TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANABİLİM DALI
YÖNETİM VE STRATEJİ TEZSİZ YÜKSEK LİSANS PROGRAMI

BİLGİ GÜVENLİĞİ SİSTEMLERİ: RİSK YÖNETİMİNE STRATEJİK BİR YAKLAŞIM

Tezsiz Yüksek Lisans Dönem Projesi

Diclehan ALTINÖZ

Ankara,2025

TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANABİLİM DALI
YÖNETİM VE STRATEJİ TEZSİZ YÜKSEK LİSANS PROGRAMI

BİLGİ GÜVENLİĞİ SİSTEMLERİ: RİSK YÖNETİMİNE STRATEJİK BİR YAKLAŞIM

Tezsiz Yüksek Lisans Dönem Projesi

Diclehan ALTINÖZ

Proje Danışmanı
Dr. Öğr. Üyesi Özgür ATEŞ

Ankara,2025

T.C.
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜ
DÖNEM PROJESİ DEĞERLENDİRME FORMU

Sosyal Bilimler Enstitüsü Müdürlüğü'ne,

Enstitünüz İşletme Anabilim Dalı 23982221 numaralı tezsiz yüksek lisans öğrencisi Diclehan ALTINÖZ' ün "Bilgi Güvenliği Sistemleri: Risk Yönetimine Stratejik Bir Yaklaşım" adlı ("Informatıon Securıty Systems: A Strategıc Approach To Rısk Management") tezsiz yüksek lisans dönem projesi tarafımca değerlendirilmiş olup,

BAŞARILI ■

BAŞARISIZ □

bulunmuştur.

Dönem projesi danışmanı olarak, adı geçen öğrencinin notunun, dönem projesinin Enstitünüz Müdürlüğü'ne tesliminden önce *Öğrenci İşleri Bilgi Sistemi*'ne (OİBS) tarafımdan işlendiğini beyan ederim.

DÖNEM PROJESİ DANIŞMANI ONAYI

30/06/2025

Dr. Öğr. Üyesi Özgür ATEŞ

TÜRKİYE CUMHURİYETİ

ANKARA ÜNİVERSİTESİ

Sosyal Bilimler Enstitüsü Müdürlüğü'ne,

Dr. Öğr. Üyesi Özgür ATEŞ danışmanlığında hazırladığım **"Bilgi Güvenliği Sistemleri: Risk Yönetimine Stratejik Bir Yaklaşım (Ankara, 2025) "** adlı dönem projesindeki bütün bilgilerin akademik kurallara ve etik davranış ilkelerine uygun olarak toplanıp sunulduğunu, başka kaynaklardan aldığım bilgileri metinde ve kaynakçada eksiksiz olarak gösterdiğimi, çalışma sürecinde bilimsel araştırma ve etik kurallarına uygun olarak davrandığımı ve aksinin ortaya çıkması durumunda her türlü yasal sonucu kabul edeceğimi beyan ederim.

30/06/2025

Diclehan ALTINÖZ

İÇİNDEKİLER

KISALTMALAR LİSTESİ

Bu çalışmada kullanılmış kısaltmalar, açıklamaları ile birlikte sunulmuştur.

Kısaltma	Açılımı
AI	Artificial Intelligence (Yapay Zeka)
BDDK	Bankacılık Düzenleme ve Denetleme Kurumu
BGYS	Bilgi Güvenliği Yönetim Sistemi
CSA	Cyber Security Agency (Siber Güvenlik Ajansı)
DORA	Digital Operational Resilience Act (Dijital Operasyonel Dayanıklılık Yasası)
DPIA	Data Protection Impact Assessment (Veri Koruma Etki Değerlendirmesi)
EHR	Electronic Health Record (Elektronik Sağlık Kaydı)
GDPR	General Data Protection Regulation (Genel Veri Koruma Tüzüğü)
IBM	International Business Machines Corporation (Uluslararası İş Makineleri Şirketi)
IoT	Internet of Things (Nesnelerin İnterneti)
ISO	International Organization for Standardization (Uluslararası Standardizasyon Örgütü)
IVR	Interactive Voice Response (Etkileşimli Sesli Yanıt Sistemi)
KVKK	Kişisel Verilerin Korunması Kanunu
MFA	Multi-Factor Authentication (Çok Faktörlü Kimlik Doğrulama)
NIST	National Institute of Standards and Technology (Ulusal Standartlar ve Teknoloji Enstitüsü)
PCI-DSS	Payment Card Industry Data Security Standard (Ödeme Kartı Endüstrisi

Kısaltma	Açılımı
	Veri Güvenliği Standardı
SIEM	Security Information and Event Management (Güvenlik Bilgisi ve Olay Yönetimi)
SOC	Security Operations Center (Güvenlik Operasyon Merkezi)
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UEBA	User and Entity Behavior Analytics (Kullanıcı ve Varlık Davranış Analizi)
X-Road	Veri paylaşımı için entegre Estonya devlet ağı
Zero Trust	Güvenilmeyen varsayımı esas alan siber güvenlik modeli

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

GİRİŞ

Bilgi, günümüz dünyasında yalnızca bir veri kümesi olmaktan çıkmış; ekonomik değeri olan, stratejik bir varlık olarak kurumların en önemli sermaye unsurlarından biri haline gelmiştir (Çetinkaya, 2008). Dijital dönüşüm sürecinin ivme kazanmasıyla birlikte; bulut bilişim, yapay zeka, büyük veri, mobilite ve nesnelerin interneti (IoT) gibi teknolojilerin iş süreçlerine entegrasyonu bilgi üretimini ve kullanımını önemli ölçüde artırmış; ancak bu durum aynı zamanda kurumları bilgi güvenliği açısından daha karmaşık ve çok katmanlı tehditlerle karşı karşıya bırakmıştır (Gencer, 2015). Bu gelişmeler ışığında, bilgi güvenliği yalnızca teknik bir mesele olmanın ötesine geçerek, yönetsel ve stratejik düzlemde ele alınması gereken çok boyutlu bir konu haline gelmiştir (Demirtaş, 2013).

Kurumlar artık yalnızca dış tehdit unsurlarına (örneğin siber saldırganlar, zararlı yazılımlar vb.) karşı değil; aynı zamanda içsel zafiyetlere, çalışan hatalarına, süreçsel eksikliklere ve kurumsal kapasite yetersizliklerine karşı da güçlü savunma mekanizmaları geliştirme sorumluluğu taşımaktadır. Bilgi güvenliğinin temelini oluşturan gizlilik, bütünlük ve erişilebilirlik ilkeleri, bu çerçevede tüm kurumsal işleyişe entegre edilmeli ve sürdürülebilir şekilde uygulanmalıdır (Güldüren, 2015). Ancak bu ilkelerin yalnızca teknolojik çözümlerle sağlanması yeterli değildir. Etkin bilgi güvenliği, stratejik bir bakış açısı, sağlam bir yönetişim anlayışı ve sistematik risk yönetimi uygulamalarıyla mümkündür (Gürcan, 2014).

Bu bağlamda, bilgi güvenliği sistemlerinde yer alan risk yönetimi süreçlerinin stratejik bir perspektiften değerlendirilmesi gerekliliği ortaya çıkmaktadır. Risk yönetimi yalnızca olası tehditlerin ve sistemsel açıkların tanımlanmasıyla sınırlı kalmayıp, bu risklerin analiz edilerek kabul edilebilir seviyelere indirgenmesini hedefleyen sürekli ve bütüncül bir süreci kapsamaktadır (Aktaş, 2020). Stratejik bir yaklaşım, bu süreci

kurumun genel hedefleri, uzun vadeli planları, insan kaynakları yapısı ve politika çerçevesi ile entegre ederek daha sürdürülebilir hale getirmektedir.

Araştırmanın temel amacı, risk yönetimi adımlarının bilgi güvenliği yönetim sistemlerine nasıl entegre edildiğini ve bu süreçlerin kurumsal stratejilerle nasıl uyumlu hale getirilebileceğini analiz etmektir. Risk yönetiminin temel aşamaları olan tanımlama, değerlendirme, kontrol altına alma ve izleme gibi süreçlerin kurumsal yapı üzerindeki etkileri detaylı olarak ele alınmıştır. Ayrıca uluslararası düzeyde kabul gören bilgi güvenliği standartları ve yasal düzenlemelerin bu süreçlere olan etkileri incelenmiştir. Dijitalleşmenin hızla arttığı çağımızda, siber tehditlerin çeşitlenmesi, veri ihlallerinin artması ve düzenleyici yükümlülüklerin karmaşıklaşması, bilgi güvenliğini yalnızca teknik değil aynı zamanda kurumsal sürdürülebilirlik, itibar ve rekabet avantajı açısından stratejik bir konu haline getirmiştir.

Bu çerçevede araştırmada bazı varsayımlar temel alınmıştır. Kurumların bilgi güvenliği ve risk yönetimi süreçlerini hayata geçirecek yeterli kaynak, altyapı ve uzmanlığa sahip oldukları kabul edilmiştir. Ayrıca bu süreçlerin yalnızca teknik unsurlardan değil, organizasyonel yapı, çalışan davranışları ve kurumsal kültür gibi sosyo-teknik faktörlerden de etkilendiği varsayılmıştır. Uluslararası bilgi güvenliği standartlarının (örneğin ISO/IEC 27001) ve yasal düzenlemelerin (KVKK, GDPR gibi) kurumsal stratejileri şekillendirdiği bir diğer varsayımdır. Son olarak, risklerin doğru bir biçimde tanımlanıp yönetilmesiyle kurumların daha güvenli ve sürdürülebilir bir yapıya kavuşacağı öngörülmektedir.

Bu çalışmada bilgi güvenliği sistemleri bağlamında risk yönetimi süreçleri, özellikle ISO/IEC 27001 gibi standartlar ve KVKK ile GDPR gibi düzenlemelerin etkileri çerçevesinde analiz edilmiştir. Hem kamu hem de özel sektöre ait vaka örnekleri

kullanılarak başarılı ve başarısız uygulamalar karşılaştırmalı olarak değerlendirilmiştir. Ancak araştırma, yalnızca bu iki sektörle sınırlı tutulmuş; diğer sektörlere yönelik genelleştirmeler yapılmamıştır. Veriler, literatür kaynakları, akademik yayınlar ve kamuya açık vaka analizlerinden elde edilmiş olup tüm kurumsal yapıların iç dinamiklerini temsil etme amacı taşımamaktadır.

Yöntemsel açıdan, çalışma nitel araştırma olarak yapılandırılmıştır. Literatür taraması, vaka analizi ve karşılaştırmalı değerlendirme gibi teknikler kullanılmıştır. İlk aşamada teorik altyapı oluşturulmuş, ikinci aşamada ise Türkiye ve uluslararası ölçekteki çeşitli kurumlar üzerinden vaka analizleri yapılmıştır. Bu analizler, bilgi güvenliği risk yönetimi süreçlerinin etkinliğini kıyaslamayı, başarılı ve başarısız uygulamaların ardındaki nedenleri ortaya koymayı ve stratejik iyileştirme alanlarını belirlemeyi hedeflemektedir.

Bu proje çalışması, bilgi güvenliği ile risk yönetimi arasındaki ilişkiyi yalnızca teknik düzeyde değil; aynı zamanda stratejik, yönetsel ve hukuki boyutlarıyla da bütüncül bir yaklaşımla ele almaktadır.

1. BİLGİ GÜVENLİĞİ: KAVRAMSAL TEMEL, RİSK YÖNETİMİ SÜRECİ VE YÖNETİM SİSTEMLERİ

1.1 Bilgi Güvenliğinin Kavramsal Temeli

1.1.1 Bilgi Güvenliğinin Tanımı ve Amacı

Bilgi güvenliği, bir kurumun sahip olduğu dijital ya da fiziksel bilgi varlıklarını yetkisiz erişim, kullanım, ifşa, bozulma veya kayıplara karşı koruma sürecidir. Bu süreç yalnızca teknik önlemlerle sınırlı kalmayıp, organizasyonel politikalar, prosedürler ve insan faktörünü de kapsayan çok boyutlu bir yaklaşımı gerektirir (Demirtaş, 2013). Günümüz kurumlarında bilgi, stratejik karar alma süreçlerinden operasyonel işleyişe kadar birçok alanda temel kaynak konumundadır. Bu nedenle, bilgi güvenliği yalnızca bilgi teknolojileri departmanının sorumluluğunda değil; kurum genelinde kolektif bir bilinçle ele alınması gereken bir konudur.

Bilgi güvenliğinin temelinde üç ana ilke yer alır: gizlilik (confidentiality), bütünlük (integrity) ve erişilebilirlik (availability). Bu ilkeler, uluslararası literatürde "CIA Triadı" olarak adlandırılmakta ve güvenlik stratejilerinin temelini oluşturmaktadır. Gizlilik ilkesi, bilginin sadece yetkili bireylerce erişilebilir olmasını sağlar ve veri mahremiyeti açısından kritik öneme sahiptir. Bütünlük ilkesi, bilginin doğruluğunun ve bütün halinin korunmasını ifade eder. Erişilebilirlik ise, bilgilerin ihtiyaç duyulan anda kesintisiz bir şekilde ulaşılabilir olmasını garanti eder (Gencer, 2015). Bu üç ilkenin bir arada ve dengeli biçimde sağlanması, etkili bir bilgi güvenliği sisteminin ön koşuludur.

Bilgi güvenliğinin amacı yalnızca bilgiye zarar verebilecek tehditleri engellemek değildir. Aynı zamanda iş sürekliliğini sağlamak, regülasyonlara uyum göstermek, kurumsal itibar kaybını önlemek ve rekabet gücünü sürdürülebilir kılmak gibi çok daha geniş hedefleri de içerir (Aktaş, 2020). Özellikle son yıllarda yaşanan büyük çaplı veri

ihlalleri, yalnızca teknik aksaklıklara değil; yetersiz kurumsal risk yönetimi ve stratejik planlama eksikliklerine de işaret etmektedir. Bu nedenle bilgi güvenliği, teknik bir tedbirler bütünü olmaktan çıkıp, kurumun genel iş yapış biçiminin ayrılmaz bir parçası haline gelmektedir.

1.1.2 Bilgi Güvenliğinin Evrimi

Bilgi güvenliği kavramı, tarihsel olarak ilk kez askeri kurumlar ve kamu güvenliği alanında, gizli bilgilerin yetkisiz kişiler tarafından ele geçirilmesini önlemek amacıyla gündeme gelmiştir. Soğuk Savaş dönemiyle birlikte, özellikle devletlerin istihbarat birimleri, iletişim sistemlerinin şifrelenmesi, belge sınıflandırmaları ve fiziksel güvenlik önlemleri gibi uygulamaları sistematik hale getirmiştir. Bu dönemde bilgi güvenliği daha çok "gizlilik" odaklı ve fiziksel sınırlamalarla çevrili bir alan olarak şekillenmiştir. Bilgisayarların kullanılmaya başlanması ve özellikle 1980'li yıllarda bilgi teknolojilerinin yaygınlaşmasıyla birlikte, bilgi güvenliği dijital ortama taşınmış ve teknik kontrollerin önemi artmıştır (Björck, 2005).

1990'lı yıllardan itibaren internetin yaygınlaşması, kurumsal işleyişin dijitalleşmesi ve ticari verilerin dijital ortamda saklanmaya başlamasıyla birlikte bilgi güvenliği, sadece devletlerin değil özel sektörün de öncelikli gündem maddesi haline gelmiştir. Bu geçişle birlikte "gizlilik" odaklı güvenlik anlayışı yerini çok daha geniş kapsamlı bir yaklaşım olan "gizlilik, bütünlük ve erişilebilirlik" ilkelerine dayanan sistematik modellere bırakmıştır. Bu dönemde ISO/IEC 27001 gibi bilgi güvenliği yönetim sistemleri (BGYS) standartlaştırılmış; kurumların bilgi güvenliğini yalnızca bir bilgi teknolojileri konusu olarak değil, bütünsel bir yönetişim yapısı içinde ele alması gerektiği anlayışı gelişmiştir (Marhad, Abd Goni & Abdullah Sani, 2024).

Günümüzde bilgi güvenliği, teknolojinin baş döndürücü hızıyla birlikte daha da karmaşık hale gelmiştir. Yapay zeka, büyük veri, nesnelerin interneti (IoT), bulut sistemleri ve mobil cihazlar, kurumlara ciddi avantajlar sunmakla birlikte yeni güvenlik açıklarını da beraberinde getirmiştir (Domínguez-Domínguez, R., Flores-Laguna, O. A., & del Valle-López, J. 2023). Bu teknolojik gelişmeler, sadece dış tehditlerin değil, iç tehditlerin ve insan kaynaklı risklerin de yeniden değerlendirilmesini zorunlu kılmıştır. Artık bilgi güvenliği; yazılım yamaları, güvenlik duvarları veya antivirüs programlarıyla sınırlı olmayan, stratejik planlama, organizasyonel farkındalık ve sürekli güncellenen risk analizleriyle sürdürülebilen canlı bir yapı halini almıştır.

