi çok çeşitli alanları kapsar. BGYS'nin uygulanması tipik olarak ISO/IEC 27001 gibi uluslararası standartlara dayanan yapılandırılmış bir yaklaşım izler. Bu standart, bir kuruluşun bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli olarak iyileştirilmesi için bir çerçeve sağlar. Riskleri değerlendirmek, güvenlik hedeflerini tanımlamak ve belirlenen riskleri ele alarak kontrolleri uygulamak için gereklilikleri ortaya koyar. Kuruluşlar bir BGYS uygulayarak bilgi güvenliği risklerini etkin bir şekilde yönetilebilir, hassas bilgileri koruma konusundaki kararlılıklarını gösterebilir ve müşteriler, ortaklar ve paydaşlar nezdinde güven oluşturabilirler. Güvenlik olaylarına proaktif olarak yanıt vermelerini, ihlallerin etkisini en aza indirmelerini ve gelişen siber tehditler karşısında iş sürekliliginin devamliligini saglar.

Çalışma kapsamında Kavramsal Çerçeve' de Güvenlik, Bilgi Güvenliği, Bilgi Güvenliği Tarihi ve Bilgi Güvenliği Anahtar Kavramları anlatılmıştır. Bilgi Güvenliği Yönetim Sistemi (BGYS) olarak ISO/IEC 27001 anlatılmıştır. Bilgi Güvenliği Tedbirleri başlığında siber güvenlik risklerinin oluşabileceği ortamlara göre varlıklarımızı koruma yöntemleri aktarılmıştır. Sonuç ve Öneri bölümü ile çalışma tamamlanmıştır.

2. Kavramsal Çerçeve

2.1. Güvenlik Nedir?

Genel olarak güvenlik, tehlikeden uzak olma niteliği veya durumudur. Başka bir deyişle, düşmanlara karşı kasten veya başka türlü zarar verecek olanlardan korunma amaçlanmaktadır. Örneğin ulusal güvenlik kavramı, bir devletin egemenliğini, varlıklarını, kaynaklarını ve halkını koruyan çok katmanlı bir sistemi kapsamaktadır. Bir kuruluş için uygun güvenlik düzeyine ulaşmak da çok yönlü bir sistem gerektirir. Başarılı bir kuruluş, operasyonlarını korumak için aşağıdaki çoklu güvenlik katmanlarına sahip olmalıdır:

- **Fiziksel güvenlik (Physical security)**, yetkisiz erişim ve kötüye kullanımdan korunmak amacıyla fiziksel ögeleri, nesneleri veya alanları koruma altına almayı sağlar.
- **Personel güvenliği (Personnel security)**, kuruluşa ve kuruluşun faaliyetlerine erişim yetkisine sahip olan bireyleri veya grupları korumayı amaçlar.
- **Operasyon güvenliği (Operations security)**, belirli bir işlem veya faaliyetin ayrıntılarını koruma altına alır.
- **İletişim güvenliği (Communications security)**, iletişim ortamını, teknolojisini ve içeriğini korur.
- **Ağ güvenliği (Network security)**, ağ cihazlarını ve düğümlerini, bağlantıları ve içeriği koruma altına alır.
- **Bilgi güvenliği (Information security)**, bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini depolama, işleme veya iletim sırasında korunmasını hedefler. Bu, politika oluşturma, eğitim, farkındalık yaratma ve teknoloji uygulamalarıyla sağlanır.

Ulusal Güvenlik Sistemleri Komitesi (CNSS), **bilgi güvenliği**ni, bilgilerin ve bu bilgileri kullanan, depolayan ve ileten sistemler ve donanımlar dâhil

olmak üzere kritik unsurlarının korunması olarak tanımlar (Kissel, 2011, Koca ve Avcı,2023). CNSS bilgi güvenliği modeli, bilgisayar güvenlik endüstrisi tarafından geliştirilen "C.I.A." üçgeni adı verilen bir kavramdan gelişmiştir. "C.I.A." üçgen, ana bilgisayarın geliştirilmesinden bu yana bilgisayar güvenliği için endüstri standardı olmuştur. Bilginin kuruluşlara değer katan üç özelliğine dayanmaktadır: gizlilik (confidentiality,), bütünlük (integrity) ve erişilebilirlik (availability).



Şekil 1: C.I.A Üçgeni (Chopra & Chaudhary, 2020)

2.1.1. Gizlilik (Confidentiality)

Veri gizliliği, dijital çağda hızla gelişen teknolojiler ve artan veri paylaşımı ortamlarıyla birlikte, kişisel ve hassas bilgilerin korunması zorlaşmaktadır. Veri gizliliği, bilgilerin ifşa edilmemesi ve yetkisiz erişimden korunması prensibine dayanır. Hassas verilerin sızdırılması veya kötüye kullanılması, mahremiyetin tehlikeye atılmasına ve maddi ve manevi kayıplara yol açabilir. Bilgi gizliliğini korumak için bazı önlemler şöyle sıralanabilir:

- Bilgi sınıflandırması,
- Güvenli belge depolama,
- Bilgi güvenlik politikalarının uygulanması,
- Bilgi sorumlularının ve son kullanıcıların eğitimi.

Bilgilerin gizliliğinin değeri, çalışanlar, müşteriler veya hastalar hakkında kişisel bilgiler söz konusu olduğunda oldukça yüksektir. Bir kuruluşla işlem yapan bireyler, kuruluş ister federal bir kurum, ister bir işletme olsun, kişisel bilgilerinin gizli kalmasını bekler. Şirketler gizli bilgileri ifşa ettiğinde sorunlar ortaya çıkar. Bazen bu ifşa kasıtlıdır, ancak gizli bilgilerin ifşasının yanlışlıkla gerçekleştiği zamanlar da vardır. Örnegin, gizli bilgilerin yanlışlıkla kuruluş içindeki biri yerine kuruluş dışındaki birine e-posta ile gönderilmesi gibi. Ayrıca gizlilik ihlallerine, bir çalışanın kritik bilgiler içeren bir belgeyi parçalamadan atması veya bir bilgisayar korsanının Web tabanlı bir kuruluşun dâhili veritabanına başarılı bir şekilde girerek müşterilerle ilgili adlar, adresler, kredi kartı numaraları gibi hassas bilgileri çalması örnek olarak verilebilir.