Bilgi güvenliğinin bu evrimi, kurumların bu alandaki yaklaşımlarını sürekli gözden geçirmesini ve teknolojik gelişmelere paralel olarak güvenlik politikalarını güncellemesini zorunlu kılmaktadır. Tarihsel gelişimin bilinmesi, bilgi güvenliği uygulamalarının yalnızca bugüne değil, geleceğe de yönelik stratejik kararlarla şekillendirilmesine katkı sağlamaktadır. Bu bağlamda, evrimsel süreç bilgi güvenliği anlayışının neden sürekli dinamik tutulması gerektiğini açık bir şekilde ortaya koymaktadır.

1.1.3 Bilgi Güvenliğinin Kurumsal Önemi

Bilgi, günümüzde kurumlar için sadece bir destek unsuru değil; aynı zamanda stratejik karar alma süreçlerinin temel girdisi ve operasyonel süreçlerin sürdürülebilirliği açısından vazgeçilmez bir değerdir (Güldüren, 2015). Ürün geliştirmeden müşteri ilişkilerine, tedarik zinciri yönetiminden finansal planlamaya kadar pek çok iş fonksiyonu, doğru ve güvenilir bilgiye dayanarak yürütülmektedir. Bu nedenle bilgi güvenliği, kurumların yalnızca dijital varlıklarını değil, aynı zamanda kurumsal verimliliğini ve rekabet gücünü de doğrudan etkileyen bir faktördür. Güvenliği

sağlanamayan bilgi, karar süreçlerini sekteye uğratarak hem maddi hem de stratejik zararlar doğurabilir.

Bilgi güvenliğinin sağlanamaması durumunda yaşanabilecek ihlaller, sadece finansal kayıplara değil; aynı zamanda kurumsal itibarın zedelenmesine ve müşteri güveninin kaybına da yol açabilmektedir (Gürcan, 2014). Özellikle kişisel verilerin korunmasına ilişkin yükümlülüklerin ihlali, kamuoyunda oluşabilecek olumsuz algının yanı sıra ciddi hukuki ve idari yaptırımları da beraberinde getirmektedir. Bu tür bir güven kaybı, müşteri bağlılığını azaltabilir, yatırımcıların güvenini sarsabilir ve markanın değerini düşürebilir. Örneğin global ölçekte yaşanan bazı veri ihlali vakalarında, şirketlerin borsa değerlerinde ani düşüşler görülmüş, üst düzey yöneticiler istifa etmek zorunda kalmış ve kurumlar yıllar süren itibar onarma süreçleriyle karşı karşıya kalmıştır.

Bilgi güvenliği, aynı zamanda kurumların yasal ve sektörel regülasyonlara uyumu açısından da büyük önem taşır. Türkiye'de yürürlükte olan 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ve Avrupa'da uygulanan Genel Veri Koruma Tüzüğü (GDPR), kurumlara kişisel verilerin işlenmesi, saklanması ve aktarılması konusunda kapsamlı sorumluluklar yüklemektedir (Erdoğan, 2016). Bu düzenlemelere uyum sağlanmaması durumunda kurumlar yüksek para cezalarına, faaliyet durdurma yaptırımlarına ya da dava süreçlerine maruz kalabilir. Dolayısıyla bilgi güvenliği sadece bir "teknik önlem" değil; aynı zamanda kurumsal yönetişim ve risk yönetimi çerçevesinin ayrılmaz bir bileşeni olarak değerlendirilmelidir.

Bilgi güvenliğini stratejik düzeyde ele alan kurumlar, yalnızca saldırılara karşı savunma oluşturmakla kalmaz; aynı zamanda proaktif güvenlik kültürü, çalışan farkındalığı, yönetim sistemleri entegrasyonu ve süreç temelli kontroller ile rekabet avantajı da elde eder. Bu nedenle bilgi güvenliği politikaları, kurumun tüm seviyelerinde benimsenmeli;

sadece bilgi teknolojileri birimlerine değil, tüm iş birimlerine entegre edilmelidir. Bu yaklaşım, bilgi güvenliğinin kurumsal bir sorumluluk olarak ele alınmasını ve güvenliğin sadece bir "bilgi teknolojileri sorunu" olarak değil, kurumun sürdürülebilirliğiyle doğrudan ilişkili bir yönetim konusu olduğunu ortaya koyar.

1.1.4 Gizlilik, Bütünlük ve Erişilebilirlik

Bilgi güvenliğinin kuramsal temelinin, literatürde sıklıkla "CIA Triadı" olarak bilinen üç temel ilkeye: gizlilik (confidentiality), bütünlük (integrity) ve erişilebilirlik (availability) dayandığından bahsetmiştik. Bu üç unsur, bilgi varlıklarının güvenliğini sağlamak amacıyla oluşturulan tüm politika, prosedür ve teknik önlemlerin merkezinde yer alır. Etkili bir bilgi güvenliği yönetim sistemi, bu üç ilke arasındaki dengeyi koruyarak hem güvenliği sağlar hem de kurumun operasyonel verimliliğini gözetir (Aktaş, 2020). Aksi takdirde, yalnızca bir unsurun aşırı ön planda tutulması diğerlerini zayıflatabilir; örneğin, aşırı gizlilik kontrolleri, erişilebilirliği olumsuz etkileyebilir.

Gizlilik, bilgiye yalnızca yetkili kullanıcıların erişebilmesini ifade eder ve genellikle "bilgiye erişim hakkı" ile ilişkilendirilir. Bu ilkenin ihlali, kişisel verilerin açığa çıkmasına, ticari sırların sızdırılmasına ve itibar kayıplarına neden olabilir. Kurumlar gizlilik ilkesini sağlamak için şifreleme teknikleri, rol tabanlı erişim kontrolleri (RBAC), çok faktörlü kimlik doğrulama (MFA) ve güvenlik duvarları gibi çeşitli teknolojik çözümlerden yararlanır. Özellikle günümüzde mobil cihazların ve uzaktan çalışma modellerinin yaygınlaşmasıyla, gizlilik ilkesinin korunması daha karmaşık hale gelmiş; dolayısıyla veri erişiminin lokasyon ve cihaz bazında da denetlenmesi gereklilik halini almıştır.

Bütünlük, bilginin doğruluğunun ve eksiksizliğinin korunması anlamına gelir. Bilgi, oluşturulduğu andan itibaren geçerliliğini korumalı; yetkisiz değişikliklere, silinmelere

veya bozulmalara karşı korunmalıdır. Bütünlük ilkesinin zedelenmesi durumunda, karar alma süreçleri hatalı bilgiye dayanabilir ve operasyonel süreçlerde ciddi aksaklıklar yaşanabilir. Bu ilkeyi korumak için kullanılan yöntemler arasında dijital imzalar, hash algoritmaları, kontrol toplamları (checksum), sürüm kontrol sistemleri ve değişiklik kayıtları (log yönetimi) yer alır. Özellikle regülasyonlara tabi sektörlerde (örneğin finans ve sağlık) bütünlük, hem yasal uyumluluk hem de veri kalitesi açısından kritik öneme sahiptir (Gencer, 2015).

Erişilebilirlik, bilgiye yetkili kişilerin ihtiyaç duydukları anda, kesintisiz biçimde ulaşabilmesini sağlar. Bu ilke, iş sürekliliği ve hizmet kalitesi açısından en az diğer ilkeler kadar önemlidir. Erişilebilirliğin engellenmesi, genellikle sistem çökmesi, donanım arızası, DDoS saldırıları, yazılım hataları veya doğal afetler gibi olaylar sonucunda meydana gelir. Bu tür riskleri azaltmak için kurumlar yüksek erişilebilirlik (HA) mimarileri, felaket kurtarma planları (DRP), veri yedekleme çözümleri ve bulut tabanlı sistem yedeklemeleri gibi önlemleri devreye sokmaktadır (Marhad, Abd Goni & Abdullah Sani, 2024). Ayrıca, siber olaylara müdahale ekiplerinin varlığı ve sistem altyapısının düzenli test edilmesi, erişilebilirliğin sürdürülebilirliğini destekleyen önemli unsurlardır.

Şekil 1.1.4: CIA Triadi– Bilgi Güvenliğinin Temel İlkeleri

CIA Triadı'nın bu üç ilkesi, yalnızca teknik altyapıya değil; aynı zamanda kurumsal stratejiye de yön verir. Kurumlar, hangi bilginin ne ölçüde korunacağına dair risk bazlı analizler yapmalı ve CIA unsurları arasında ihtiyaçlara uygun, dengeli bir güvenlik politikası oluşturmalıdır. Bu bağlamda, bilgi güvenliği yalnızca teknolojik önlemlerle değil; aynı zamanda kurumsal farkındalık, eğitim programları, yönetişim yapıları ve sürekli gözden geçirme süreçleriyle bütünleşik olarak yürütülmelidir.

1.2 Bilgi Güvenliğinde Tehditler, Zafiyetler ve Risk Temelli Yaklaşımlar

Bilgi güvenliği risklerinin doğru anlaşılabilmesi için "tehdit" ve "zafiyet" kavramlarının ayrı ayrı ama birbiriyle bağlantılı şekilde ele alınması gerekmektedir. Kurumların bilgi varlıklarını etkin bir biçimde koruyabilmesi, potansiyel tehditleri tanımlaması, bu tehditlerin istismar edebileceği zafiyetleri belirlemesi ve tüm bu unsurları bir arada değerlendirerek risk seviyesini ölçebilmesiyle mümkündür. Bu bölümde tehdit ve zafiyet kavramları detaylandırılarak, bilgi güvenliği risk yönetiminin temel dinamikleri ortaya konulacaktır.

1.2.1 Tehdit Türleri ve Kaynakları

Tehdit, bilgi sistemlerine ya da bilgi varlıklarına zarar verme potansiyeline sahip her türlü olay, durum ya da aktör olarak tanımlanmaktadır. Tehditler doğrudan zarara yol açmaz; ancak eğer sistemde uygun bir zafiyet mevcutsa, ciddi güvenlik olaylarına neden olabilir. Tehditler, genel olarak aşağıdaki üç ana kategoride incelenebilir:

1. **Doğal Tehditler:** Deprem, yangın, sel gibi doğal afetlerdir. Kontrol edilemeyen bu olaylar, veri merkezlerine, sunuculara veya fiziksel bilgi taşıyıcılarına zarar vererek bilgi erişimini ve bütünlüğünü tehlikeye sokabilir Felaket kurtarma planları (DRP), bu tür tehditlere karşı başvurulan başlıca yöntemdir.
2. **İnsan Kaynaklı Tehditler:** Bilinçli veya bilinçsiz insan eylemleri sonucu ortaya çıkar. Bilinçli tehditler arasında siber saldırılar, sabotaj ve iç tehditler (örneğin kötü niyetli çalışanlar) yer alırken; bilinçsiz tehditler arasında kullanıcı hataları, yanlış yapılandırmalar veya eğitimsizlik sonucu gelişen olaylar öne çıkar.
3. **Teknik Tehditler:** Donanım arızaları, yazılım açıkları, sistem çökmeleri ve ağ kesintileri gibi bilgi sistemlerinin işleyişinden kaynaklanan sorunlardır. Bu tehditlerin önlenmesi veya etkilerinin azaltılması için sürekli bakım, sistem güncellemeleri ve izleme çözümleri gereklidir.

Modern tehdit ortamı, klasik tehdit anlayışının ötesine geçmektedir. Günümüzde kurumlar; fidye yazılımları (ransomware), kimlik avı saldırıları (phishing), sosyal mühendislik, zero-day açıkları ve içeriden gelen tehditler gibi daha sofistike saldırılarla karşı karşıya kalmaktadır (Marhad, Abd Goni & Abdullah Sani, 2024). Bu tehditlerin önemli bir kısmı, teknik önlemlerin yanı sıra organizasyonel farkındalıkla da kontrol altına alınmalıdır.

1.2.2 Zafiyet Türleri ve Yaygın Kaynakları

Zafiyet, bilgi sistemlerinde mevcut olan ve tehditlerin başarıyla sonuçlanmasını mümkün kılan güvenlik açıklarıdır. Zafiyetler genellikle yazılım, donanım, yapılandırma hataları, zayıf süreçler veya insan kaynaklı eksikliklerden kaynaklanmaktadır (Güldüren, 2015). Bu açıklar tek başına zarara neden olmazlar; ancak bir tehdit unsuru ile birleşmeleri durumunda sistemler için ciddi risk oluşturmaktadırlar.

Yaygın zafiyet türleri şunlardır:

- **Güncellenmemiş Yazılımlar:** Yazılım güncellemeleri, çoğunlukla güvenlik açıklarını gidermek amacıyla yayınlanır. Bu güncellemelerin yapılmaması, bilinen açıkların siber saldırganlar tarafından kolayca istismar edilmesine yol açabilmektedir.
- **Zayıf Parola Politikaları:** Kısa, tahmin edilebilir veya tekrar kullanılan parolalar, siber saldırılarda en sık istismar edilen zafiyetlerden biridir. Parola yönetimi ve çok faktörlü kimlik doğrulama bu sorunun önüne geçebilmektedir.
- **Yetersiz Erişim Kontrolleri:** Bilgiye gereksiz ya da aşırı yetkili erişim verilmesi, içeriden ya da dışarıdan gerçekleşebilecek yetkisiz erişim riskini artırmaktadır.
- **Güvenlik Farkındalığı Eksikliği:** Kurum çalışanlarının bilgi güvenliği konularında eğitimsiz veya dikkatsiz olması, insan kaynaklı zafiyetlerin başlıca nedenidir. Özellikle sosyal mühendislik saldırılarında bu zafiyet sıklıkla kullanılmaktadır.
- **Hatalı Ağ Yapılandırmaları:** Güvensiz ağ protokolleri, açık portlar ya da segmentasyon eksikliği, siber saldırganların sisteme sızmasını kolaylaştırabilmektedir.

Zafiyetler, düzenli olarak zafiyet tarayıcıları**,** sızma testleri ve otomatik güvenlik analiz araçları kullanılarak tespit edilmelidir. Ayrıca kurumlar, yalnızca teknik zafiyetlere odaklanmakla kalmamalı; çalışan farkındalığı, süreç denetimi ve politikaların uygulanabilirliği gibi yönetsel zafiyetleri de göz önünde bulundurmalıdır.

1.2.3 Tehdit-Zafiyet-Risk İlişkisi

Bilgi güvenliği yönetimi, yalnızca tehditleri ya da zafiyetleri izlemekle sınırlı değildir; bu iki unsurun etkileşimini değerlendirerek ortaya çıkan riskleri önceden tahmin etmeyi ve kontrol altına almayı hedefler (Demirtaş, 2013). Bu bağlamda tehdit, zafiyet ve risk arasındaki ilişki aşağıdaki formülle özetlenebilir:

$$Risk = Tehdit \times Zafiyet \times Etki\ Düzeyi$$

Bu formülde, riskin büyüklüğü hem tehdidin gerçekleşme olasılığına hem de zafiyetin ne ölçüde istismar edilebileceğine bağlıdır. Ayrıca, bir tehdit gerçekleştiğinde kurum üzerindeki etki düzeyi (finansal, operasyonel, hukuki, itibari) riskin nihai ağırlığını belirler. Bu nedenle kurumların risk değerlendirme sürecinde, tehdit istihbaratı, zafiyet analizleri ve etki tahmin modellerini birlikte kullanması gereklidir.

Etkili bir risk yönetimi için kurumların düzenli olarak tehdit ortamını analiz etmesi**,** zafiyet taramaları yapması ve bu bulgular doğrultusunda öncelikli risk alanlarını belirleyerek stratejik kontroller geliştirmesi gerekir. Bu yaklaşım, bilgi güvenliğini yalnızca reaktif bir savunma değil, aynı zamanda proaktif bir kurumsal güvenlik stratejisi olarak konumlandırmaktadır.

1.2.4 İçeriden Gelen Tehditler: İnsan Faktörünün Rolü

Bilgi güvenliği süreçlerinde en zayıf halkalardan biri, çoğu zaman insan faktörü olmaktadır. Çalışanların ihmalkar davranışları, farkındalık eksikliği veya kötü niyetli hareketleri, içeriden gelen tehditleri oluşturmaktadır (Gürcan, 2014). Bu tehditler, dış saldırganlara göre daha yıkıcı olabilir çünkü iç kaynaklar zaten sisteme erişim yetkisine sahiptir ve güvenlik duvarlarını aşmak zorunda değildir.

İç tehditler genellikle üçe ayrılmaktadır:

1. **Kasıtlı İç Tehditler**: Örneğin gizli bilgileri sızdıran ya da sabotaj yapan çalışanlar.
2. **İhmalkar Kullanıcılar**: Farkında olmadan zararlı yazılım yükleyen ya da yetkisiz kişilerle şifre paylaşan personel.
3. **Ayrılan Çalışanlar**: Kuruma olan bağlılığı azalmış ya da yönetime kızgın eski çalışanlar.

Bu tür tehditlere karşı etkili önlemler arasında, işten ayrılan çalışanların hesaplarının anında kapatılması (offboarding), erişim kayıtlarının düzenli izlenmesi, çalışan davranış analizleri ve bilgi güvenliği farkındalık eğitimleri yer almaktadır. Kurumlar bu alanda, insan kaynakları ve bilgi güvenliği ekipleri arasında koordinasyonu artırmalıdır.

1.2.5 Sıfırıncı Gün Açıkları ve Gelişen Tehdit Vektörleri

"Sıfırıncı gün (zero-day)" açıkları, henüz üretici firma ya da güvenlik topluluğu tarafından bilinmeyen ve bu nedenle yaması veya çözümü bulunmayan yazılım güvenlik açıklarıdır. Saldırganlar bu açıklardan yararlanarak hedef sistemlere sızabilir. Çünkü sistem sahiplerinin bu açık hakkında bilgisi olmadığı için savunmasızdırlar.

Zero-day saldırılar özellikle devlet destekli tehdit aktörleri ya da gelişmiş kalıcı tehdit (APT – Advanced Persistent Threat) grupları tarafından kullanılır. Bu tür tehditlere karşı savunma mekanizmaları arasında, davranış tabanlı tehdit algılama sistemleri (heuristic analysis), sandbox teknolojileri ve yapay zeka destekli güvenlik çözümleri yer almaktadır (Gürcan, 2014).

Ayrıca gelişen teknolojilerle birlikte tehdit vektörleri de değişmektedir. IoT cihazları, mobil uygulamalar, bulut sistemleri gibi yeni platformlar siber saldırganlar için yeni hedefler yaratmıştır. Kurumlar, sadece klasik ağ güvenliği önlemleriyle değil, bu yeni tehdit yüzeylerini de kapsayacak şekilde güvenlik mimarilerini tasarlamalıdır.

1.2.6 Tehdit İstihbaratı ve Proaktif Güvenlik Yaklaşımları

Modern bilgi güvenliği anlayışı, sadece "olduktan sonra önlem alma" yaklaşımını değil, önceden tespit ve engellemeye dayalı proaktif güvenliği temel almaktadır. Bu noktada tehdit istihbaratı kavramı devreye girer. Tehdit istihbaratı, siber tehditler hakkında bilgi toplayarak, kurumların bu tehditleri önceden tanımasını ve önlem almasını sağlar.

İstihbarat kaynakları; açık kaynaklar (OSINT), kapalı ağlar (dark web izleme), saldırı günlüğü analizleri ve siber güvenlik servis sağlayıcıları olabilir. Bu bilgiler analiz edilerek kurumun özel risk profiline uygun önlemler belirlenir. Ayrıca SIEM (Security Information and Event Management) sistemleri sayesinde, farklı sistemlerden gelen loglar tek bir platformda analiz edilerek saldırı belirtileri erken aşamada tespit edilebilir (Aktaş, 2020).

Proaktif güvenlik stratejileri, klasik savunma yaklaşımlarına göre daha maliyetlidir; ancak zarar meydana geldikten sonra oluşan kayıplarla kıyaslandığında, uzun vadede çok daha avantajlıdır.

1.3. Bilgi Güvenliğinde Risk Yönetimi Süreci

1.3.1 Risk Tanımı ve Kavramları

Bilgi güvenliği kapsamında risk; bir tehdidin, belirli bir zafiyet aracılığıyla bir bilgi varlığına zarar verme olasılığı ve bu zararın kurumsal etkileriyle birlikte değerlendirilmesiyle tanımlanmaktadır. Bu tanım, ISO/IEC 27005 standardında da belirtilmiştir (ISO/IEC 27005, 2022). Bu tanım yalnızca teknik bir çerçeve sunmaz; aynı zamanda iş sürekliliği, yasal sorumluluklar, itibari kayıplar ve stratejik hedefler üzerinde yaratabileceği etkiler açısından da çok boyutlu bir yaklaşımı zorunlu kılar. Risk, önlem alınmadığında gerçekleşme ihtimali bulunan ancak gerçekleştiğinde sonuçları belirsiz olan bir durumdur.

Bir riskin oluşabilmesi için üç temel unsurun bir araya gelmesi gerekir: tehdit, zafiyet ve değerli bir varlık. Örneğin; güncel olmayan bir yazılım (zafiyet), dış kaynaklı bir fidye yazılımı saldırısı (tehdit) ile birleştiğinde müşteri verilerinin şifrelenmesine ve işletmenin hizmet dışı kalmasına (riskin gerçekleşmesi) yol açabilir. Bu çerçevede risk kavramı sadece bilgi teknolojileri departmanının değil, insan kaynaklarından hukuk birimine kadar tüm organizasyonun gündeminde olmalıdır.

Risk, doğası gereği belirsizlik içerir ve bu da yönetimini karmaşık hale getirir. Tüm riskler ortadan kaldırılamaz; ancak ölçülebilir, sınıflandırılabilir ve etkisi azaltılabilir. Bu nedenle modern risk yönetimi, riski “sıfırlamak” değil, “yönetilebilir düzeye indirmek” üzerine kurgulanmaktadır (NIST SP 800-30, 2012). Bu yaklaşım, bilgi güvenliğini reaktif değil proaktif bir sürece dönüştürmektedir. (ISO/IEC 27005 standardı, riskin bu üç unsur temelinde modellenmesini destekler ve bu bağlamda riskin kurumsal karar alma süreçleriyle entegrasyonunu önerir.)

1.3.2 Risk Analizi ve Değerlendirme

Risk analizi, tanımlanan tehdit ve zafiyetlerin hangi koşullarda ve ne ölçüde kurumsal etkiler doğurabileceğini belirlemeye yönelik sistematik bir süreçtir. Analiz süreci, bilgi varlıklarının değerlemesini içerdiği gibi; gerçekleşme olasılığı ve potansiyel etki gibi nicel ve nitel parametreleri de hesaba katmaktadır. Burada kullanılan yöntemler üçe ayrılabilir: nitel (qualitative), nicel (quantitative) ve melez (semi-quantitative) (ISO/IEC 27005, 2022).

Nitel analizde uzman görüşleri, tecrübeye dayalı değerlendirmeler ve matris tabanlı yaklaşımlar ön plandayken, nicel analizde matematiksel modellemeler, geçmiş veri analizleri ve finansal kayıp tahminleri öne çıkmaktadır. Melez yöntemler ise bu iki yaklaşımı birleştirerek daha gerçekçi sonuçlar üretir. Özellikle sınırlı veri setine sahip kurumlar için melez yöntemler pratik çözümler sunar.

Risk değerlendirme aşamasında ise riskin organizasyonel bağlamda ne ölçüde kabul edilebilir olduğu belirlenmektedir. Bu noktada genellikle "risk matrisi" kullanılır. Matris, her riskin olasılığı ve etkisi üzerinden derecelendirilmesini sağlar ve bu sayede "kırmızı bölge"de yer alan kritik riskler önceliklendirilebilir (NIST SP 800-30, 2012).

Basit Risk Matrisi

(Risklerin Etki ve Olasılık ekseninde sınıflandırıldığı 3x3 matris örneği)

Kullanılacak renkler: Kırmızı (yüksek risk), Sarı (orta risk), Yeşil (düşük risk)

Tablo 1.3.2: Örnek Risk Matrisi

Risk Olasılığı	**Düşük Etki**	**Orta Etki**	**Yüksek Etki**
Yüksek	Orta Risk	Yüksek Risk	Kritik Risk
Orta	Düşük Risk	Orta Risk	Yüksek Risk
Düşük	Önemsiz	Düşük Risk	Orta Risk

Bu matris, kurumların risk önceliklendirmesini görsel olarak yapmasını sağlar.

Vaka Örneği 1.3.2: Veri Hırsızlığı

Bir bankanın müşteri veritabanının eski bir sürüm kullanması nedeniyle siber saldırıya uğraması ve verilerin çalınması:

Zafiyet → güncel olmayan sistem,

Tehdit → dış kaynaklı saldırı,

Risk → müşteri bilgisi ihlali

Sonuç olarak bankaya BDDK cezası kesildi.

1.3.3 Riskin Azaltılması ve Kontrollerin Belirlenmesi

Tespit edilen risklerin etkisini en aza indirmek için kurumlar çeşitli kontrol mekanizmaları uygulamaktadırlar. Bu kontroller, türlerine göre dört ana kategoriye ayrılır: teknik**,** yönetsel**,** fiziksel ve hukuki**.** Teknik kontroller arasında şifreleme algoritmaları, antivirüs yazılımları, IDS/IPS sistemleri ve güvenlik duvarları yer alırken; yönetsel kontroller politika ve prosedürler, çalışan eğitimi ve farkındalık programları, rol bazlı erişim kontrolleri gibi unsurları içermektedir.

Fiziksel kontroller, veri merkezlerine yetkisiz erişimin önlenmesi, güvenlik kameraları, biyometrik doğrulama sistemleri gibi uygulamaları kapsamaktadır. Hukuki kontroller ise hizmet sözleşmeleri, veri işleme taahhütnameleri ve KVKK/GDPR gibi yasal düzenlemelere uyum çerçevesinde alınan önlemleri içermektedir. Bu kontrollerin etkili olabilmesi için her birinin uygulanabilirliği, sürdürülebilirliği ve etkinliği değerlendirilmelidir (ISO/IEC 27005, 2022).

Her riski azaltmak ekonomik olarak mümkün olmayabilir. Bu nedenle kurumlar bazı riskleri kabul edebilir (düşük etkili olanlar), bazılarını transfer edebilir (örneğin siber sigorta, dış kaynak kullanımı) veya ortadan kaldırabilir (örneğin riskli hizmeti sonlandırmak). Bu kararların alınmasında maliyet-fayda analizi yapılmalı, risk iştahı ile kurumun stratejik hedefleri dengelenmelidir (NIST SP 800-30, 2012). (NIST SP 800-30 rehberi, kontrol türlerinin seçimi için kurumların hem iç risk toleransını hem de dış tehdit ortamını birlikte değerlendirmesini önerir.)

Vaka Örneği 1.3.3: Kritik Verilerin Açığa Çıkması (Fidye Yazılımı Saldırısı)

Bir enerji şirketinin fidye yazılımı saldırısına uğraması ve saldırganların, şirketin yedekleme sisteminde bir açık tespit ederek tüm müşteri verilerine erişim sağlaması;

Kurum, güncel IDS sistemi kullanmasına rağmen yetersiz yedekleme politikaları nedeniyle verilerini geri getiremedi,yalnızca teknik değil yönetsel zafiyetlerin de risk doğurduğu ortaya kondu.

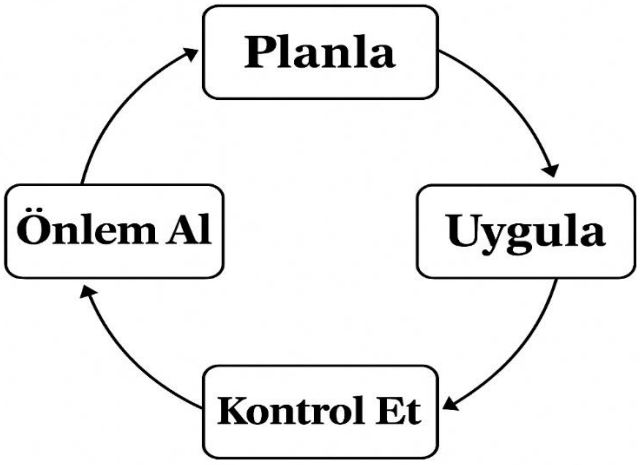
Sonuç olarak şirket itibar kaybına uğradı, müşteri şikayetleriyle karşı karşıya kaldı ve düzenleyici kurumlar tarafından ceza aldı.

1.3.4 Sürekli İyileştirme ve İzleme

Risk yönetimi, bir defaya mahsus uygulanan bir işlem değil; çevresel koşullar, teknolojik değişiklikler ve kurumsal gelişmeler doğrultusunda sürekli gözden geçirilmesi gereken döngüsel bir süreçtir. ISO/IEC 27001 standardı bu yapıyı "Planla-Uygula-Kontrol Et-Önlem Al (PUKÖ)" döngüsüyle sistematize etmektedir (ISO/IEC 27001, 2022). Bu döngü, risk yönetimiyle birlikte bilgi güvenliği yönetim sisteminin tamamının sürekli olarak geliştirilmesini sağlamaktadır.

Sürekli iyileştirme sürecinde birçok izleme ve ölçüm mekanizması kullanılır: log (kayıt) analizleri, iç ve dış denetim raporları, düzenli sızma testleri, çalışan anketleri, olay bildirim sistemleri vb. Bu araçlar sayesinde sadece teknik sistemler değil, kullanıcı davranışları ve kurumsal farkındalık da değerlendirilebilmektedir. Elde edilen veriler, kontrollerin yeniden gözden geçirilmesi, yeni politika oluşturulması veya kaynakların farklı önceliklere yönlendirilmesi gibi stratejik kararların temelini oluşturmaktadır (ISO/IEC 27005, 2022).

Sürekli iyileştirme yalnızca sistemin teknik altyapısını değil, aynı zamanda organizasyonun güvenlik kültürünü de kapsamalıdır. Bilgi güvenliği bir teknoloji sorunu değildir, kurum kültürünün ve yönetişimin bir parçası haline geldiğinde sürdürülebilirlik kazanır. Bu anlayış, kurumların sadece mevcut tehditlere değil; gelecekteki risklere karşı da dirençli olmasını sağlamaktadır.



- **Planla:** Riskleri analiz et, politika oluştur
- **Uygula:** Güvenlik önlemlerini devreye al
- **Kontrol Et:** Performansı ölç, izleme yap
- **Önlem Al:** Geliştirmeler yap, eksikleri gíder

Şekil 1.3.4: PUKÖ Döngüsü – Sürekli İyileştirme Süreci (ISO/IEC 27001)

Planla → Uygula → Kontrol Et → Önlem Al

Bu döngü, BGYS'nin sürdürülebilirliğini sağlamaktadır.

1.3.5 Risk İletişimi ve Kurumsal Farkındalık

Risk yönetimi yalnızca teknik ve yönetsel kontrollerle sınırlı değildir; aynı zamanda kurumsal iletişim ve farkındalık süreçlerinin bir parçasıdır. Çalışanların bilgi güvenliği risklerini tanıyabilmesi, bu risklerin etkilerine dair bilinç geliştirmesi ve kurumsal hedefler doğrultusunda bu süreçlere katılım göstermesi, etkin bir risk yönetiminin temel koşuludur. Güvenlik uygulamalarının başarısı, önemli ölçüde bireysel farkındalık ve kurumsal bağlılığa bağlıdır (Çek, 2017).

İletişim süreçlerinin etkili şekilde yapılandırılması için kurum içi eğitimler, bilgilendirme seminerleri ve etkileşimli güvenlik farkındalık programları

düzenlenmelidir. Özellikle sosyal mühendislik saldırılarının arttığı günümüzde, çalışanlara yönelik düzenli tehdit simülasyonları yapılması önerilmektedir. Whitman ve Mattord (2022), çalışanların güvenlik tehditlerini tanıma kapasitesinin artırılmasının, siber risklerin azaltılmasında doğrudan etkili olduğunu belirtmektedir.

Yöneticiler, bilgi güvenliği farkındalığının yaygınlaştırılmasında lider rol üstlenmeli; risk iletişimini açık, sürdürülebilir ve iki yönlü bir mekanizma olarak kurmalıdır. Bu doğrultuda geliştirilen "kurumsal risk iletişim stratejileri", yalnızca üst yönetimi değil; orta kademe ve operasyonel birimleri de kapsamalı; bireylerin güvenlik süreçlerine olan katılımını teşvik etmelidir (Güldüren, 2015).

1.3.6 Mevzuat Uyumu ve Risk Yönetimi Entegrasyonu

Bilgi güvenliği risk yönetiminin sadece teknik ve organizasyonel süreçlerden ibaret olmadığı; aynı zamanda ulusal ve uluslararası düzenlemelere uyum sağlanması gereken yasal bir çerçeveye sahip olduğu unutulmamalıdır. Türkiye'de yürürlükte olan 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), Avrupa Birliği'ndeki Genel Veri Koruma Tüzüğü (GDPR) gibi mevzuatlar, kurumlardan belirli güvenlik standartlarına göre veri işleme ve risk kontrolü uygulamaları yürütmesini talep etmektedir (Erdoğan, 2016).