Bir tüketici olarak, neredeyse her gün kolaylık sağladığı için veya belirli bir değer karşılığında gizli bilgilerden vazgeçilebilir. Bir markette "üyelere özel" bir kart kullanarak, bazı harcama alışkanlıkları ifşa edilebilir. Çevrimiçi bir anket doldurulduğunda, çevrimiçi ayrıcalıklara erişim için kişisel geçmiş ayarları değiştirilir. Bilginin ifşa edildiği parçalar kopyalanır, satılır, çoğaltılır, dağıtılır ve sonunda profiller eksiksiz dosyaları hâlinde birleştirilir. Salam hırsızlığı (salami theft) adı verilen bir suç girişiminde de benzer bir teknik kullanılır. Bir şarküteri çalışanı salamın tamamını çalamayacağını bilir, ancak burada veya orada birkaç dilim haber verilmeksizin eve götürülebilir. Sonunda şarküteri çalışanı bütün bir salamı çalmıştır. Bilgi güvenliğinde salam hırsızlığı, bir çalışanın daha fazla alındığında fark edileceğini bilerek bir defada birkaç bilgi çalması, ancak sonunda çalışanın eksiksiz veya kullanılabilir bir şey alması durumunda gerçekleşir.

2.1.2. Bütünlük (Integrity)

Bilgi bütünlüğü, doğru, eksiksiz ve bozulmamış bir şekilde bilginin korunması anlamına gelir. Ancak bilgi çeşitli tehditlerle karşı karşıya kalabilir ve bozulabilir, hasar görebilir, yok olabilir veya yanlış bir şekilde değiştirilebilir. Bu durumlar, bilginin bütünlüğünü tehdit eder. Bütünlüğün sağlanması için güvenlik kontrolleri ve doğrulama mekanizmaları kullanılır. Bilgiler depolanırken veya iletilirken bozulma meydana gelebilir. Birçok zararlı yazılım (bilgisayar virüsü ve solucanı vb.) verileri bozmak amacıyla tasarlanmıştır. Bu nedenle, bir virüs veya solucanı algılamak için önemli bir yöntem, dosya boyutu yardımıyla gösterilen dosya bütünlüğündeki değişiklikleri aramaktır. Bilgi bütünlüğünü sağlamanın başka bir anahtar yöntemi, bir dosyanın, özet değer

(hash) adı verilen tek bir büyük sayıyı hesaplamak için dosyadaki bitlerin değerini kullanan özel bir algoritma tarafından okunduğu dosya özetidir. Herhangi bir bit kombinasyonu için özet (hash) değeri benzersizdir. Bir bilgisayar sistemi bir dosya üzerinde aynı hashing algoritmasını uygular ve o dosya için kaydedilen özet değerinden farklı bir sayı elde ederse, dosya tehlikeye girmiş demektir ve bilgilerin bütünlüğü kaybolmuştur. Bilgi bütünlüğü, bilgi sistemlerinin mihenk taşıdır, çünkü kullanıcılar bütünlüğünü doğrulayamazsa bilginin hiçbir değeri veya faydası yoktur.

Dosya bozulması, bilgisayar korsanları gibi dış güçler tarafından meydana gelmek zorunda değildir. Örneğin iletim ortamındaki gürültü (noisy) de verilerin bütünlüğünü kaybetmesine neden olabilir. Düşük voltaj seviyeli bir devrede veri iletmek, verileri değiştirebilir ve bozabilir. Fazlalık bitleri ve kontrol bitleri, bilginin bütünlüğüne yönelik iç ve dış tehditleri telafi edebilir. Her iletim sırasında algoritmalar, özet (hash) değerleri ve hata düzeltme kodları bilginin bütünlüğünü sağlar. Bütünlüğü tehlikeye giren veriler yeniden iletilir.

2.1.3. Erişilebilirlik (Availability)

Erişilebilirlik, bilgilere yetkili kullanıcıların sorunsuz bir şekilde erişebilmesini ve gerekli durumlarda uygun formatta alabilmesini sağlayan önemli bir kavramdır. Bir bilginin erişilebilir olması, ilgili kişilerin veya sistemlerin engellenmeden veya müdahale olmadan bilgiye erişim sağlamasını gerektirir. Örneğin, girişten önce tanımlama gerektiren araştırma kütüphaneleri düşünüldüğünde kütüphaneciler, kütüphanenin içeriğini yalnızca yetkili kullanıcılara açık olacak şekilde korurlar. Kütüphaneci, kullanıcının kitap arşivine ücretsiz erişimi olmadan önce kullanıcının kimliğini kabul etmelidir. Yetkili kullanıcılar arşivin içeriğine eriştikten sonra, ihtiyaç duydukları bilgileri kullanılabilir bir formatta ve tanıdık bir dilde bulmayı beklerler.

Bilginin gizlilik, bütünlük ve erişilebilirlik özellikleri günümüzdeki bilgi güvenliği için önemlidir, ancak bu üç özellik artık değişen tehditlerle karşı karşıyadır. Bilgiye yönelik tehditler, kazara veya kasıtlı hasar, imha, hırsızlık, değişiklik veya insan/insan dışı tehditlerden kaynaklanan kötüye kullanımlar gibi çeşitli olayları içermektedir. Bu nedenle, daha sağlam bir bilgi güvenliği modeli geliştirme ihtiyacı ortaya çıkmıştır. Bu model, teknolojik yenilikler, güvenlik politikaları, eğitim ve farkındalık çalışmalarıyla birlikte tehditlere karşı etkili koruma sağlayabilir.

2.2. Bilgi Güvenliği Tarihi

Bilginin güvenliği, yazılı ve sözlü metinlerin güvenliğinden başlayan dijital ve fiziksel nesnelerin güvenliğine varan köklü bir geçmişe sahiptir. Bilgi güvenliği, dijital ortamda bilgi depolama ve iletişimin yaygınlaşmasıyla önemli bir konu hâline gelmiştir. Bilgisayarlar, internet ve diğer iletişim teknolojileri, bilgi güvenliği tehditlerini artırmış ve güvenlik önlemlerinin geliştirilmesini gerektirmiştir. Şirketler, hükûmetler ve diğer kuruluşlar, bilgilerini korumak için çeşitli yöntemler ve teknolojiler kullanmaktadır. Ancak sürekli olarak gelişen tehditler karşısında bilgi güvenliği alanında uzmanların ve altyapıların güncel kalması ve etkili önlemler geliştirmesi gerekmektedir.

İletişim teknolojilerinin gelişmesi ve bilgisayarların birbirine bağlama ihtiyacı bilgi güvenliği açısından yeni riskler ve fırsatlar oluşturmuştur. İnternet, daha önce hükûmet, akademi ve özel endüstri profesyonellerinin alanı olan 1990'larda genel halkın kullanımına sunuldu. İnternet, bir telefon hattına veya İnternete bağlı bir yerel alan ağına (LAN) ulaşabilen neredeyse tüm bilgisayarlara bağlantı sağladı. İnternet ticarileştikten sonra, teknoloji yaygınlaştı ve genişleyen bir kullanım alanıyla dünyanın hemen her köşesine ulaştı. İlk başlarda bilgi güvenliğini sağlamak öncelik değildi ve bunun için önlemler alınmadı. Ancak bu öncü teknolojiler geniş çapta benimsenip endüstri standartları hâline geldikçe, bir dereceye kadar güvenlik getirildi. Aslında, bugün İnternet'te e-posta özelinde yaşanan çoğu güvenlik sorunu, güvenlik eksikliğinin sonucudur. Tüm İnternet ve e-posta kullanıcılarının (muhtemelen güvenilir) bilgisayar bilimcisi olduğu o zamanlar, posta sunucusu kimlik doğrulaması ve e-posta şifreleme gerekli görünmüyordu. Önceden bilgi işlem yaklaşımları, bilgisayarları barındıran veri merkezinin fiziksel ortamına yerleştirilmiş güvenliğe dayanıyordu. Ağa bağlı bilgisayarlar baskın bilgi işlem tarzı hâline geldikçe, ağa bağlı bir bilgisayarı fiziksel olarak koruma yeteneği kayboldu ve depolanan bilgiler zamanla güvenlik tehditlerine daha açık hâle geldi.

Bugün internet, milyonlarca güvenli olmayan bilgisayar ağının birbiriyle sürekli iletişim hâlinde olmasını sağlamaktadır. Her bilgisayarın depolanan bilgilerinin güvenliği, artık bağlı olduğu diğer tüm bilgisayarların güvenlik düzeyine bağlıdır. Son yıllarda, bilgi güvenliğini geliştirme ihtiyacına dair artan bir farkındalık ve bilgi güvenliğinin ulusal savunma için önemli olduğunun farkına varıldı. Artan siber saldırı tehdidi, hükûmetleri ve şirketleri, kamu hizmetlerinin ve diğer kritik altyapıların bilgisayar kontrollü sistemlerini savunma ihtiyacı konusunda daha fazla bilinçlendirdi. Ulus-devletlerin bilgi sa-

vaşına girmesi ve iş veya kişisel bilgi sistemlerinin savunmasız olmaları hâlinde zayiat verme olasılığı konusunda da artan bir endişe oluşturmuştur.

21. yüzyılda, erken dönem ana bilgisayar sistemlerinden daha fazla bilgi işlem gücüne sahip akıllı telefonlar ve tabletlerle mobil bilgi işlemde büyük bir artış görülmeye başlanmıştır. Gömülü cihazlar, Nesnelerin İnterneti'nde (IoT) günlük nesnelere yerleşik bilgi işlemin de oluşmasını sağlamıştır. Bu ağa bağlı bilgi işlem platformlarının her biri bulut tabanlı hizmet sağlama sistemleri ile ağlara bağlandıklarında kendi güvenlik sorunları ve endişelerini beraberinde getirmektedir. Kablosuz ağ (Wireless networking) İnternet'e erişim için yaygın olarak kullanılan bir bağlantı hâline gelmiştir. Kablosuz ağlar sürekli bir anonim saldırı tehdidine açık bir bağlantı yoludur ve güvenliği sağlanmadığı takdirde yüksek riskleri mevcuttur.

2.3. Bilgi Güvenliği Anahtar Kavramlar

Bilgi güvenliği kapsamında kullanılan birçok önemli kelime ve kavram vardır ve bu kavramlar, bilgi güvenliği kavramının anlaşılabilmesi için önemlidir. Bilgi Güvenliği erişim, varlık, saldırı, kontrol, koruma, önlem gibi kavramlar açıklanmaktadır.

Erişim, bir özne veya nesnenin başka bir özne veya nesneyi kullanma, manipüle etme, değiştirme veya etkileme yeteneğini ifade eder. Bilgisayar sistemlerinde erişim, yetkili kullanıcıların bir sisteme yasal erişime sahip olmasıyla sağlanırken, bilgisayar korsanları yasa dışı erişime sahip olabilir. Erişim denetimleri, bu yeteneği düzenleyerek bilgi güvenliğini sağlamak için kullanılır.

Varlık, korunması gereken kurumsal kaynak veya değeri ifade eder. Varlıklar, fiziksel veya mantıksal olabilir. Fiziksel varlıklar somut nesneleri, mantıksal varlıklar ise bilgileri veya verileri temsil eder. Saldırılar ise kasıtlı veya kasıtsız eylemlerdir ve bilgilere veya sistemlere zarar verebilir. Saldırılar farklı tiplerde olabilir ve doğrudan veya dolaylı olarak gerçekleştirilebilir. Önemli olan, varlıkların korunması için gerekli önlemlerin alınması ve saldırıların engellenmesidir.

Saldırı, kasıtlı veya kasıtsız olarak bilgilere veya onları destekleyen sistemlere zarar verme veya tehlikeye atma eylemidir. Saldırılar aktif veya pasif, doğrudan veya dolaylı olabilir. Örneğin, saldırganın doğrudan bilgi sistemlerine erişmeden açık kaynaklar üzerinden hassas bilgilere erişmesi pasif bir sal-

dırıdır, bilgi sistemlerine izinsiz erişerek hassas bilgilere erişmesi ise kasıtlı bir saldırıdır. Saldırılar, doğrudan bir tehdidin eylemlerinden kaynaklanabileceği gibi güvenlik açığı bulunan bir sistem veya başka bir kaynak üzerinden de dolaylı olarak gerçekleşebilir.

Kontrol, koruma, önlem terimleri, saldırılara karşı koyma, riski azaltma ve güvenlik açıklarını çözebilme yeteneklerini ifade eder. Kontroller, bir kuruluşun güvenlik mekanizmalarını, politikalarını ve prosedürlerini içeren önlemlerdir. Bu kontroller, bir organizasyonun güvenlik duruşunu güçlendirir ve güvenlik açıklarını ele alarak bilgi varlıklarını koruma altına alır.

Tehdit, bir varlık veya sistem için potansiyel tehlike oluşturan nesneleri, olayları veya durumları ifade eder. Tehditler, bilgileri veya bilgi sistemlerini zarar vermek, çalmak, bozmak veya erişimini engellemek amacıyla kasıtlı veya kasıtsız olarak kullanabilecek olan potansiyel tehlikelerdir. Tehditler, farklı kaynaklardan gelerek çok çeşitli olabilir. Örneğin, kötü niyetli kullanıcılar, bilgisayar korsanları, virüsler, kötü amaçlı yazılımlar, doğal afetler, hatalı kullanıcı davranışları veya güvenlik açıkları gibi unsurlar birer tehdit oluşturabilir.