Bu düzenlemeler sadece veri koruma açısından değil; aynı zamanda risk yönetimi yaklaşımının kurumsal yönetim sistemlerine entegrasyonu açısından da belirleyicidir. Yasal uyum, kurumsal itibarı korumanın yanında müşteriler, iş ortakları ve denetleyici kurumlarla güven ilişkisini sürdürmek açısından da kritik öneme sahiptir (Marhad, Abd Goni & Abdullah Sani, 2024).

Risk yönetimi süreçlerinin mevzuatlarla bütünleştirilmesi, kurumların yalnızca iç denetim ve kontrol sistemlerini güçlendirmekle kalmaz; aynı zamanda bilgi güvenliği politikalarının sürekli güncellenmesini, personel sorumluluklarının tanımlanmasını ve hukuki yükümlülüklerin yerine getirilmesini sağlar. Bu bağlamda, hukuk birimleri ile bilgi teknolojileri birimleri arasında koordineli bir çalışma ortamı kurulmalı, uyum stratejileri teknik ve yönetsel kontrollerle bütünleşik şekilde tasarlanmalıdır (Demirtaş, 2013).

1.4. Bilgi Güvenliği Yönetim Sistemleri (BGYS)

1.4.1 ISO/IEC 27001 Standardı

ISO/IEC 27001, bilgi güvenliği alanında dünya çapında tanınan en önemli standartlardan biridir. Bu standart, organizasyonlara bilgi varlıklarını koruma konusunda sistematik ve yönetilebilir bir çerçeve sunmaktadır (ISO/IEC, 2022). ISO/IEC 27001 yalnızca teknik önlemleri değil, aynı zamanda organizasyonun kültürel, yönetsel ve stratejik yapılarını da kapsayacak şekilde bilgi güvenliğinin bütünsel bir yaklaşımla ele alınmasını sağlamaktadır. Standart; bilgi güvenliği risklerini tanımlama, değerlendirme, kontrol altına alma ve sürekli izleme aşamalarını içeren bir yönetim sistemi kurulmasını öngörmektedir.

ISO/IEC 27001'in en belirgin özelliklerinden biri, Planla-Uygula-Kontrol Et-Önlem Al (PUKÖ) döngüsünü esas almasıdır. Bu döngü, bilgi güvenliği yönetim sisteminin (BGYS) sürekli olarak gelişmesini sağlar. "Planla" aşamasında riskler tanımlanır ve güvenlik hedefleri belirlenir. "Uygula" adımı, kontrollerin devreye alındığı aşamadır. "Kontrol Et" bölümünde sistemin etkinliği denetlenir; "Önlem Al" aşamasında ise iyileştirmeler yapılır.

ISO/IEC 27001 sertifikası, bir kurumun bilgi güvenliği alanında uluslararası standartlara uygun hareket ettiğini belgelendirmektedir. (ISO/IEC 27001:2022). Bu durum, kurumun paydaşlarına, müşterilerine ve düzenleyici otoritelerine karşı güven vermesinin yanı sıra, yasal uyumluluk açısından da kritik önemdedir. Özellikle KVKK, GDPR gibi regülasyonlara uyum açısından ISO/IEC 27001'in sistematik yapısı önemli bir avantaj sağlar.

Vaka Örneği 1.4.1:

Bir e-ticaret firması, müşteri verilerinin sızmasından sonra ISO/IEC 27001 uygulamaya başladı. 6 ay içinde süreçler dokümante edildi, kontroller tanımlandı ve dış denetimden geçilerek sertifikasyon sağlandı.

Sonuç olarak, güvenlik açıkları kapatıldı, müşteri şikayetleri azaldı ve güven seviyesi yükseldi.

Tablo 1.4.1: PUKÖ Döngüsü ile BGYS Süreci

Aşama	**Açıklama**
Planla	Risk değerlendirme, politika belirleme
Uygula	Kontrollerin devreye alınması
Kontrol Et	Performans ölçümü, denetim
Önlem Al	Sürekli iyileştirme, yeni hedeflerin tanımı

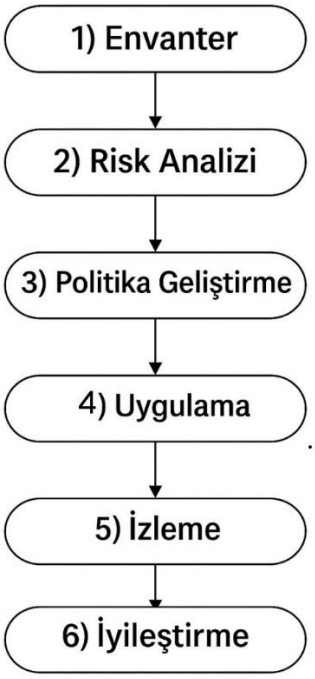
1.4.2 BGYS'nin Kurulması ve Sürdürülmesi

BGYS'nin kurulması yalnızca teknik sistemlerin yapılandırılmasını değil, aynı zamanda organizasyonel farkındalık, stratejik planlama ve kültürel değişim süreçlerini de içermektedir. Başlangıçta, organizasyonun sahip olduğu tüm bilgi varlıkları envantere alınır (Humphreys, 2010). Bu envanter üzerinden tehdit-zafiyet analizi yapılır ve risk

değerlendirme çalışmaları başlatılır. Bu noktada kritik olan, her bilginin kurumsal önemiyle ilişkilendirilerek değerlendirilmesidir.

Kurulum sürecinde, kuruma özel bilgi güvenliği politikaları ve prosedürleri geliştirilir. Ayrıca yetkilendirme mekanizmaları, erişim kontrol yapıları ve kayıt tutma sistemleri oluşturulur. Bu süreç yalnızca teknik ekiplerin değil; insan kaynakları, hukuk, finans ve operasyon gibi farklı departmanların birlikte çalışmasını gerektirir. Böylece BGYS, tüm organizasyonu kapsayan bir yönetişim sistemine dönüşür.

Sürdürülebilir bir BGYS yapısı için sürekli izleme ve denetim çok önemlidir. Belirli periyotlarla iç denetimler gerçekleştirilerek kontrollerin etkinliği değerlendirilmelidir. Ayrıca, çalışan eğitimleri ve farkındalık çalışmaları düzenli olarak tekrarlanmalıdır. Üst yönetimin sürece verdiği destek ve kaynak tahsisi, BGYS'nin kurumsallaşmasındaki en kritik faktörlerden biridir. (Humphreys, 2010).



Şekil 1.4.2: BGYS Kurulum Aşamaları

1.4.3 Denetim ve Uyum Süreçleri

Bir bilgi güvenliği yönetim sisteminin etkinliğini sağlayan en önemli bileşenlerden biri düzenli denetim süreçleridir. Denetimler hem iç hem de dış kaynaklar tarafından gerçekleştirilebilir ve genellikle üç temel amaca hizmet eder: mevcut güvenlik kontrollerinin etkinliğini ölçmek, uyum düzeyini değerlendirmek, iyileştirme alanlarını tespit etmek. Denetim süreçleri yalnızca ISO 27001 kapsamında değil, aynı zamanda KVKK, GDPR ve sektörel regülasyonlarla da entegre şekilde yürütülmelidir (Calder & Watkins, 2018).

İç denetimler, kurum içindeki denetim ekipleri veya bilgi güvenliği birimleri tarafından düzenli olarak yapılır. Bu süreçte; politika uyumu, log kayıtları, kullanıcı yetkileri ve güvenlik prosedürleri değerlendirilir. Dış denetimler ise sertifikasyon kuruluşları tarafından yapılır ve ISO 27001 uygunluk seviyesi bu denetimlerle belirlenir. Denetim bulguları, düzeltici ve önleyici faaliyet planları oluşturularak sürekli iyileştirme sürecine entegre edilir.

Yasal uyumluluk bağlamında ise denetimler kritik bir rol oynmaktadır. Özellikle kişisel verilerin korunması (KVKK, GDPR), kamu bilişim denetimleri (Türkiye'de Kamu SM) ve sektör bazlı regülasyonlar (bankacılıkta BDDK, sağlıkta HIMSS) bilgi güvenliği denetimlerinde rehber olarak kullanılır (Calder & Watkins, 2018). Bu düzenlemelere uyum, sadece yasal yaptırımlardan kaçınmak için değil, aynı zamanda müşteri güveni ve kurumsal itibarın sürdürülebilirliği için de gereklidir.

Vaka Örneği 1.4.3:

Bir sağlık hizmetleri şirketi, ISO 27001 sertifikası olmasına rağmen KVKK uyum denetiminde başarısız oldu,

Nedeni, iç süreçlerde kişisel veri sınıflandırmasının yanlış yapılmasıydı.

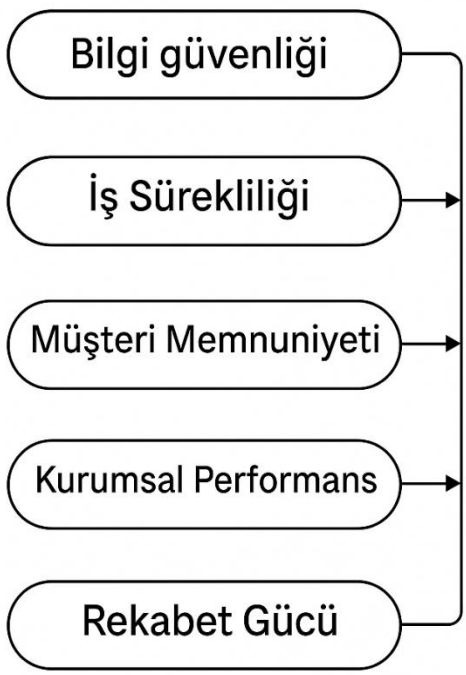
Sonuç olarak, olay sonrası şirket veri işleme süreçlerini revize etti ve veri sahibi hakları süreçlerini yeniden yapılandırdı.

1.4.4 BGYS'nin İşletme Performansına Etkisi

BGYS yalnızca bilgi güvenliğini sağlamakla kalmaz; aynı zamanda organizasyonel süreçlerin verimliliğini artırarak işletme performansını da doğrudan etkiler. Bilginin güvenli, bütünlüklü ve erişilebilir olması, kurum içinde karar alma süreçlerinin hızlanmasına ve operasyonel aksamaların azalmasına katkı sağlar. Bu sistem, olaylara karşı reaktif değil proaktif bir yapı kurarak, iş sürekliliğinin sağlanmasına destek olur.

Örneğin, bir e-ticaret şirketinde sistemsel bir saldırı yaşanması ve sipariş altyapısının çökmesi, doğrudan gelir kaybına neden olabilir. Güçlü bir BGYS ile bu tür kesintilerin önlenmesi, performans üzerindeki olumsuz etkilerin azaltılması anlamına gelir. Ayrıca ISO 27001 sertifikalı bir kurumun müşteri güveni daha yüksektir; bu da satış artışı, pazar büyümesi ve rekabet gücü gibi alanlara pozitif yansır (Calder & Watkins, 2018).

BGYS'nin işletme süreçlerine entegre edilmesi, özellikle süreç standardizasyonu, kaynak planlaması, iç denetim mekanizmalarının kurulması ve performans göstergelerinin izlenmesi gibi alanlarda fayda sağlar. Bu bağlamda bilgi güvenliği yalnızca bilgi teknolojileri departmanına özgü değil, tüm organizasyonu kapsayan stratejik bir yapıdır. İyi kurgulanmış bir BGYS, yalnızca maliyet azaltmaz, aynı zamanda organizasyonel olgunluk seviyesini de yükseltir.



Şekil 1.4.4: BGYS'nin Performans Etkisi Haritası

Vaka Örneği 1.4.4:

Bir finans şirketi, dijital dönüşüm sürecinde BGYS'yi temel alan süreç haritalaması yaparak karar süreçlerinde %35 zaman tasarrufu sağladı. Ayrıca müşteri destek taleplerinde hata oranı %22 azaldı.

1.4.5 BGYS'nin Risk Yönetimi ile Entegrasyonu

Risk yönetimi ve BGYS, doğası gereği birbiriyle entegre çalışmalıdır. ISO/IEC 27001'in tamamlayıcı standardı olan ISO/IEC 27005, bilgi güvenliği risklerinin tanımlanması, analiz edilmesi ve kontrol altına alınmasına yönelik detaylı yöntemler sunmaktadır (ISO/IEC, 2018). BGYS, bu risk yönetimi yapısına dayanarak, sistemli ve izlenebilir bir güvenlik mekanizması kurmaktadır.

Bu entegrasyonun temel bileşenleri; varlıkların tanımlanması, tehdit ve zafiyet analizleri, risk skorlaması ve kontrol seçimi süreçleridir. (ISO/IEC 27005). Ayrıca, bu

süreçler sürekli olarak gözden geçirilir, PUKÖ döngüsüne dahil edilir ve organizasyonun stratejik hedefleriyle hizalanır. Kurumlar bu yapıyı, iş sürekliliği planları ve kriz yönetim protokolleri ile destekleyerek, riskleri yönetilebilir seviyelere indirger.

Bir başka önemli konu ise riskin maliyetiyle kontrolün maliyetinin dengelenmesidir. BGYS, kaynakların optimum düzeyde kullanılması için öncelikli risklere odaklanmayı sağlar. Bu sayede organizasyonlar, hem güvenlik seviyesini artırır hem de gereksiz harcamalardan kaçınır.

Vaka Örneği 1.4.5:

Bir kamu kurumunda ISO 27001 uygulanmadan önce risk değerlendirme süreci yoktu.

Uygulama sonrası tüm bilgi varlıkları sınıflandırıldı, risk derecelendirme puanları belirlendi ve her risk için aksiyon planları geliştirildi.

Sonuç: %47 daha az güvenlik olayı raporlandı.

Tablo 1.4.5: Risk Yönetimi ile BGYS İlişkisi

BGYS Bileşeni	**Risk Yönetimi Unsuru**
Varlık Envanteri	Risk Konuları ve Kapsam
Güvenlik Politikaları	Risk Kontrol Seçimi
Denetim Planı	İzleme ve Risk İzleme
İyileştirme Süreci	Riskin Güncellenmesi ve Azaltımı

1.4.6 BGYS'nin Kültürel ve Organizasyonel Boyutu

BGYS'nin başarısı yalnızca teknik uygulamalara değil, kurum kültürü, liderlik desteği ve çalışan farkındalığına bağlıdır. Güçlü bir güvenlik kültürü oluşturulmadan en gelişmiş teknolojiler bile etkisiz kalabilir. Bu nedenle organizasyonlar, bilgi güvenliğini kurumsal bir değer olarak benimsemeli ve tüm çalışanlara yaymalıdır (Schein, 2010).

Kurumsal farkındalık, bilgi güvenliği eğitimleriyle başlar ancak burada sürdürülebilirlik önemlidir. Eğitimler düzenli, güncel ve role özel olmalıdır. Örneğin sistem yöneticileriyle ön büro çalışanlarının ihtiyaç duyduğu bilgi düzeyi farklıdır. Ayrıca oyunlaştırılmış eğitimler, e-öğrenme platformları ve iç denetimlerle çalışan davranışları izlenerek etkili bir farkındalık modeli inşa edilebilir.

Yöneticilerin örnek olması, kaynak tahsisi sağlaması ve iletişimi desteklemesi BGYS'nin kültürel boyutunun en güçlü bileşenidir (Schein, 2010). Liderlik desteği olmadan güvenlik farkındalığı kalıcı hale gelemez. Bununla birlikte, çalışanların sisteme olan bağlılığı arttıkça iç tehditler azalır, güvenlik politikaları benimsenir ve olay bildirim oranları yükselir.

Şekil 1.4.6: Güvenlik Kültürü Olgunluk Modeli (SCMM)

Vaka Örneği 1.4.6:

Bir yazılım firması, çalışanlarına düzenli güvenlik farkındalık eğitimleri vermeye başladı.

1 yıl içinde phishing simülasyonlarında tıklama oranı %52'den %11'e düştü. Sonuçlar, farkındalığın ölçülebilir faydasını gösterdi.

1.4.7 BGYS'nin Sektörlere Göre Uyarlamaları ve Farklılaşması

Bilgi güvenliği gereksinimleri, her sektörde aynı yoğunlukta veya öncelikte olmayabilir. Bu nedenle Bilgi Güvenliği Yönetim Sistemlerinin sektörel özelliklere göre özelleştirilmesi büyük önem taşımaktadır. Örneğin, bir finans kuruluşu ile bir üniversite aynı ISO/IEC 27001 çerçevesine bağlı kalsa da, uygulama detayları, kontrol öncelikleri ve yasal yükümlülükleri büyük oranda farklılık gösterir.

Finans sektöründe BGYS, sıkı regülasyonlara, para transferi süreçlerinin korunmasına ve dolandırıcılık öncesi risk yönetimine odaklanır. Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) rehberleri bu sektörde ISO 27001 uygulamalarını destekler niteliktedir. Sağlık sektöründe ise Hasta Verilerinin Korunması, HIPAA (ABD) veya KVKK (Türkiye) gibi düzenlemeler çerçevesinde veri mahremiyeti daha ön plandadır. Sağlık bilgilerine erişim kısıtlamaları, rol tabanlı erişim ve acil durum senaryoları bu sistemlerde çok daha karmaşık biçimde planlanmalıdır (Furnell, 2021).

Enerji ve altyapı sektörlerinde ise BGYS, fiziksel ve dijital varlıkların birlikte korunmasını gerektirir. Bu sektörde SCADA sistemleri gibi endüstriyel kontrol sistemlerinin siber saldırılara karşı savunulması önceliklidir. Ayrıca, kamu kurumlarında kamu ağı güvenliği, açık veri politikaları ve vatandaş verilerinin korunması öne çıkar (Furnell, 2021).

Vaka Örneği 1.4.7:

Bir devlet hastanesinde uygulanan BGYS sayesinde personelin hasta dosyalarına erişim seviyeleri sınırlanarak, izinsiz erişim vakaları %100 oranında önlenmiştir. Ancak aynı yapı bir bankaya aynen uygulanamaz; çünkü bankada işlem takibi ve hız farklı güvenlik önceliklerine sahiptir.

Tablo 1.4.7: Sektörel BGYS Uygulama Karşılaştırması

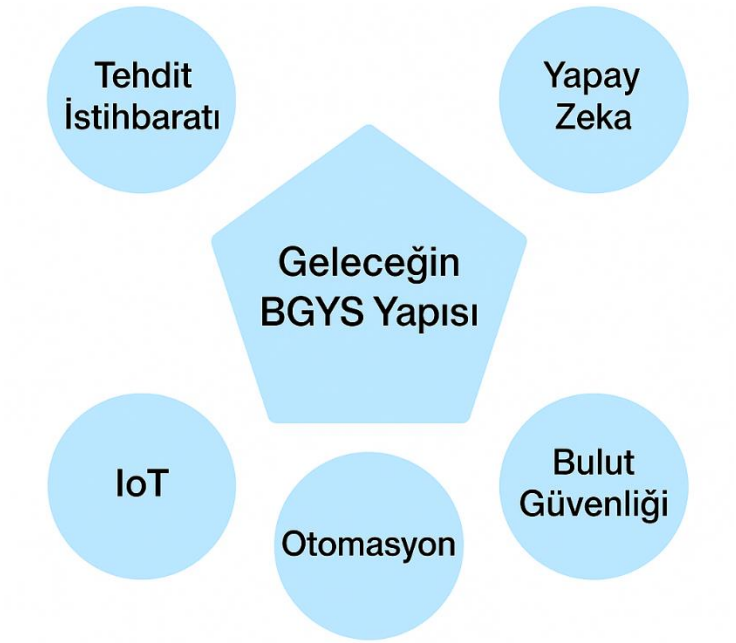
Sektör	Öncelikli Güvenlik Alanı	Regülasyonlar	BGYS Odak Noktası
Finans	İşlem Güvenliği	BDDK, Basel III	Olay müdahale, şifreleme
Sağlık	Hasta Verisi Mahremiyeti	KVKK, HIPAA	Rol tabanlı erişim, log kayıtları
Enerji	Endüstriyel Sistem Güvenliği	ISO 27019	Fiziksel/siber entegrasyon
Kamu	Vatandaş Verisi Koruma	E-Devlet, KVKK	Şeffaflık, denetim uyumu

1.4.8 BGYS'nin Geleceği ve Teknolojik Gelişmelerin Etkisi

Teknolojik gelişmeler, BGYS sistemlerini hem güçlendiren hem de zorlayan bir dinamiğe sahiptir. Özellikle yapay zeka, bulut bilişim, nesnelerin interneti (IoT) ve blokzincir gibi teknolojiler, bilgi güvenliğinde hem yeni çözümler hem de yeni tehditler ortaya çıkarmaktadır. Bu nedenle modern BGYS'lerin, yalnızca mevcut sistemleri değil, gelecekteki güvenlik ihtiyaçlarını da kapsayan esnek bir yapıda tasarlanması gerekmektedir.

Bulut sistemlerinde verilerin coğrafi olarak farklı noktalarda saklanması, veri egemenliği ve yedekleme stratejilerinin yeniden yapılandırılmasını zorunlu kılmaktadır. Ayrıca IoT cihazlarının çoğunun güvenlik katmanı içermemesi, endüstriyel ortamlar başta olmak üzere siber saldırganlar için açık kapı yaratmaktadır. Yapay zeka ise hem tehdit tespiti hem de saldırganlar açısından "akıllı" saldırı yöntemlerinin önünü açmaktadır.

BGYS'nin geleceği, tehdit istihbaratı, otomasyon, veri analitiği ve yapay zeka destekli kontrol sistemleriyle şekillenecektir. ISO 27001 ve 27002 standartlarının yeni sürümleri, bu gelişmeleri içerecek şekilde revize edilmektedir. Kurumların bu teknolojilere sadece yatırım yapmaları yetmez; aynı zamanda personel becerilerini ve yönetişim yapılarını da bu dönüşüme uyumlu hale getirmeleri gerekir (Tikk, Kaska, & Vihul, 2010).



Tehdit İstihbaratı + Yapay Zeka + Bulut Güvenliği + IoT + Otomasyon

Şekil 1.4.8: Geleceğin BGYS Yapısı

Vaka Örneği 1.4.8:

Bir üretim firması, IoT cihazlarını içeren üretim hattında saldırı yaşadı.

Olay sonrası tüm IoT cihazlarına özel ağ segmentasyonu ve izinsiz erişim tespiti için yapay zeka tabanlı sistemler entegre edildi.

Bu dönüşüm sonucunda sistem kesintileri %80 azaldı.

1.4.9 BGYS'nin Dış Kaynak Kullanımı ile İlişkisi

Modern işletmelerin sınırlı kaynaklar ve hızla değişen güvenlik tehditleri karşısında uzman dış hizmet sağlayıcılarla iş birliği yapması yaygın bir uygulamadır. BGYS süreçlerinde dış kaynak kullanımı; danışmanlık firmaları, bulut hizmet sağlayıcıları, siber güvenlik ekipmanları ve dış denetim firmaları şeklinde olabilir. Bu yapı kurumlara hem maliyet avantajı hem de uzmanlığa erişim imkanı sunmaktadır.

Ancak dış kaynak kullanımı, bilgi güvenliği açısından yeni sorumluluklar ve riskler doğurur. Kurumlar, dış hizmet sağlayıcılarının sözleşmelerle tanımlanmış güvenlik taahhütlerini sağlamasını teminat altına almalıdır. Hizmet seviyeleri, yedekleme prosedürleri, veri işleme izinleri ve kriz senaryoları net biçimde belirlenmelidir. Ayrıca üçüncü taraflara yönelik denetim prosedürleri uygulanmalı ve gerekiyorsa dış hizmet sağlayıcılar da ISO/IEC 27001 veya SOC gibi sertifikasyonlara sahip olmalıdır.

Etkin bir dış kaynak yönetimi için iş birliği yapılan firmalarla "Hizmet Seviyesi Anlaşması (SLA)", "Bilgi Güvenliği Protokolü" ve "Gizlilik Sözleşmesi (NDA)" imzalanmalıdır (Jaatun, Zhao, & Rong, 2009). Dış kaynak riski, risk envanterine dahil edilmeli, düzenli izlenmeli ve gerektiğinde alternatif sağlayıcılarla çalışmaya geçilmelidir (Jaatun, Zhao, & Rong, 2009).

Vaka Örneği 1.4.9:

Bir belediye, bilgi teknolojileri sistemlerini bir dış kaynak firmaya emanet etti.

Ancak yeterli güvenlik protokolleri sağlanmadığı için firma çalışanları sistem loglarına yetkisiz erişim sağladı.

Olay sonucunda firma ile olan sözleşme feshedildi, yeni hizmet sağlayıcı seçim süreci yeniden yapılandırıldı.

Tablo 1.4.9: BGYS Dış Kaynak Risk Analizi

Risk Türü	**Olası Sonuçlar**	**Kontrol Mekanizması**
Yetkisiz Erişim	Veri İhlali	SLA, erişim kontrolü, denetim
Süreç Uyuşmazlığı	Hizmet kesintisi	Süreç dokümantasyonu, yedek sağlayıcı
Hukuki Uyuşmazlık	Yasal ceza veya dava	Sözleşme yönetimi, danışman desteği

2. BİLGİ GÜVENLİĞİNE STRATEJİK YAKLAŞIM VE YÖNETİM PERSPEKTİFİ

2.1 Kurumsal Risk Yönetimi ile Entegrasyon

Bilgi güvenliği yönetim sistemlerinin (BGYS) etkinliği, yalnızca teknik güvenlik önlemlerinin uygulanmasıyla değil, aynı zamanda kurumsal risk yönetimi süreçlerine nasıl entegre edildiğiyle doğrudan ilişkilidir (ISO/IEC, 2022). Kurumsal risk yönetimi, organizasyonların finansal, operasyonel, hukuki ve bilgi güvenliğine ilişkin tüm risklerini tanımlayıp analiz etmelerini ve bu risklere karşı stratejik çözümler geliştirmelerini sağlar (Yılmaz & Yıldırım, 2020). BGYS'nin bu süreçle bütünleşmesi, bilgi güvenliği risklerinin sistematik bir yaklaşımla değerlendirilmesine olanak tanır.

Bu entegrasyon sayesinde bilgi güvenliği, organizasyonun stratejik karar alma yapılarıyla da uyumlu hale gelmektedir. BGYS, sadece teknik bir altyapı değil; aynı zamanda organizasyonun genel hedeflerini destekleyen stratejik bir bileşen haline gelmektedir (Calder & Watkins, 2018). Bilgi varlıklarının korunması yoluyla kurumun iç ve dış tehditlere karşı dayanıklılığı artırılır; risklere yönelik alınan önlemler proaktif ve sürdürülebilir bir şekilde şekillendirilir.

2.1.1 BGYS'nin Kurumsal Risk Yönetimine Katkısı ve Karar Alma Süreçleriyle Uyum

BGYS'nin kurumsal risk yönetimi ile bütünleşmesi, risklerin erken aşamalarda tespit edilmesini ve etkin şekilde yönetilmesini mümkün kılmaktadır (Gencer, 2015). Bu sistem, stratejik karar alma süreçlerinde bilgi güvenliği risklerinin de dikkate alınmasını sağlar. Üst düzey yöneticilerin bu entegrasyon sayesinde güvenlik odaklı kararlar alması kolaylaşır. Aynı zamanda BGYS, kurumsal hedeflerle uyumlu güvenlik politikalarının oluşturulmasını destekler.

2.1.2 Risk Değerlendirme ve İzleme Süreçlerinde BGYS'nin Rolü

BGYS, organizasyonların bilgi güvenliği risklerini tanımlamasına, değerlendirmesine ve sürekli olarak izlemesine yardımcı olan yöntem ve araçlar sunmaktadır (ISO/IEC, 2022). Risk analizleri, zafiyet değerlendirmeleri ve sürekli izleme sistemleri sayesinde tehditlere karşı dinamik ve esnek önlemler geliştirilebilir. Bu yapılar, zaman içinde değişen koşullara uyum sağlamada organizasyonlara çeviklik kazandırabilmektedir.

2.1.3 BGYS ile Kurumsal Hedefler Arasındaki Uyum

Bilgi güvenliği yalnızca günlük operasyonların korunmasıyla sınırlı değildir; aynı zamanda organizasyonun uzun vadeli hedeflerine ulaşmasında da belirleyici bir rol oynamaktadır (Demirtaş, 2013). BGYS, kurumsal risk yönetiminin bir parçası olarak stratejik hedeflerle uyumlu hale getirildiğinde, hem güvenlik bilinci yaygınlaşır hem de kurumun dayanıklılığı artar. Bu entegrasyon, güvenlik önlemlerini yalnızca bir zorunluluk değil, stratejik bir avantaj haline dönüştürür.

2.2 Stratejik Planlama, Kurumsal Hedefler ve Bilgi Güvenliği

Stratejik planlama, organizasyonların uzun vadeli hedeflerini gerçekleştirebilmek için gerekli olan yönetsel kararları sistematik biçimde belirlediği ve kaynaklarını bu doğrultuda yapılandırdığı süreçtir (Whitman & Mattord, 2022). Bu bağlamda bilgi güvenliği, yalnızca teknik bir unsur değil, stratejik planlamanın temel bileşenlerinden biri olarak değerlendirilmelidir. Güçlü bir Bilgi Güvenliği Yönetim Sistemi (BGYS), organizasyonun sürdürülebilirliğini, itibarını ve rekabet gücünü doğrudan etkileyen stratejik bir avantaj sağlar.

BGYS'nin stratejik planlama sürecine entegre edilmesi, sadece mevcut tehditlere karşı koruma sağlamakla kalmaz; aynı zamanda kurumun büyüme hedeflerine ulaşabilmesi

için güvenli ve kararlı bir altyapı oluşturur. Bu entegrasyon sayesinde, karar alma mekanizmaları daha sağlam ve veri odaklı bir zemine oturtulur, risk odaklı düşünce yapısı kurum kültürünün bir parçası haline gelir.

2.2.1 Bilgi Güvenliği Stratejilerinin Kurumsal Hedeflerle Uyumlaştırılması

Bilgi güvenliği stratejilerinin kurumsal hedeflerle bütünleşmesi, organizasyonun uzun vadeli vizyonuna hizmet eden stratejik bir gerekliliktir. Bilgi güvenliği yalnızca operasyonel risklerin azaltılmasını sağlamakla kalmaz; aynı zamanda organizasyonun itibarını, paydaş güvenini ve yasal uyumluluğunu da güçlendirir. BGYS'nin kurumsal hedeflerle uyumlu hale getirilmesi, bilgi güvenliğinin yalnızca teknik bir tedbir değil, aynı zamanda kurumsal değer üretiminin bir aracı olarak konumlanmasını sağlar.

Bu uyum süreci, yöneticilerin bilgi güvenliğini stratejik karar alma süreçlerine dahil etmelerini kolaylaştırır (Çetinkaya, 2008). Güvenliğin iş stratejileriyle paralel ilerlemesi; dijital dönüşüm projeleri, dış kaynak kullanımı ya da yeni pazar açılımları gibi alanlarda daha sağlıklı ve güvenli kararların alınmasını mümkün kılmaktadır.

2.2.2 Stratejik Karar Alma Süreçlerinde Bilgi Güvenliği Risklerinin Rolü

Bilgi güvenliği riskleri, stratejik karar alma süreçlerinde dikkate alınmadığında kurumları ciddi operasyonel ve yasal tehditlerle karşı karşıya bırakabilir. Bu nedenle, özellikle üst düzey yöneticilerin ve karar vericilerin, bilgi güvenliği risklerini stratejik değerlendirme kriterleri arasına yerleştirmesi kritik öneme sahiptir.

Stratejik kararlar,örneğin; yeni sistem yatırımları, birleşme & satın alma süreçleri ya da bilgi teknolojileri altyapısının modernizasyonu gibi bilgi güvenliği riski taşır. BGYS'nin bu karar süreçlerine entegre edilmesi, tehditlere karşı dirençli, krizlere karşı

hazırlıklı ve sürdürülebilir bir yapı oluşturulmasına katkı sağlar (Calder & Watkins, 2018).

2.2.3 Stratejik Planlama Sürecinde Bilgi Güvenliği Performansının İzlenmesi

Stratejik planlama süreci, yalnızca hedef belirleme ile sınırlı değildir; aynı zamanda belirlenen hedeflerin ne ölçüde başarıldığını ölçmeye yönelik performans izleme süreçlerini de içermektedir. BGYS'nin etkinliği, bu çerçevede periyodik olarak değerlendirilmeli ve güvenlik stratejileri güncel tehdit ortamına göre dinamik şekilde revize edilmelidir.

Performans göstergeleri (KPI'lar), bilgi güvenliği hedeflerinin ne ölçüde karşılandığını, hangi alanlarda zafiyet oluştuğunu ve hangi kontrollerin etkili olduğunu ortaya koymaktadır (Erdoğan, 2017). Bu göstergeler, sadece iç denetim süreçlerine değil, aynı zamanda stratejik planın genel başarısına da ışık tutar.