Saldırıya açıklık veya zafiyet, bir sistemde veya koruma mekanizmasında saldırıya veya zarara yol açabilecek bir zayıflık veya hata durumudur. Bir yazılımsal eksikten veya iyi yapılandırılmamış özellikten kaynaklanan güvenlik açıkları ve zafiyetler bulunabilir. Güvenlik açıkları, yazılım hataları, korumasız sistem bağlantı noktaları veya kilidi açık bir kapı gibi örneklerle ortaya çıkabilir. Bazı güvenlik açıkları belgelenmiş ve yayınlanmışken, diğerleri henüz keşfedilmemiş olabilir.

Diğer önemli kavramlar arasında açıklardan yararlanan yazılım, maruz kalma, kayıp/zarar, koruma profili ve risk bulunur. Açıklardan yararlanan yazılım, bir sistemi tehlikeye atmak için kullanılan teknikleri ifade ederken, maruz kalma yetkisiz bir kişi veya sistem tarafından güvenlik açığından yararlanılması durumunu ifade eder. Kayıp veya zarar, bir bilgi varlığının zarar görmesi, değiştirilmesi veya ifşa edilmesidir. Koruma profili veya güvenlik duruşu, bir organizasyonun güvenlik politikaları, eğitim, teknoloji ve kontrolleri içeren tüm güvenlik önlemlerini ifade eder. Risk ise istenmeyen bir olayın olma olasılığını ifade eder ve kuruluşlar riski en aza indirerek bilgi varlıklarını korumayı hedefler.

3. Bilgi Güvenliği Yönetim Sistemi

Bilgi; kurum, kuruluş ve şirketler için her zaman önemli bir varlık olmuştur ve bu varlığın korunması gerekmektedir. Günümüzde, çoğu bilgi dijital olarak depolanmakta, erişimi kolaylaştırmak ve arşivleme süresini en aza indirmek için bilgiye çevrimiçi erişilebilmektedir. Ancak bunun bir dezavantajı vardır: tüm bu bilgiler önemine göre çeşitli risk ve tehditlere maruz kalabilir (Mishra, 2015). Gizli veya hassas bilgilere yönelik siber saldırılar yıllar içinde artış göstermiştir. Bir şirketin büyümesi onu siber saldırılar için daha çekici bir hedef hâline getirebilir ve bilgi sızıntısı şirketin itibarına, gelirine ve güvenilirliğine zarar verebilir (Sen, Verma ve Heim, 2020). Bu bağlamda her kurum, kuruluş ve şirket için bir bilgi güvenliği yönetim sisteminin (BGYS) kurulması zorunludur. Her müşterinin/kişinin, paylaşılan bilgilerin güvenli ve doğru bir şekilde yönetildiğini bilmesi gerekir.

3.1. ISO/IEC 27001

ISO 27000 ailesine ait olan ve ISO/IEC 17799 standardının yerini alan ISO/IEC 27001 standardı, bilgi güvenliği yönetimini geliştirmek için tasarlanmış bir bilgi güvenliği standardıdır. Türk Standartları Enstitüsü (TSE) tarafından Türkçe'ye çevrilen ve teknik olmayan ISO/IEC 27001, kurum, kuruluş ve şirketlerin güvenlik gereksinimlerini tanımlar, ancak uygulama görevini kurum, kuruluş ve şirketlere bırakır. Standart temel olarak verilerin dâhili veya harici şekilde kötüye kullanımdan korumak için gereklilikleri belirtir. TSE tarafından yayınlanan TS ISO/IEC 27001 standardının derlenmesindeki amaç; bir bilgi güvenliği yönetim sistemi (BGYS) oluşturmak, uygulamak, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için bir model ortaya çıkarmaktır.

Uluslararası Standardizasyon Organizasyonu (ISO) 27001, herhangi bir risk için başa çıkma mekanizmalarını tanımlayan, değerlendiren ve öneriler sunan bir yönetim sistemidir. Bir kurum ve kuruluşun ihtiyaçlarına göre etkili bir BGYS geliştirilmesi için rehberlik sağlamaktadır. Bir BGYS'nin uygulanması, bilgi güvenliği riskleri ve tehditleriyle daha iyi başa çıkmak için stratejilerin geliştirilmesi ve sonunda ISO 27001 ile uyumlu bir BGYS kurulması gerektiği anlamına gelir. ISO 27001 standardı, koşulları gerçekleştirmek için özel prosedürler belirtmez, içerisinde bilgi güvenliğini sağlamak adına verilen gereklilikler geneldir ve her kurum kendi teknolojisine özgü olarak güvenlik sağlama sürecini yürütmelidir (Disterer, 2013). ISO/IEC 27001 standardı bir çerçeve-

dir ve büyüklüğü, çalışan sayısı, faaliyet alanı, organizasyon yapısı ne olursa olsun her organizasyonda uygulanabilir.

Standart, BGYS'nin etkin işleyişini sürdürmek amacıyla algoritma ve metodoloji için gereklilikleri ve ayrıca izleme faaliyetlerinin sistematik organizasyonu ve yönetim sisteminin sürekli iyileştirilmesi için gereklilikleri tanımlar. ISO/IEC 27001 uyarınca, BGYS'nin gereklerini yerine getirirken ve uygularken, BGYS kapsamı dikkate alınarak kuruluşu etkileyen tüm faktörlerin dikkate alınması gerekmektedir. ISO/IEC 27001 gereksinimlerine uygun olarak BGYS geliştirme ve uygulama süreci, mevcut yönetim sistemlerinin denetimleri, programların ve uygulama algoritmalarının geliştirilmesi, süreçleri açıklayan yerel düzenleyici belgelerin geliştirilmesi ve uygulanması ile ilgili aşamaları içerir. Risk yönetim sisteminin oluşturulması, süreçlerin kurulması ve izlenmesi, sistemin iç denetim programının yönetilmesi, üst yönetim tarafından BGYS'nin analizi de BGYS uygulama sürecine dâhildir. 50 kişiye kadar olan küçük kuruluşlar, BGYS'nin uygulanması için yalnızca bir çalışma grubunun seferber edilmesini değil, kuruluşun tüm çalışanlarının katılımını gerektirir (Aleksandrov, Vasiliev ve Aleksandrova, 2021).