Tablo 2.2.3: Bilgi Güvenliği KPI Örnekleri

Performans Göstergesi	**Değerlendirme Aracı**	**İzleme Periyodu**
Aylık güvenlik ihlali sayısı	Güvenlik olay kayıtları	Aylık
Güncel yama uygulanma oranı	Bilgi teknolojileri sistem raporları	Haftalık
Bilgi güvenliği eğitimine katılım oranı	İnsan kaynakları kayıtları	3 ayda bir
İç denetim uyumsuzluk sayısı	İç denetim raporları	6 ayda bir

Bu bölümde bilgi güvenliği yönetimi ile stratejik planlama süreçlerinin nasıl iç içe geçtiği ve BGYS'nin sadece teknik değil, stratejik bir kaldıraç olduğu vurgulanmıştır.

Stratejik hedeflere ulaşmak isteyen kurumlar için bilgi güvenliği, sürdürülebilirliğin temel taşıdır.

2.3 Liderlik, İnsan Faktörü ve Güvenlik Kültürü

Bilgi güvenliği yönetim sistemlerinin başarısı yalnızca teknolojik altyapılara değil, aynı zamanda organizasyonel yapının sosyal ve kültürel unsurlarına da bağlıdır. Liderlik, insan faktörü ve güvenlik kültürü; bu sistemlerin işlevselliğini doğrudan etkileyen, birbiriyle iç içe geçmiş temel bileşenlerdir.

Organizasyonlar siber tehditlerle mücadele ederken yalnızca güvenlik duvarları ve antivirüs yazılımlarına değil, aynı zamanda güvenlik bilinci yüksek insan kaynağına ve bu bilinci destekleyen kurumsal liderliğe ihtiyaç duymaktadır (Schein, 2010). Güçlü bir güvenlik kültürü ise bu iki öğenin etkin şekilde yönetilmesiyle mümkündür.

2.3.1 Liderlik ve Güvenlik Kültürünün Oluşturulması

Liderlik, bilgi güvenliği kültürünün gelişiminde belirleyici bir unsurdur. Özellikle üst yönetimin bilgi güvenliği konusundaki tutumu ve kararlılığı, çalışanların güvenlik politikalarına uyum gösterme düzeyini doğrudan etkilemektedir. Etkin liderler, sadece politika ve prosedürleri onaylayan kişiler değil, aynı zamanda bu politikaları örnek davranışlarıyla pekiştiren rehberlerdir.

Liderlerin güvenlik vizyonu oluşturması, kaynak tahsisinde öncelik vermesi ve süreçleri sahiplenmesi; bilgi güvenliği stratejilerinin organizasyonel düzeyde benimsenmesini kolaylaştırmaktadır. Ayrıca liderlerin açık iletişim kurması, güvenlik konusunu yalnızca bilgi teknolojileri departmanının sorumluluğu olmaktan çıkarıp tüm organizasyonun ortak hedefi haline getirmesi açısından önemlidir (Schein, 2010).

2.3.2 İnsan Faktörü ve Farkındalık Temelli Güvenlik Yaklaşımı

Bilgi güvenliği zincirinin en zayıf halkası çoğu zaman insandır. Teknolojik sistemler ne kadar gelişmiş olursa olsun, insan hataları, kötü niyetli tıklamalar, zayıf şifre kullanımı veya farkında olmadan yapılan veri paylaşımı gibi etkenler büyük güvenlik açıklarına yol açabilir. Bu nedenle insan faktörü, bilgi güvenliği stratejilerinde öncelikli olarak ele alınması gereken bir konudur.

Etkin bir bilgi güvenliği yönetim sistemi, teknik kontrollerin yanı sıra insan odaklı önlemleri de kapsamalıdır (Furnell, 2021). Bunlar arasında sürekli eğitim programları, simülasyonlar (örneğin phishing testleri), davranış analizi temelli güvenlik değerlendirmeleri ve ödüllendirme sistemleri yer alabilir.

Tablo 2.3.2: İnsan Faktörüne Yönelik Farkındalık Faaliyetleri

Faaliyet Türü	**Açıklama**	**Uygulama Sıklığı**
E-posta üzerinden phishing testi	Gerçekçi senaryo ile çalışan farkındalığı ölçümü	Aylık
E-öğrenme modülü	Politika, parola güvenliği, veri erişimi konuları	3 ayda bir
Güvenlik bülteni	Güncel tehditler ve öneriler içeren içerik	Aylık
Canlı seminer/atölye	Etkileşimli sunum ve örnek vaka incelemesi	6 ayda bir

2.3.3 Güvenlik Kültürünün Oluşturulması ve Sürdürülmesi

Güvenlik kültürü, çalışanların bilgi güvenliğine dair ortak değer ve inançları benimsediği bir organizasyonel iklimdir. Bu kültür, yalnızca politikaların varlığıyla

değil, bu politikaların içselleştirilmesi ve davranışlara yansımasıyla inşa edilir. Güçlü bir güvenlik kültürü, bireylerin yalnızca kurallara uymalarını değil, gerektiğinde inisiyatif alarak güvenlik risklerine karşı önlem almalarını da sağlar.

Bu kültürün sürdürülebilirliği; sürekli eğitimlerle, liderlik desteğiyle, performans değerlendirmeleriyle ve açık iletişim mekanizmalarıyla sağlanabilir. Kurumlar; güvenlik kültürünü destekleyen ölçülebilir hedefler belirlemeli, çalışan geri bildirimlerini dikkate almalı ve başarıyı teşvik etmelidir (Erdoğan, 2016). Güvenlik kültürü oluşturulurken, yalnızca cezai yaklaşıma değil, pozitif davranış modeline dayalı ödüllendirme sistemlerine de yer verilmelidir.Liderlik desteği olmadan kültür gelişemez; farkındalık olmadan insan faktörü riski kontrol altına alınamaz; güvenlik kültürü olmadan hiçbir politika kalıcı hale gelemez.

2.4 Bilgi Güvenliği Yönetişimi ve Stratejik Kurumsallaşma

Bilgi güvenliği, sadece teknik kontrollerle değil, aynı zamanda yönetişim ilkeleri çerçevesinde stratejik düzeyde ele alındığında kurumsal sürdürülebilirliği destekleyen bir yapıya dönüşmektedir. Bilgi güvenliği yönetişimi, organizasyonun tüm kademelerinde güvenliğe dair sorumlulukların paylaşılması, karar alma süreçlerinin şeffaf ve izlenebilir olması, ve bilgi varlıklarının korunmasına yönelik politikaların kurum genelinde benimsenmesini sağlayan sistematik bir yaklaşımdır (Weill & Ross, 2004).

Yönetişim yapısı, bilgi güvenliği politikalarının sadece bilgi teknolojileri departmanlarının sorumluluğunda kalmamasını, yönetim kurulu ve üst düzey yöneticilerin de bu sürece aktif olarak dahil olmasını zorunlu kılar. Bu bağlamda oluşturulacak bilgi güvenliği komiteleri, hem risk değerlendirmesi hem de politika

güncellemeleri gibi stratejik kararlarda belirleyici rol oynar. Ayrıca bilgi güvenliği yönetişimi, iç denetim mekanizmalarıyla da entegre edilerek sürdürülebilirliği artırır.

Stratejik kurumsallaşma ise bilgi güvenliği uygulamalarının kalıcı ve tekrarlanabilir hale gelmesini sağlayan bir diğer temel unsurdur (Demir, 2018). Bu kapsamda kurumlar; bilgi güvenliği politikalarını yazılı standartlara dönüştürmeli, periyodik değerlendirmelerle uygulama sonuçlarını analiz etmeli ve bu süreçleri iç kontrol sistemlerine entegre etmelidir. Böylece bilgi güvenliği, bireysel inisiyatiflere bağlı olmaktan çıkar, kurumsal refleks haline gelir.

Kurumsal yönetişimle desteklenen bir BGYS yapısı; sadece kurum içi işleyişi güvence altına almakla kalmaz, aynı zamanda regülasyonlara uyum, dış denetimlerde şeffaflık ve müşteri güveni gibi dış faktörler açısından da stratejik avantaj sağlar.

Tablo 2.4: Bilgi Güvenliği Yönetişimi Unsurları

Unsur	**Açıklama**	**Uygulama Örneği**
Bilgi Güvenliği Komitesi	Karar alma ve denetim süreçlerini üstlenen birim	Bilgi teknolojileri, hukuk, insan kaynakları temsilcilerinden oluşur
Politika Sahipliği ve Güncelleme	Belge ve prosedürlerin sahiplenilmesi ve periyodik güncellenmesi	Her politika yılda en az bir kez gözden geçirilir
Performans Göstergeleri (KPI)	Güvenlik uygulamalarının ölçülebilirliği	Aylık saldırı sayısı, yanıt süresi, ihlal oranı
Uyumluluk ve Denetim	Yasal ve sektörel düzenlemelere tam uyumun sağlanması	ISO/IEC 27001, KVKK, GDPR denetimlerine hazırlık

Bilgi güvenliği yönetişimi ve stratejik kurumsallaşma birlikte ele alındığında, organizasyonlar sadece mevcut tehditlere değil, aynı zamanda uzun vadeli güvenlik vizyonlarına da hazırlıklı hale gelmektedir. Bu yaklaşım, bilgi güvenliğinin yalnızca teknik değil, aynı zamanda yönetsel bir sorumluluk olduğunu gösterir ve bilgi güvenliğini kurumsal rekabet avantajına dönüştürür.

3. BİLGİ GÜVENLİĞİ ÖRNEK UYGULAMALARI VE VAKA ANALİZLERİ

3.1 Başarılı BGYS Uygulamaları

Bilgi Güvenliği Yönetim Sistemleri (BGYS), yalnızca teknolojik altyapılarla değil; aynı zamanda yönetişim, risk farkındalığı, eğitim politikaları ve sürdürülebilir stratejilerle başarıya ulaşmaktadır (Calder & Watkins, 2018). Aşağıda, sektörler bazında BGYS'nin etkin şekilde uygulandığı örnekler sunulmaktadır.

3.1.1 Finans Sektöründe: Garanti BBVA Örneği

Stratejik Yaklaşım: Garanti BBVA, ISO/IEC 27001 standardını rehber edinerek bilgi güvenliğini kurumsal stratejinin merkezine konumlandırmıştır. Bu yaklaşım, dijital varlıkların korunmasının yanında müşteri verilerinin mahremiyetini de kapsayan geniş bir güvenlik yelpazesi sunmaktadır.

- **Çok Faktörlü Kimlik Doğrulama (MFA):** Erişim kontrolleri, MFA sistemleriyle güçlendirilerek yetkisiz erişimler engellenmektedir (ISO/IEC 27001:2022).
- **SIEM Altyapısı:** Güvenlik Olayı ve Bilgi Yönetimi (SIEM) sistemleriyle anlık tehdit algılama ve otomatik müdahale sağlanmaktadır.
- **Tedarikçi Güvenliği:** Üçüncü taraf erişimleri denetlenmekte ve risk bazlı kısıtlamalar uygulanmaktadır.
- **Siber Dayanıklılık:** Penetrasyon testleri ve kriz simülasyonları düzenli olarak gerçekleştirilmekte; çalışanlara sürekli eğitim verilmektedir.

3.1.2 Sağlık Sektöründe: Mayo Clinic (ABD)

Hastaya Özgü Güvenlik: Hasta gizliliği ve kritik veri korumasının öncelikli olduğu sağlık sektöründe Mayo Clinic, BGYS'yi hasta güvenliği politikalarıyla entegre ederek sektörde öncü konumda yer almaktadır.

- **Rol Bazlı Yetkilendirme:** EHR sistemlerine erişim yalnızca ilgili personelle sınırlı tutulur.
- **Tıbbi Cihaz Güvenliği:** Tüm medikal cihazlar ağ içinde davranış analitiğiyle izlenmekte ve güvenlik politikalarına göre sınıflandırılmaktadır.
- **Veri Anonimleştirme:** Kişisel veriler analizlerde şifreleme ve anonimleştirme yöntemleriyle işlenir (Gritzalis, D., Kandias, M., Stavrou, V., & Mitrou, L. 2014).

3.1.3 Teknoloji Sektöründe: Microsoft ve "Zero Trust" Modeli

Yapısal Dönüşüm: Microsoft'un benimsediği "Zero Trust" yaklaşımı, her kullanıcı ve her erişimi potansiyel tehdit olarak değerlendiren proaktif bir güvenlik felsefesidir.

- **Kimlik Temelli Denetim:** Kullanıcı davranışı, cihaz güvenirliği ve lokasyon gibi değişkenler analiz edilerek erişim kararı verilir (Jaatun, Zhao, & Rong, 2009).
- **Mikro Segmentasyon:** Ağ, küçük güvenlik bölgelerine ayrılarak saldırıların yayılması engellenir.
- **Tehdit İstihbaratı:** Yapay zeka destekli sistemlerle güncel tehditler sürekli analiz edilir.

3.2 Güvenlik İhlalleri ve Risk Yönetimi Başarısızlıkları

Başarısız BGYS uygulamaları, genellikle ihmal edilen güncellemeler, zayıf süreç yönetimi ve organizasyonel iletişim eksikliklerinden kaynaklanır (Calder & Watkins, 2018). Aşağıdaki örnekler, bu tür hataların sonuçlarını açıkça ortaya koymaktadır.

3.2.1 Equifax Veri Sızıntısı (2017)

- **Olay:** Apache Struts açık kaynak bileşenindeki bilinen bir zafiyet zamanında giderilmedi ve 147 milyon kullanıcının kişisel verisi sızdırıldı (Martin, A., Gupta, S., & Sanders, B. 2017).
- **Eksiklikler:** Zayıf yama yönetimi, sistem envanterinin eksikliği, müdahale süreçlerinin yetersizliği.
- **Sonuç:** 575 milyon dolar ceza, regülasyon baskısı ve itibar kaybı.

3.2.2 Target Saldırısı (2013)

- **Olay:** Güvenlik zafiyetine sahip bir taşeron üzerinden sızan saldırganlar, ödeme sistemlerine erişerek milyonlarca kredi kartı bilgisi çaldı.
- **Sorun:** Tedarikçi güvenliğinin göz ardı edilmesi ve ağ segmentasyonunun yetersizliği.
- **Ders:** Tedarik zinciri yönetimi bilgi güvenliği stratejisinin ayrılmaz parçasıdır (Humphreys, 2010).

3.2.3 British Airways Web Açığı (2018)

- **Olay:** Web uygulamasında tespit edilmeyen açık nedeniyle 500.000 müşterinin kredi kartı bilgileri sızdırıldı.
- **Eksiklikler:** Güvenlik testlerinin yetersizliği, veri şifrelemede standarda uyulmaması (Furnell, 2021).
- **Sonuç:** GDPR kapsamında yaklaşık 230 milyon dolar ceza.

3.3 Türkiye ve Dünyadan Kurumsal Örnekler

Bu bölümde ulusal ve uluslararası uygulamalar, karşılaştırmalı analizlerle değerlendirilmiştir.

3.3.1 Türkiye'den Başarı Örnekleri

- **TÜBİTAK:** Yerli yazılım, kriptografi çözümleri ve eğitimlerle kamu kurumlarına destek sağlar. KamuSM ile dijital imza ve e-belge sistemlerinde liderdir.
- **E-Devlet:** Kimlik doğrulama, erişim denetimi ve kullanıcı hareketlerinin kaydıyla BGYS ilkelerini yüksek seviyede uygular (Karakaya & Aydın, 2021).

3.3.2 Türkiye'de Karşılaşılan Zorluklar

Altyapı Yetersizlikleri, eğitim açığı ve kaynak kısıtları BGYS uygulamalarını sekteye uğratmaktadır (Demirtaş, 2013).

- **Altyapı Yetersizlikleri:** Eski donanım ve güncel olmayan ağ altyapıları.
- **Eğitim Açığı:** Personel farkındalığı düşük, güvenlik kültürü kurumsallaşmamış.
- **Kaynak Kısıtları:** Güvenlik için ayrılan bütçeler yetersizdir.

3.3.3 Uluslararası Başarı Örnekleri

Estonya:

- X-Road sistemiyle kamu verileri şifreli ve entegre şekilde paylaşılır.
- Erişimler izlenir, siber senaryolarla testler yapılır.
- Dijital kimlik ve oylama süreçleri güvenli yürütülür.

Singapur:

- CSA (Cyber Security Agency) ile tüm kamu altyapılarında BGYS merkezileştirilmiştir.
- Güvenlik sertifikaları zorunlu, sektörel bilgi paylaşımı aktif yürütülür.

Genel Değerlendirme

Yapılan vaka analizleri, etkili BGYS uygulamalarının teknik tedbirlerin çok ötesinde kurumsal irade ve yönetsel sürdürülebilirlikle mümkün olduğunu göstermektedir.

Başarılı örneklerin ortak noktaları:

- Üst yönetim desteği,
- Farkındalık odaklı eğitimler,
- Dinamik tehdit analizi,
- Denetlenebilirlik ve şeffaflık.

Başarısız örneklerin ortak sorunları:

- Zayıf güncelleme politikaları,
- Tedarikçi yönetiminin ihmal edilmesi,
- Yetersiz web güvenliği,
- Eğitim eksikliği ve kültür zafiyeti.

Sonuç olarak, bilgi güvenliği yalnızca bilgi teknolojiler birimlerinin değil; tüm kurumun, stratejik ve yönetsel düzeyde sahiplenmesi gereken bir öncelik olmalıdır.

4. BİLGİ GÜVENLİĞİNDE GELECEK ODAKLI DEĞERLENDİRMELER PERSPEKTİFİ

Bilgi Güvenliği Yönetim Sistemleri (BGYS), dijital dönüşümle birlikte durağan bir yapının ötesine geçerek sürekli evrilen, çevik ve öngörülü bir yapıya dönüşmektedir. Veri hacmindeki patlama, saldırı vektörlerinin çeşitlenmesi, teknolojik altyapıların hibritleşmesi ve yasal düzenlemelerin hızla gelişmesi, kurumların bilgi güvenliği stratejilerini geleceğe dönük olarak yeniden kurgulamalarını zorunlu hale getirmiştir (Çetinkaya, 2008; Demirtaş, 2013). Bu bölümde yapay zeka ve otomasyonun güvenlik mimarisine etkisinden, yeni nesil tehdit alanlarına ve gelişen düzenleyici çerçevelere kadar uzanan kapsamlı bir değerlendirme sunulmuştur.

4.1 Yapay Zeka ve Otomasyonun Rolü

Yapay zeka ve otomasyon, bilgi güvenliği alanında köklü bir dönüşüm yaratmakta; geleneksel, insan odaklı ve tepkisel yaklaşımların yerine öngörücü, sürekli izleyen ve kendi kendine karar verebilen sistemlerin kurulmasını sağlamaktadır.

4.1.1 Yapay Zeka Destekli Tehdit Tespiti ve Müdahale

Yapay zeka algoritmaları, devasa hacimdeki veriyi analiz ederek anomali tespiti yapabilir ve daha önce tanımlanmamış tehditleri dahi öngörebilir hale gelmiştir (Sadeghi, A., Wachsmann, C., & Waidner, M**.** 2020).

- **Kullanıcı Davranış Analizi (UEBA):** Olağan dışı erişim girişimleri, sistem içi hareketlilik ve dosya davranışları analiz edilerek şüpheli aktiviteler anında tespit edilebilmektedir (Rani, M., Kumar, V., & Singh, A. 2021).

- **Sıfırıncı Gün Saldırılarıyla Mücadele:** Yapay zeka destekli sistemler, geleneksel imza tabanlı çözümlerle tespit edilemeyen yeni tehditleri sezgisel olarak tanımlayabilir (Alotaibi, 2023).

4.1.2 Otomasyon ile Sürekli İzleme ve Uyum Denetimi

- **Politika Uyumluluğu ve Sürekli Gözlem:** ISO/IEC 27001, NIST gibi standartlara uygunluk otomatikleştirilmiş betikler aracılığıyla sürekli denetlenebilmektedir (Gencer, 2015).
- **Anlık Risk Skorlama:** Sistemler üzerindeki değişiklikler gerçek zamanlı izlenerek risk skorlamaları yapılmakta ve otomatik uyarı mekanizmaları çalıştırılmaktadır (Güldüren, 2015).

4.1.3 Güvenlik Operasyon Merkezlerinin (SOC) Evrimi

Yapay zeka tabanlı SOC yapıları, reaktif bir yapıdan çıkıp tehdit avcılığı (threat hunting), önceliklendirme ve karar destek sistemleriyle proaktif bir yapıya dönüşmektedir (IBM, 2023). Bu dönüşüm, olay yanıt sürelerinin kısalmasına ve güvenlik ekiplerinin yükünün azalmasına katkı sunmaktadır.

4.2 Yeni Tehditler ve Genişleyen Saldırı Yüzeyleri

Dijitalleşme ile birlikte saldırganların kullandığı araçlar gelişmiş, kurumların saldırı yüzeyleri genişlemiştir. Geleceğe dönük BGYS stratejilerinde aşağıdaki yeni tehdit alanları öncelikli olarak ele alınmalıdır.

4.2.1 Nesnelerin İnterneti (IoT) Güvenliği

- **Zayıf Kimlik Doğrulama:** Varsayılan şifrelerin değiştirilmemesi, IoT cihazlarını doğrudan hedef haline getirmektedir.

- **Firmware Güvencesizliği:** Yazılım güncellemeleri sırasında yetkisiz müdahale riski yüksektir; güvenli güncelleme altyapısı kurulmalıdır.

4.2.2 Yapay İçerik Tabanlı Tehditler (Deepfake, Ses Klonlama)

- **Sahte Video/Ses ile Kimlik Avı:** Yöneticilere aitmiş gibi gösterilen videolar ve klon sesler, sosyal mühendisliğe dayalı saldırılarda kullanılmaktadır.
- **Sesli Doğrulama Sistemlerinin Atlama Riski:** IVR tabanlı güvenlik sistemleri ses manipülasyonlarıyla kandırılabilmektedir.
- Deepfake ve ses klonlama gibi teknolojilerle kimlik avı saldırılarında artış gözlenmektedir (Marhad, Abd Goni & Abdullah Sani, 2024).
- Bu durum sesli doğrulama sistemlerinin güvenilirliğini de tehdit etmektedir.

4.2.3 Bulut ve Hibrit Ortamlarda Güvenlik Zorlukları

- **Yanlış Yapılandırmalar:** Bulut tabanlı platformlarda yapılan erişim yapılandırma hataları büyük ölçekli veri sızıntılarına yol açabilmektedir (Whitman & Mattord, 2022).
- **Yetki Çakışmaları:** DevOps süreçlerinde tanımlanamayan otorite sınırları, yetki suistimallerine açık kapı bırakmaktadır.

4.3 Regülasyonlar ve Uyumluluk (KVKK, GDPR ve Ötesi)

Gelecekte bilgi güvenliği yalnızca teknik değil, aynı zamanda hukuki ve etik bir sorumluluk haline gelmektedir. Kurumlar, değişen regülasyonlara uyum sağlamak zorundadır.

4.3.1 KVKK ve GDPR: Kapsam ve Yaklaşım Farkları

KVKK ve GDPR'ın hem kapsam hem de uygulama açısından önemli farklılıkları bulunmaktadır. KVKK, veri minimizasyonuna ve açık rızaya odaklanırken; GDPR, veri taşınabilirliği ve unutulma hakkı gibi kavramları da içermektedir (Erdoğan, 2016; Erdoğan, 2017).

- **KVKK (Türkiye):** Açık rıza, veri minimizasyonu, amaçla sınırlı işleme ve güvenlik ilkeleri temel alınmaktadır.
- **GDPR (AB):** "Unutulma hakkı", "veri taşınabilirliği" ve "veri koruma etki değerlendirmesi (DPIA)" gibi detaylı hak ve yükümlülükler sunmaktadır.

4.3.2 Uyum Süreçlerinde Yaşanan Zorluklar

Büyük kurumlar için veri envanteri oluşturmak, farklı regülasyonlara aynı anda uyum sağlamak önemli bir zorluktur (Demir, 2018).

- **Veri Envanteri Oluşturma:** Özellikle büyük kurumlarda veri akışlarını tanımlamak ve görselleştirmek oldukça zordur.
- **Çoklu Regülasyona Uyum:** Aynı anda KVKK, GDPR ve sektörel düzenlemelere uyum sağlamak hem maliyet hem de insan kaynağı açısından zorlayıcıdır.

4.3.3 Sektörel Düzenlemeler ve Farklılaşmalar

- **Finans Sektörü:** BDDK ve PCI-DSS standartlarına uyum zorunludur. Sıkı şekilde denetlenmektedir.
- **Sağlık Sektörü:** ISO 27799 gibi özel standartlara tabidir (Güldüren, 2015) ve Sağlık Bakanlığı yönetmelikleri hasta verilerinin korunmasını şart koşar.

- **Kritik Altyapılar:** Sektör bazlı devlet müdahale alanları oluşturulmuştur. Enerji, ulaştırma ve haberleşme gibi sektörlerde özel siber güvenlik yükümlülükleri ve devlet müdahale alanları belirlenmiştir.

4.3.4 Geleceğe Yönelik Regülasyon Trendleri

Avrupa Birliği'nin yeni regülasyonları (örneğin AI Act, DORA) yapay zeka ve dijital dayanıklılık üzerine yeni çerçeveler sunmaktadır (Calder & Watkins, 2018).

- **AI Act (AB):** Yapay zeka sistemlerinin şeffaflığı, denetlenebilirliği ve etik ilkeler çerçevesinde sınıflandırılması gündemdedir.
- **DORA:** Finansal kuruluşlar ve teknoloji sağlayıcılarının dijital dayanıklılıklarının ölçülmesi ve zorunlu testlerden geçirilmesi planlanmaktadır.
- **Veri Egemenliği ve Bulut Yönetişimi:** Ulusal veri merkezlerinin önemi artmakta; sınır ötesi veri aktarımı ciddi biçimde düzenlenmektedir.

Bilgi güvenliği yönetimi artık sadece bugünün tehditlerine karşı değil, geleceğin teknolojik ve hukuki zorluklarına karşı da kurumsal bir direnç oluşturmak anlamına gelmektedir. Geleceğe dönük BGYS stratejileri;

- Yapay zeka ve otomasyonun entegre edilmesi,
- Yeni nesil tehditlerin tanımlanması,
- Değişen yasal çerçevelere uyum,
- Kurum içinde güvenlik kültürünün olgunlaştırılması

gibi boyutlarıyla kurumsal sürdürülebilirliğin temel unsurlarından biri haline gelmiştir. Bu bağlamda bilgi güvenliği, sadece bilgi teknolojileri birimlerinin değil, tüm organizasyonun ortak ve stratejik sorumluluğu olmalıdır.

SONUÇ

Bu rapor çalışması, Bilgi Güvenliği Yönetim Sistemleri (BGYS) bağlamında risk yönetimi, stratejik yönetişim, teknolojik dönüşüm, insan faktörü, düzenleyici çerçeveler ve örnek olay analizleri aracılığıyla çok katmanlı bir bakış açısı sunarak, bilgi güvenliğinin yalnızca teknik bir mesele değil; aynı zamanda yönetsel, kültürel ve politik bir gereklilik olduğunu ortaya koymuştur. Dijitalleşmenin hız kazandığı bu çağda, kurumların sürdürülebilir başarısı, bilgi varlıklarını koruma kabiliyetiyle doğrudan ilişkilidir.

Çalışmanın teknik düzeydeki bulguları, bilgi güvenliği uygulamalarının başarıya ulaşabilmesi için yalnızca belirli teknolojik çözümlerin değil, bu çözümlerin sistematik entegrasyonunun da gerekli olduğunu göstermektedir. Özellikle ISO/IEC 27001 standardının sunduğu Planla–Uygula–Kontrol Et–Önlem Al (PUKÖ) döngüsü; bilgi güvenliği süreçlerinin sürekliliğini sağlamada kritik rol oynamaktadır. Başarılı uygulama örneklerinde, güvenlik duvarları, çok faktörlü kimlik doğrulama sistemleri, veri sınıflandırma politikaları ve ağ segmentasyonu gibi teknik önlemler, güvenlik olaylarının etkisini önemli ölçüde azaltmaktadır. Bununla birlikte, otomasyon, tehdit istihbaratı sistemleri ve yapay zeka temelli davranış analizleri gibi yeni nesil teknolojiler, saldırıların erken tespiti ve etkili müdahale süreçleri açısından vazgeçilmez hale gelmiştir. Ancak Equifax örneğinde olduğu gibi, yetersiz yama yönetimi, zayıf erişim kontrolleri ve altyapı eksiklikleri büyük ölçekli veri ihlallerine zemin hazırlamaktadır. Bu bulgular, teknik altyapının sürekli izlenmesi, denetlenmesi ve güncellenmesinin bilgi güvenliği açısından yaşamsal önemde olduğunu ortaya koymaktadır.

Yönetsel düzeyde ise bilgi güvenliği, sadece bilgi teknolojileri birimlerinin değil, tüm kurumun ortak stratejik sorumluluğudur. Üst yönetim desteği olmaksızın hiçbir BGYS girişimi kalıcı başarı sağlayamaz. Güvenlik kültürünün oluşturulması ve sürdürülmesi açısından liderliğin rolü kritik olup, Garanti BBVA örneğinde görüldüğü üzere, üst yönetimin güvenlik politikalarını kurumun genel iş hedefleriyle entegre etmesi başarıyı beraberinde getirmiştir. İnsan faktörü ise, güvenlik zincirinin en zayıf halkası olmaya devam etmektedir. Etkili uygulamalar; düzenli farkındalık eğitimleri, görev tanımlarına güvenlik sorumluluklarının dahil edilmesi ve sınırlı erişim politikalarıyla bu zafiyeti minimize etmektedir. Öte yandan, kurum içi güvenlik kültürü yeterince gelişmediğinde, ne kadar güçlü teknik önlemler alınmış olursa olsun, ihmal kaynaklı güvenlik açıkları kaçınılmaz hale gelmektedir. Target ve British Airways vakaları bu gerçeği somut biçimde ortaya koymaktadır. Dolayısıyla, bilgi güvenliği yönetimi yalnızca sistemsel değil, aynı zamanda kültürel bir dönüşüm süreci olarak ele alınmalıdır.

BGYS uygulamaları aynı zamanda yasal ve politik sorumluluklar çerçevesinde değerlendirilmelidir. KVKK, GDPR, BDDK ve sektörel düzenlemeler bilgi güvenliğini etik bir gereklilik olmaktan çıkararak yasal bir zorunluluk haline getirmiştir. Avrupa Birliği'nde uygulanan GDPR; unutulma hakkı ve veri taşınabilirliği gibi kullanıcı haklarını ön plana çıkarırken, Türkiye'deki KVKK veri işleme faaliyetlerini daha sıkı kontrol altına almayı zorunlu kılmaktadır. Özellikle finans ve sağlık gibi hassas veri barındıran sektörlerde ISO 27799 ve PCI-DSS gibi standartlara uyum artık bir tercih değil, bir gerekliliktir. Bununla birlikte, bazı gelişmekte olan ülkelerde yasal uyum süreçleri çoğu zaman yalnızca denetime hazırlık olarak algılanmakta; bu da sürdürülebilir bir güvenlik kültürünün oluşmasını engellemektedir. Bu nedenle, yasal yükümlülüklerin yalnızca teknik denetimlerle değil, kurumsal politika ve farkındalık çalışmalarıyla da desteklenmesi gerekmektedir.

Son olarak, bilgi güvenliği yönetimi, teknoloji, yönetişim, sosyoloji ve hukuk gibi çok farklı disiplinlerin entegre bir şekilde yönetilmesini zorunlu kılmaktadır. Bu bağlamda, disiplinler arası bir olgunluk modelinin geliştirilmesi kaçınılmaz hale gelmiştir. Çalışmada analiz edilen örnekler, bilgi güvenliğinin yalnızca teknik bir konu değil; kurumun stratejik hedefleriyle doğrudan uyumlu bir yönetişim süreci olduğunu göstermektedir. Bilgi güvenliği, saldırılara karşı koruma sağlamanın ötesinde; müşteri güvenini artıran, kurumsal itibarı güçlendiren ve rekabet gücünü destekleyen kritik bir yapı taşıdır. BGYS'nin stratejik rolü sadece kriz yönetimi anlarında değil; iş sürekliliği, sürdürülebilirlik, dijital dönüşüm ve inovasyon gibi alanlarda da belirleyici hale gelmektedir. Bu nedenle bilgi güvenliği, artık yalnızca bir maliyet kalemi olarak değil; kurumun geleceğini şekillendiren stratejik bir yatırım alanı olarak değerlendirilmelidir.

GENEL DEĞERLENDİRME

Bilgi teknolojilerinin hızlı dönüşümü ve dijitalleşmenin kurumsal yapılar üzerindeki etkisi, bilgi güvenliğini yalnızca teknik bir zorunluluk olmaktan çıkarıp yönetsel, stratejik ve kültürel bir alan haline getirmiştir. Bu rapor, bilgi güvenliğini çok boyutlu bir yaklaşımla ele alarak Bilgi Güvenliği Yönetim Sistemleri'nin (BGYS) yalnızca bilgi teknolojileri birimlerine bırakılmaması, aksine tüm organizasyonun ortak sorumluluğu olarak değerlendirilmesi gerektiğini ortaya koymaktadır. Rapor boyunca yapılan analizler, bilgi güvenliğinin gizlilik, bütünlük ve erişilebilirlik ilkeleri doğrultusunda yürütülmesi gerektiğini vurgularken, bu üç temel kavramın kurumun iş sürekliliği, itibarı ve hukuki yükümlülükleri açısından kritik bir rol oynadığını göstermektedir.