ISO 27001' de ana bölüm 11 maddeyi içerir ve Ek A olarak adlandırılan alt bölüm, güvence görevi görecek 93 güvenlik kontrolünün yönergelerini içerir. 0'dan 10'a kadar numaralandırılmış 11 madde giriş, kapsam, normatif referanslar, terimler ve tanımlar, kuruluşun bağlamı, liderlik, planlama, destek, operasyon, performans değerlendirme, iyileştirmedir ve 0'dan 3'e kadar olan maddeler giriş, kapsam, referanslar, terimler ve tanımları içerir. Kalan maddeler (4 ila 10), ISO 27001 için zorunlu gereksinimlerdir ve bir kuruluşun bir ISO 27001 sertifikasına ihtiyacı varsa, tüm bu zorunlu gereksinimleri yerine getirmeli ve sürdürmelidir. Madde 4, organizasyonun bağlamını, organizasyonel ihtiyaçları ve beklentileri anlamak ve onu yönetmek için BGYS kapsamını belirlemekle ilgilidir. Madde 5, her bir otoritenin rollerini ve sorumluluklarını tanımlayarak tamamen liderlik ve onun taahhüdü ve politikası ile ilgilidir. Bir sonraki madde, riski değerlendirerek ve uygun tedaviyi uygulayarak risk ve fırsatları ele alacak planlamadır. Madde 8, operasyonel planlama ve risk değerlendirmesi ve risk işleme kontrolü için operasyon olarak belirtilir. Bir sonraki madde, iç denetim için performans değerlendirmesi, değerlendirmenin gözden geçirilmesi ve izlenmesidir. Bir kuruluş, iyileştirme olarak bilinen son maddede tanımlanan çevik (agile) ortama uymak için her zaman iyileştirmeye ve düzeltici eyleme ihtiyaç duyar (Junaid, 2022).

BGYS'nin etkin işleyişini sağlamak için, geliştirme için bir rehber olarak ISO 27000 serisi standartlarının kullanılması tavsiye edilir. BGYS'yi uygula-

maya yönelik metodoloji ISO 27001 Standardı için klasik Planla (Plan) - Uygula (Do) - Kontrol Et (Check) - Önlem Al (Action) (PDCA) modeline dayanmaktadır. BGYS'nin kalitesi, PDCA döngüsünü izleyerek zaman geçtikçe artacaktır. Zorunlu maddeler 4, 5, 6 (organizasyon bağlamı, liderlik, planlama), BGYS'nin kurulması ile Plan aşamasına girer. BGYS'nin uygulanmasının, zorunlu 7 ve 8. maddeleri kapsayan Uygulama aşamasına kadar tamamlanması gerekir. Kontrol aşaması, zorunlu 9. maddeyi (performans değerlendirmesi) yerine getirmek için BGYS'nin izlenmesini ve gözden geçirilmesini ele alır. Döngünün son kısmı, madde 10'a (iyileştirme) uygun olarak BGYS'nin sürdürülmesi ve iyileştirilmesi ile ilgilidir.

3.1.1. Planlama

Bilgi Güvenliği Yönetim Sisteminin ISO/IEC 27001'e göre planlanması şunları gerektirir: Kuruluş riskleri ve potansiyellerini tanımlamalı ve yönlendirmelidir. Bilgi güvenliği amacıyla, riskin işlenmesinde elde edilen sonuçlara dikkat edilmelidir (Stefanova-Stoyanova ve Danov, 2022).

3.1.2. Uygulama

BGYS ile ilgili olarak, ISO/IEC 27001 şu maddeleri içerir: Kuruluş, BGYS ile ilgili paydaşları belirlemelidir; Kuruluş, bilgi güvenliği risk değerlendirmelerinin sonuçlarına ilişkin belgelenmiş bilgileri tutmalıdır; Kuruluş, riski tanımlarken, risk kaynaklarını, etki alanlarını, olayları ve bunların nedenlerini ve bunların potansiyel sonuçlarını tanımlamalıdır; Bilgi güvenliği risklerini belirlemek için Bilgi güvenliği yönetim sistemi içindeki bilgilerin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin kaybıyla ilgili riskleri belirlemek için bilgi güvenliği risk değerlendirme süreci uygulanmalıdır; Bilgi güvenliği risk yönetiminden elde edilen sonuçlar raporlara yansıtılmalı ve ISO 27001 dokümantasyonuna uygun şekilde saklanmalıdır; Risk yönetimi sürecinin önemli bir aşaması da rutin izleme, önceden planlanmış kontroller, düzenli teftiş veya gözetimi içermektedir

3.1.3. Kontrol Etme

Üst yönetim, uygunluğunu ve geçerliliğini sağlamak için kuruluşun BGYS' sini önceden belirlenmiş tarihlerde incelemelidir. Yönetimin gözden geçirmesi, tehdit değerlendirmesinin etkilerinin ve risk yönetim planının derecelendirilmesinin gözden geçirilmesini içerir.

3.1.4. Önlem Alma

Kuruluş, bilgi güvenliği yönetim sisteminin uygunluğunu, yeterliliğini ve etkinliğini sürekli iyileştirmelidir. Bir uygunsuzluk oluştuğunda, kuruluş uygunsuzluğa tepki vererek kontrol altına almak ve düzeltmek için eyleme geçmelidir. Durumun getirdiği sonuçlarla ilgilenmeli ve uygunsuzluğun tekrar etmemesi veya başka bir yerde meydana gelmemesi için uygunsuzluğun nedenlerini ortadan kaldıracak eylem ihtiyacını değerlendirmelidir.

4. Bilgi Güvenliği Tedbirleri

Bilgi Güvenliği elektronik ve/veya fiziksel olarak bulunan verinin işlenmesi, aktarılması ve saklanması süreçlerinin tamamının kapsamaktadır. Bilgi Güvenliği için öncelikli olarak "varlık"ların tanımlanması gerekmektedir. Bilgi Güvenliği açısından "varlık" elektronik ve/veya fiziksel olarak bulunan, iletişim altyapıları ile aktarılabilen, ilgili taraflarca değer taşıyan, bilgiyi kullanan, taşıyan ve barındıran fiziksel mekânlar olarak tanımlanmaktadır (CBDDO, 2020). Bilgi güvenliği tedbirleri, bir organizasyonun veya bireyin bilgilerini korumak ve güvende tutmak için alınan önlemleri ifade eder. Bu tedbirler, bilgilerin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamayı amaçlar. Bilgi güvenliği tedbirleri, farklı alanlarda uygulanabilir ve çeşitli yöntemleri içerebilir. Bunlar arasında fiziksel güvenlik önlemleri (örneğin, güvenlik kameraları, erişim kartları, kilitli odalar), ağ güvenliği önlemleri (örneğin, güvenlik duvarları, saldırı tespit sistemleri, şifreleme), yazılım güvenliği önlemleri (örneğin, güvenlik yamaları, güçlü parola politikaları, oturum açma doğrulama) ve kullanıcı eğitimi yer alır. Bilgi güvenliği tedbirleri, potansiyel tehditlere karşı koruma sağlamak, saldırıları tespit etmek ve durdurmak, veri kaybını önlemek ve iş sürekliliğini sağlamak için önemli bir rol oynar. Her organizasyon veya birey, bilgi güvenliği politikaları ve prosedürleri oluşturarak, uygun tedbirleri alarak ve sürekli olarak güvenlik durumunu değerlendirerek bilgilerini korumaya odaklanmalıdır.

4.1. Ağ ve Sistem Güvenliği

Bilgi Güvenliği Yönetim sisteminde fiziksel ve dijital sistemlerin ve uygulamaların bilgilerini korumak için ağlar yönetilmeli ve kontrol edilmelidir (Disterer, 2013). Kuruluş, herhangi bir bilgiyi korunduğundan emin olmak için uygun yöntemleri kullanmalıdır. Ağın güvenlik kontrolleri dikkatli bir şekilde ele almalı, uygun şekilde ve orantılı olarak tasarlanmalı ve iş gereksinimlerine,

risk değerlendirmesine, sınıflandırmalara ve uygun şekilde ayırma gereksinimlerine göre uygulanmalıdır.

Bilginin güvenliğinin sağlanması için teknik kontroller Ağ bağlantı kontrolü ve uç noktaların doğrulaması, güvenlik duvarları ve saldırı tespit/önleme sistemleri, erişim kontrol listeleri ve fiziksel, mantıksal veya sanal ayrımları içerebilir. Genel ağlara veya kurumsal kontrol dışındaki diğer kuruluşların ağlarına bağlanırken, risk seviyelerinin arttığını dikkate almak ve bu riskleri uygun şekilde ek kontrollerle uygulamak da önemlidir (Koca ve ark., 2021).

Ağ hizmetlerini güvence altına almak için aldığı tüm güvenlik önlemlerini ağ hizmetleri anlaşmalarına dâhil etmelidir. Yönetici, personel, müşteri ve misafir ağları birbirinden izole edilmelidir. Ağların fiziksel veya mantıksal alt ağlara bölünmesi, kullanıcı doğrulaması yapmayan kullanıcıların ağa dâhil edilmemesi, ağın saldırı tespit sistemlerine ilaveden izlenmesi ve alarmların koralesyonlarıyla birlikte değerlendirilmesi gerekmektedir. Ağ üzerinde en az üç ayda bir iç ve altı ayda bir dış paydaşlarla güvenlik testleri yapılmalıdır.

4.2. Uygulama ve Veri Güvenliği

Bilgi sistemleri üzerinde bireysel ve kurumsal ihtiyaçlar için birçok uygulama kullanılmaktadır. Bu uygulamaların yerleşik ve bulut sistemleri üzerinde yer alması açısından farklı avantaj ve güvenlik riskleri bulunmaktadır. Yerel cihaz veya ağ üzerinde kullanılan uygulamalar dış dünyadan gelen saldırılara karşı daha güvenli olmasına karşın iç ağda oluşabilecek saldırgan veya yetkisiz erişim durumlarına karşı genellikle savunmasızdır. Bulut sistemleri üzerinde yer alan uygulamalar genellikle iyi yapılandırılmış olmasına karşın hatalı konfigürasyonlar dolayısıyla yetkisiz erişim veya kurum içi yetkilendirme hatalarıyla karşılaşılabilmektedir. Ayrıca bulut sistemlerinde çalışan uygulamalar özellikle bir güvenli sanal özel ağ (VPN) ve beyaz liste gibi koruma yöntemleri ile kullanılmıyorsa olası bir zafiyetin etki derecesi yüksek olmaktadır. Uygulama güvenliği için kimlik doğrulama, oturum yönetimi ve yetkilendirme temel güvenlik seviyeleridir. Yetkili ve son kullanıcılar periyodik olarak kontrol edilmeli ve yetki matrisleri çıkarılmalıdır. Uygulamaların yetkilendirme ve doğrulama olmadan herhangi bir bilgi/dokümanı/kullanım kılavuzu dışarı sağlamamalıdır. Uygulamalar üzerinde varsayılan kullanıcılar bulundurulmamalıdır. Dosyaların ve kaynakların yerel ağ üzerinde bile yetkisiz paylaşılması engellenmelidir. Uygulamaların güvenli kurulum ve doğru yapılandırmanın yapıldığından emin olunmalı, yedek ve tekrar kurulumlar için dosya, sistem,

ağ ve kullanıcı yetki matrisleri çıkarılmalıdır. Kurum içi geliştirilen uygulamaların güvenli yazılım geliştirme süreçlerinin uygulanması sağlanmalı güncel veritabanı uygulamaları kullanılmalıdır. Kayıt yönetimi açısından yalnızca tutulması gereken bilgiler kaydedilmeli ayrıca verilerin görüntülenmesi de yetkilendirilmesidir. Olası felaket senaryoları değerlendirilmeli ve alınması gereken aksiyonlar belirlenmelidir. Uygulamalara erişim için güvenli iletişim protokolleri tercih edilmelidir. Kötücül, sahte ve hatalı işlemler izlenmeli ve sisteme zarar verme ihtimali olan işlemleri engellemelidir. Üçüncü taraflardan alınan ve verilen servisler doğrudan veritabanı üzerinden değil programlama arayüzü (API) üzerinden sağlanmalı ve mutlaka işlem kayıt defterleri tutulmalıdır.

4.3. Cihaz ve Ortam Güvenliği

Kurum çalışanlarının bilgisayar, tablet ve telefon gibi taşınabilir cihazları ile basılı kopya, taşınabilir bellek gibi taşınabilir ortam gruplarını içeren bu tür varlıkların cihaz ve ortam güvenliği kapsamında risk değerlendirmesinin yapılması gerekmektedir. Özellikle taşınabilir cihazların kurum dışına çıkışında kayıt tutulması, düzenli yedek alınması ve cihaz ve ortamların şifrelenmesi kayıp ve çalıntı durumlarına karşı temel güvenlik önlemleri olarak görülmektedir. Kullanılan mobil cihazları mutlaka kullanıcı bazında hesap oluşturularak parola tanımlayarak kullanılması gerekmektedir. Bu cihazların kurum dışında şahsi amaçlarla kullanılmamalı ve içerisine personel ile ilgili kişisel bilgi konulmamalıdır. Herhangi bir amaçla yazılım lisansı bulunmayan yazılımlar kurulmamalı ve işletim sistemi ve yüklü uygulamalar güncel tutulmalıdır. Halka açık veya ağa kimlerin bağlandığı bilinmeyen kablosuz ağ hizmetlerine cihazları bağlanmamalıdır. Cihaz ve ortamların kullanım ömrünü tamamlaması veya ikinci el olarak satılması durumunda güvenli silme prosedürleri uygulanmalı mümkün olmayan durumlarda cihaz ve ortamlar imha edilmelidir.

4.4. Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği

Kurumsal ortamlarda kullanılan akıllı beyaz eşya, akıllı sensör, IP kamera vb. cihaz grupları Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği çerçevesinde değerlendirilmelidir. IoT cihazları kurulum yetkilendirme aşamasında varsayılan parola bulundurulmamalıdır. Her bir personel için ayrı kullanıcı tanımlanmalı üzerine tanımlanan kullanıcıların yetkilendirilmesi yapılmalıdır. Özellikle üretici ve tedarikçi servis/güncelleme desteği bulunmayan cihazlar

tercih edilmemelidir. Bu cihazlar kısıtlı kaynaklarla çalıştığı için güvenli bir iletişim altyapısı kullandığından emin olunmadığı sürece internete bağlanmamalıdır. Cihaz üzerinde bulunan üçüncü taraf servisler ve programlama arayüzlerinin güvenli bağlantı protokolleri kullandığından emin olunmalıdır. Özellikle üzerinde çalışan servisler kontrol edilmeli özellikle bir botnet parçası olması durumunda alınması gereken tedbirler belirlenmelidir. Bu cihazlar çalınması, fiziksel ya da uzaktan saldırganın müdahalesine açık hâle gelmesi durumunda alınacak tedbirler ve riskler belirlenmelidir.

4.5. Kritik Altyapılar Güvenliği

Kritik altyapı güvenliği, yaşamsal öneme sahip olan enerji, su, iletişim, ulaşım, finans, sağlık ve hükûmet gibi sistemlerin güvenliğini sağlama disiplinidir. Bu sistemlerin zarar görmesi veya hedef alınması ciddi sonuçlara yol açabilir. Kritik altyapı güvenliği, fiziksel ve siber güvenlik önlemleri, erken tehdit algılama, yedekleme ve kurtarma planları gibi tedbirleri içerir. Kritik altyapıların güvenliği sürekli izleme ve iyileştirme gerektiren dinamik bir süreçtir. Bir kurumun doğrudan bir kritik altyapı olarak değerlendirilmesi veya bünyesinde bir kritik altyapı bulundurması durumunda sistem güvenliğini ve risk değerlendirmesini sıfır kesinti üzerine planlaması gerekmektedir (TCUAB, 2017). Bu durumda olası bilgi güvenliği açısından risk teşkil edecek gerektiğinde kapatılabilecek hizmetlerin kritik altyapılardan ayrıştırılması gerekmektedir (Kıran ve Soğukpınar, 2021).

4.6. Personel Güvenliği

Kurum bünyesinde görev yapan personel/uzman grupları eğitim ve görevlerine göre gruplandırılması yapılmalı fiziksel ve dijital verilere erişimleri görev ve sorumluluklarına göre sınırlandırılmalıdır. Personel parola seçimi, erişim matrisi bilgilendirmesi, güvenli sosyal medya ve e-posta kullanımı gibi genel güvenlik tedbirleri hakkında bilgilendirilmelidir. Periyodik olarak eğitim ve farkındalık çalışmaları yürütülmeli, rastgele zaman ve senaryolarda sosyal mühendislik tatbikatları yapılmalı ve sonuçlar paylaşılmalıdır.

4.7. Fiziksel Mekânların Güvenliği

Bilgi güvenliği, yalnızca dijital ortamları değil, fiziksel ortamları da kapsar. Fiziksel ortamın güvenliği, bir organizasyonun bilişim altyapısının ve de-

ğerli varlıklarının korunmasında kritik bir rol oynar. Fiziksel güvenlik önlemleri, binaların, ofislerin, veri merkezlerinin ve diğer tesislerin güvenliğini sağlamayı amaçlar. Fiziksel ortamların güvenliği, yetkisiz erişim, hırsızlık, sabotaj veya doğal afetler gibi tehditlere karşı korumayı hedefler. Kurum kontrolünde olan mekânların 24 saat kamera kaydının alınması ve gerektiğinde bu kayıtların incelenebilmesi gerekmektedir. Ortamlara fiziksel erişim kontrol altına alınmalı ve raporlanmalıdır. Sunucu odası ve fiziksel evrakların erişimi kilitli olarak güvenlik altına alınmalı olası bir felaket durumunda kurtarma senaryoları belirlenmelidir. Kablosuz ağ hizmetinin bina dışından erişilmesinin engellenmesi tavsiye edilmektedir. Ayrıca açıkta kablolu ağ erişim ucu bırakılmamalı ve mac üzerinden beyaz liste çalışması yapılmalıdır.

4.8. Kişisel Verilerin Güvenliği

Kurumlar yasal olarak bulundukları ve sorumlu oldukları kişisel verileri koruma regülasyonları şartlarına uymakla yükümlüdür. Ayrıca hizmet verdikleri başka ülkelerdeki regülasyonlara da müşterileri dolayısıyla dâhildirler. Bu sebeple bulundukları ülkedeki sorumlulukları yanında hizmet verdikleri müşterilerinin bulunduğu ülkedeki regülasyon gerekliliklerini de sağlamalıdırlar. Kişisel Verileri Koruma Kanunu çerçevesin de müşterilerden toplamakla yükümlü oldukları açık rıza onaylarını gerektiğinde satabilmeleri için yedekli bir şekilde saklamaları gerekmektedir. Ayrıca müşterileri ve personelleri ile ilgili tuttukları verileri sınıflandırmalı kişisel veri olan verileri ayrıca hangi personelin ne süre ile erişebileceğini belirlemelidir. Personellere kişisel veri farkındalığı eğitimleri verilmeli olası ihlallerde bildirim kanalları aktif olarak kullanılmalıdır. Ayrıca gerektiğinde kişisel verilerin silme ve imha süreçleri planlanmalı olası kullanım ve felaket senaryoları belirlenmelidir.

5. Sonuç ve Öneri

Bilgisayarlar, telefonlar veya sensörler gibi çeşitli kaynaklardan her gün önemli miktarda veri üretilmekte ve farklı bir ifadeyle veri devrimi çağı yaşanmaktadır. Bu duruma bağlı olarak operasyon kesintilerinin oluşması, hassas verilerin kaybolması veya tehlikeye atılması, ürün veya hizmetlerin kalitesine ve hatta fiziksel mülkiyete zarar verilmesi gibi gelişen teknolojiler ve artan veriler üzerinde büyük etkisi olan siber saldırılar artış göstermektedir. Bu siber tehditlerle mücadele etmek için kuruluşlara yönelik, bilgisayar saldırıla-

rına karşı koymayı veya bunları azaltmayı amaçlayan siber güvenlik kontrolleri, normları ve standartları belirlenmeli ve uygulanmalıdır.

Devletin, kurum/kuruluşların ve toplumun birçok faaliyet alanında bilgisayar ve internet teknolojilerinin uygulanması, yönetim süreçlerinin otomasyonu ve gerçekleştirilen hizmetlerin etkinliğinin artmasını sağlamaktadır. Aynı zamanda birçok sektörde bilgisayar/internet teknolojilerinin kullanılmaya başlanması, gerçekleştirilen hizmetlerin güvenliğinin sağlanması gerekliliğini de beraberinde getirmektedir. Bu nedenle kurum ve kuruluşlarda, bilgi kaynaklarının güvenliğini sağlamak ve kurum misyonunun kesintisiz olarak gerçekleşmesini sağlamak için Bilgi Güvenliği Yönetim Sistemi (BGYS) uygulanmaktadır. BGYS, bir dizi planlama ve organizasyonel taahhüdü kapsar ve kurum/kuruluş veya devlet işleyişi üzerinde olumsuz etkisi olabilecek bilgi tehditlerinin risk yönetimine dayanır. Bu nedenle bilgi güvenliği yönetimi, gerçekleştirilen görevlerin etkinliğini, güvenilirliğini ve kalitesini etkiler.

Bir Bilgi Güvenliği Yönetim Standardı olan ISO 27001, Bilgi Güvenliği Yönetim Sistemi kavramını tanımlar ve dört temel aşamaya (Planla, Uygula, Doğrula ve Önlem Al) dayalı yapılandırılmış bir çalışma metodolojisi geliştirerek, bilgiye erişilebilirliği yöneten bir dizi sürecin yürütülmesini sağlar. Veri güvenliğinin sürekli olarak gözden geçirilmesi, denetlenmesi ve yönetilmesi, ilgili süreçlerde sürekli bir iyileştirme eğilimi gösterir. Siber saldırılar geliştikçe, bilgilerin korunduğu prosedürler de gelişmeli, uyarlanmalı veya güncellenmelidir.

Sonuç olarak bu çalışma kapsamında bilgi güvenliği kavramı incelenmiş olup sahada yaygın olarak kullanılan ISO/IEC 27001 bilgi yönetim sistemi açıklanmıştır. Bilgi sistemi ortamlarında farklı bilgi güvenliği varlıkları ve varlık grupları için bilgi güvenliği tedbirleri açıklanmıştır. Bilgi varlıklarını korunması için teknik tedbirler kadar idari süreçlerinde önemlidir ve kurumun bir bütün olarak değerlendirildiğinde siber risklerin yönetebilir.

Kaynaklar

Aleksandrov, M. N., Vasiliev, V. A., & Aleksandrova, S. V. (2021, September). Implementation of the risk-based approach methodology in information security management systems. In *2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)* (pp. 137-139). IEEE.

Ali, S. E. A., Lai, F. W., Hassan, R., & Shad, M. K. (2021). The long-run impact of information security breach announcements on investors' confidence: The context of efficient market hypothesis. *Sustainability*, *13*(3), 1066.

Chen, L., Zhen, J., Dong, K., & Xie, Z. (2020). Effects of sanction on the mentality of information security policy compliance. *Revista Argentina de Clinica Psicologica*, *29*(1), 39.

Chopra, A., & Chaudhary, M. (2020). Implementing an Information Security Management System. *Apress, New York*.

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CBDDO) (2020). Bilgi ve İletişim Güvenliği Rehberi. https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg_rehber.pdf

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, *4*(2).

Junaid, (2022) T. S. ISO 27001: Information Security Management Systems.

Kıran, E. & Soğukpınar, İ. (2021). Kritik Altyapılarda Siber Risk Analizi ve Yönetimi. Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, 14 (1), 15-33. DOI: 10.54525/tbbmd.649913

Kissel, R. (Ed.). (2011). *Glossary of key information security terms*. Diane Publishing.

Koca, M., & Avcı, İ. (2023). Siber güvenlik yönetim sistemi. In Mühendislik Alanında Uluslararası Araştırmalar Sayfalar (s. 163-183). Platanus Publishing. ISBN: 978-625-6971-54-7, doi: 10.5281/zenodo.7744333.

Koca, M., Aydin, M. A., SERTBAŞ, A., & Zaim, A. H. (2021). A new distributed anomaly detection approach for log IDS management based ondeep learning. Turkish Journal of Electrical Engineering and Computer Sciences, 29(5), 2486-2501. doi: 10.3906/elk-2102-89

Mishra, S. (2015). Organizational objectives for information security governance: a value focused assessment. *Information & Computer Security*, *23*(2), 122-144.

Rehak, D., Bernatik, A., Dvorak, Z., & Hromada, M. (Eds.). (2020). *Safety and Security Issues in Technical Infrastructures*. IGI Global

Sen, R., Verma, A., & Heim, G. R. (2020). Impact of cyberattacks by malicious hackers on the competition in software markets. *Journal of Management Information Systems*, *37*(1), 191-216.

Stefanova-Stoyanova, V., & Danov, P. (2022, May). Comparative Analysis of Specialized Standards and Methods on Increasing the Effectiveness and Role of PDCA for Risk Control in Management Systems. In *2022 10th International Scientific Conference on Computer Science (COMSCI)* (pp. 1-4). IEEE.

T.C. Ulaştırma ve Altyapı Bakanlığı (TCUAB), (2017) Ulaştırma ve Kritik Altyapı Bilgi Sistemleri için Asgari Güvenlik Önlemleri Dokümanı

Türkiye İstatistik Kurumu TUİK, Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması, Ağustos 2022.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security*. Cengage learning.