Kurumsal düzeyde bilgi güvenliğinin sürdürülebilirliği, teknik altyapının yanı sıra stratejik planlama, yönetişim, politika geliştirme ve çalışan farkındalığı gibi tamamlayıcı unsurlarla desteklenmelidir. Bu bağlamda BGYS; politika oluşturma, risk

yönetimi, olay müdahalesi, erişim kontrolleri ve sürekli iyileştirme gibi mekanizmalar aracılığıyla kurumsal bilgi varlıklarının korunmasına katkı sunmaktadır. ISO/IEC 27001 gibi uluslararası standartlara dayalı sistemlerin uygulanması, kurumların iç tehditlere karşı daha dirençli, dış saldırılara karşı ise daha hazırlıklı olmasını sağlamaktadır. Sistematik uygulama, aynı zamanda denetlenebilirlik, ölçülebilirlik ve sürekli gelişim döngüsünü de beraberinde getirmektedir.

Raporda incelenen ulusal ve uluslararası vaka analizleri, bilgi güvenliği uygulamalarının başarısının yalnızca teknolojik çözümlerle değil, aynı zamanda organizasyonel farkındalık, liderlik ve iş birliğine dayalı güvenlik kültürüyle desteklenmesi gerektiğini göstermektedir. Başarılı uygulamalarda görülen planlı risk yönetimi, proaktif denetim süreçleri ve sürekli eğitim faaliyetleri, güvenliğin yalnızca bir proje değil, kurumsal bir değer olarak ele alındığını ortaya koymaktadır. Buna karşılık başarısız uygulamalarda dikkat çeken ortak noktalar arasında; yetersiz güncellemeler, tedarik zinciri açıkları, insan hatası ve yönetişim eksiklikleri yer almaktadır.

Türkiye özelinde yapılan değerlendirmelerde, kamu kurumlarının BGYS konusundaki gelişim sürecinde farklı olgunluk seviyelerinde olduğu gözlemlenmiştir. TÜBİTAK, KamuSM ve e-Devlet gibi örneklerde olumlu sonuçlar elde edilirken, özellikle bazı kamu kuruluşlarında görülen altyapı yetersizlikleri, personel farkındalığı eksikliği ve süreçlerin merkezi olmayan yapısı bilgi güvenliğini tehdit eden faktörler arasında yer almaktadır. Bu durum, daha kapsayıcı ve koordineli ulusal stratejilere duyulan ihtiyacı gündeme getirmektedir.

Dijital dönüşümle birlikte ortaya çıkan yeni teknolojiler, bilgi güvenliğinin kapsamını daha da genişletmiştir. Yapay zeka, büyük veri, nesnelerin interneti ve bulut bilişim gibi gelişmeler, hem yeni güvenlik olanakları yaratmakta hem de karmaşık tehdit

senaryolarını gündeme getirmektedir. Zero Trust mimarisi gibi modern yaklaşımlar, güvenlik süreçlerinin yeniden tanımlanmasını gerektirmekte; geleneksel sınır temelli modellerin yerine adaptif ve sürekli izleme temelli sistemlerin benimsenmesini zorunlu kılmaktadır. Bu bağlamda, kurumların yalnızca mevcut riskleri yönetmesi değil, aynı zamanda geleceğe yönelik öngörüler geliştirmesi de bilgi güvenliği stratejilerinin ayrılmaz bir parçası olmalıdır.

Yasal düzenlemeler de bilgi güvenliğinin yönünü belirleyen temel etkenlerden biridir. KVKK ve GDPR gibi mevzuatlar, kurumlara yalnızca teknik değil etik ve hukuki sorumluluklar da yüklemektedir. Verilerin yasal çerçevede işlenmesi, kullanıcıların bilgilendirilmesi, açık rızanın alınması ve veri sızıntılarının hızlı şekilde raporlanması, hem kullanıcı haklarının korunması hem de kurumların itibarlarının sürdürülebilirliği açısından büyük önem taşımaktadır. Uyum süreçleri, sadece mevzuatlara karşı yükümlülüklerin yerine getirilmesi değil, aynı zamanda kurumsal sorumluluk bilincinin bir göstergesi olarak da değerlendirilmelidir.

Sonuç olarak bu değerlendirmeler, bilgi güvenliğinin sadece teknik bir zorunluluk olarak değil, stratejik bir rekabet avantajı ve kurumsal sürdürülebilirlik unsuru olarak görülmesi gerektiğini ortaya koymaktadır. Bilgi güvenliği, sürekli gelişen tehdit ortamında yalnızca korunması gereken bir unsur değil; aynı zamanda kurumların dijital çağdaki varlıklarını sürdürebilmesi için yapılandırılması gereken temel bir stratejik değerdir.

ÖNERİLER

Bilgi güvenliği, yalnızca teknik sistemlerin yönetimi değil, kurumsal kültürün, yönetişim anlayışının ve stratejik planlamanın bir bileşeni olarak ele alınmalıdır. Bu bağlamda, kurumların Bilgi Güvenliği Yönetim Sistemleri'ni (BGYS) daha etkin ve

sürdürülebilir bir şekilde uygulayabilmeleri için geliştirilen öneriler, çok boyutlu bir perspektifle değerlendirilmelidir. Öncelikle bilgi güvenliğinin kurumsal vizyon ve misyonla uyumlu hale getirilmesi, yalnızca bilgi teknolojileri departmanlarının değil, üst yönetim ve tüm paydaşların ortak sorumluluğu olarak benimsenmesi gerekmektedir. Bu doğrultuda yöneticilerin bilgi güvenliği stratejilerine açık taahhüt göstermesi, organizasyonel düzeyde güvenlik kültürünün yerleşmesini kolaylaştıracaktır. Üst düzey yöneticilerin katılımı yalnızca politika belirleme süreçlerinde değil, aynı zamanda uygulama, denetim ve kriz yönetimi aşamalarında da aktif olmalıdır.

İnsan faktörü, bilgi güvenliğinin en zayıf halkası olarak görülse de, etkin yönetildiğinde en güçlü savunma hattına da dönüşebilir. Bu nedenle tüm çalışanlara, görevlerine özel içeriklerle şekillendirilmiş sürekli eğitimler sunulmalıdır. Eğitimlerin yalnızca teorik bilgi aktarmakla sınırlı kalmaması, sosyal mühendislik, kimlik avı, parola güvenliği ve uzaktan çalışma gibi güncel tehditler üzerinden vaka temelli senaryolarla desteklenmesi önerilmektedir. Bilgi güvenliği farkındalığının yalnızca kampanya düzeyinde değil, içselleştirilmiş davranış biçimi haline gelmesi için kurum içi iletişim araçları etkin şekilde kullanılmalı; dijital afişler, hatırlatma e-postaları, kısa video içerikleri ve güvenlik bültenleri gibi materyaller yıl boyunca düzenli olarak yayımlanmalıdır.

Risk yönetimi, bilgi güvenliğinin stratejik merkezidir. Bu nedenle risk analizleri periyodik olarak güncellenmeli ve kurumun değişen tehdit ortamına göre yeniden yapılandırılmalıdır. Risk analizlerine yalnızca teknik veriler değil, aynı zamanda organizasyonel değişiklikler, tedarik zinciri yapısı ve çalışan sirkülasyonu gibi faktörler de dahil edilmelidir. Risk değerlendirmelerinin çıktıları, kurumun stratejik karar alma mekanizmalarına entegre edilmeli; risk iştahı ve tolerans eşiği net şekilde belirlenmelidir. Ayrıca, bilgi güvenliği olaylarına yönelik müdahale planları sadece kağıt üzerinde değil, düzenli tatbikatlarla test edilmeli ve güncellenmelidir. Kurumların

saldırı öncesi, sırası ve sonrasına dair kriz senaryoları oluşturması, siber dayanıklılık açısından büyük önem taşımaktadır.

Tedarikçi yönetimi, modern bilgi güvenliği stratejilerinin ayrılmaz bir parçasıdır. Özellikle bulut servis sağlayıcıları, dış danışmanlık firmaları ve üçüncü taraf yazılım entegratörleri ile yürütülen işbirliklerinde, sözleşmelere bilgi güvenliği taahhütleri açık ve denetlenebilir biçimde eklenmelidir. Tedarikçilerin güvenlik olgunluk düzeyleri düzenli aralıklarla denetlenmeli, yüksek risk taşıyan sağlayıcılara karşı alternatif planlar oluşturulmalıdır. Özellikle finans ve sağlık sektörlerinde, veri sınıflandırmasına dayalı olarak tedarikçilere erişim kısıtlamaları uygulanmalı ve erişim kayıtları şeffaf biçimde loglanmalıdır. Bu doğrultuda, üçüncü taraflara erişim sırasında çok faktörlü kimlik doğrulama ve mikro segmentasyon uygulamaları zorunlu hale getirilmelidir.

Teknoloji yatırımlarında yalnızca mevcut risklerin giderilmesi değil, gelecekteki tehditlerin öngörülmesi de önem taşımaktadır. Bu nedenle kurumlar, “Zero Trust” (Sıfır Güven) gibi modern güvenlik mimarilerini aşamalı olarak hayata geçirmelidir. Aynı zamanda, uç nokta tehdit algılama sistemleri (EDR/XDR), veri kaybı önleme yazılımları (DLP), merkezi log yönetimi ve tehdit istihbarat platformları gibi yeni nesil araçların entegrasyonu sağlanmalıdır. Kritik sistemler için düzenli penetrasyon testleri yapılmalı ve bulgular, bilgi güvenliği stratejilerinin yeniden şekillendirilmesinde referans alınmalıdır. Bu teknolojik yatırımlar, yalnızca bilgi teknolojileri bütçesinden değil, stratejik kurumsal bütçeden finanse edilmelidir.

Yasal uyum ve düzenlemelere yönelik uygulamalar, kurumların bilgi güvenliği stratejilerini yalnızca sürdürülebilir değil aynı zamanda denetlenebilir hale getirmektedir. KVKK ve GDPR gibi düzenlemelere uyum için kapsamlı veri envanteri çıkarılmalı, kişisel veriler sınıflandırılmalı ve her veri kümesinin işlenme amacı, süresi

ve yasal dayanağı net şekilde belirlenmelidir. Ayrıca, veri koruma görevlileri (DPO) görevlendirilerek yasal uyum ile teknik uygulamalar arasında köprü kurulmalıdır. Şikayet yönetimi ve veri ihlali bildirim süreçleri için kurum içi yönlendirme prosedürleri geliştirilmeli ve çalışanlara bu konuda özel eğitim verilmelidir. Tüm bu adımlar, kurumun yalnızca yasal sorumluluklarını değil, aynı zamanda etik sorumluluklarını da yerine getirmesini sağlar.

Son olarak, kurumların geleceğe hazırlanması için siber dayanıklılık perspektifiyle hareket etmesi gerekmektedir. Yapay zeka, IoT, blockchain ve kuantum bilişim gibi teknolojilerin güvenli entegrasyonu için bugünden yol haritaları hazırlanmalı; bu teknolojilerin getireceği potansiyel tehditlere karşı senaryolar geliştirilmelidir. Ulusal düzeyde kamu–özel sektör iş birlikleri artırılmalı; ortak tehdit istihbaratı paylaşım platformları kurulmalı ve üniversite–sanayi–devlet üçgeninde yerli güvenlik teknolojileri desteklenmelidir. Bu tür ortaklıklar, sadece kurumsal düzeyde değil, ulusal siber güvenlik ekosistemi açısından da stratejik önem taşımaktadır.

KAYNAKÇA

1. **Aktaş, K.** (2020). *ISO 27001 bilgi güvenliği yönetim sistemi: Erişim kontrol politikası üzerine bir inceleme* (Yüksek lisans tezi). Doğuş Üniversitesi.
2. **Alimardani, M., & Hashemi, S.** (2022). *Bilgi güvenliği yönetim sistemlerinin organizasyonel performansa etkisi.* Bilgi Yönetimi Dergisi, 17(2), 123–145.
3. **Alotaibi, S.** (2023). Artificial intelligence in cybersecurity: Techniques and challenges. International Journal of Cyber Research, 12(2), 55–68.
4. **Bilgi Teknolojileri ve İletişim Kurumu (BTK)**. (2022). *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020–2023)*. https://www.btk.gov.tr
5. **Björck, F. J.** (2005). *Discovering information security management* (Yüksek lisans tezi). Stockholm University.
6. **Calder, A., & Watkins, S.** (2018). *Information security risk management for ISO 27001/ISO 27002*. IT Governance Publishing.
7. **Calder, A., & Watkins, S.** (2019). *IT governance: An international guide to data security and ISO27001/ISO27002*. Kogan Page.
8. **Çek, E. (2017).** *Kurumsal bilgi güvenliği yönetişimi ve bilgi güvenliği için insan faktörünün önemi* (Yüksek lisans tezi). İstanbul Bilgi Üniversitesi.
9. **Çetinkaya, M.** (2008). *Bilgi güvenliği yönetim sistemi altyapısının değerlendirilmesi için bir test aracı geliştirilmesi* (Yüksek lisans tezi). İstanbul Kültür Üniversitesi.
10. **Cyber Security Agency of Singapore.** (2022). *National cybersecurity strategy*. https://www.csa.gov.sg/
11. **Demir, C.** (2018). Şeffaflığı artırmaya yönelik mekanizmalar ve finansal başarının değerlendirilmesi. DergiPark. https://dergipark.org.tr/tr/download/article-file/941275

12. **Demirtaş, H.** (2013). *Bilgi güvenliği yönetiminin gerekleri ve başarı dayanakları: Bir uygulama örneği* (Yüksek lisans tezi). Sakarya Üniversitesi.
13. **Domínguez-Domínguez, R., Flores-Laguna, O. A., & del Valle-López, J.** (2023). Evaluation of an information security management system at a Mexican higher education institution. arXiv. https://arxiv.org/abs/2306.11050
14. **ENISA – European Union Agency for Cybersecurity.** (2021). *Threat landscape report*. https://www.enisa.europa.eu/publications
15. **ENISA.** (2022). *Threat landscape report 2022*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
16. **Erdoğan, Ş.** (2016). Kurumsal yönetim ilkeleri ışığında şeffaflık ve Türkiye uygulaması. Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi, 18, 45–61.
17. **Erdoğan, Ş.** (2017). Kurumsal yönetimde kamuyu aydınlatma ve şeffaflık ilkesinin yeri ve önemi. Journal of Economics and Political Economy, 4, 186–199.
18. **Estonian Information System Authority.** (2020). *Cyber security strategy 2020–2030*. https://www.ria.ee/en/cyber-security.html
19. **Furnell, S.** (2021). *Cybersecurity: Everything you need to know about computer security and how to stay safe online*. Springer.
20. **Gencer, K.** (2015). *ISO 27001 kapsamında kurumsal bilgi güvenliğine dinamik bir yaklaşım* (Yüksek lisans tezi). Afyon Kocatepe Üniversitesi.
21. **Giritli, H. S.** (2020). *Bilgi güvenliği yönetim sistemleri ve uygulamaları*. Seçkin Yayıncılık.
22. **Gritzalis, D., Kandias, M., Stavrou, V., & Mitrou, L.** (2014). History of information: The case of privacy and security in medical information systems. International Journal of Medical Informatics, 84(6), 340–354.

23. **Güldüren, C.** (2015). *Yükseköğretim kurumlarındaki öğretim elemanlarının bilgi güvenliği farkındalık düzeylerinin değerlendirilmesi* (Doktora tezi). Ankara Üniversitesi.
24. **Gürcan, İ. A.** (2014). *Finans sektörü için bilgi güvenliği yönetim gereksinimlerinin ISO 27001 tabanlı incelenmesi* (Yüksek lisans tezi). İstanbul Üniversitesi.
25. **Humphreys, E.** (2010). Information security management standards: Compliance, governance and risk management. *Information Security Technical Report*, 15(2), 55–65.
26. **IBM.** (2023). *AI in SOC: A paradigm shift in security operations*. IBM Security Whitepaper.
27. **ISO/IEC.** (2018). *ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management*. International Organization for Standardization.
28. **ISO/IEC.** (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. International Organization for Standardization.
29. **Jaatun, M. G., Zhao, G., & Rong, C.** (2009). Trust and accountability in cloud computing. In *Proceedings of the 2009 7th International Conference on Ubiquitous Intelligence & Computing* 104–115. IEEE.
30. **Kamu Sertifikasyon Merkezi (KamuSM).** (2023). *Güvenli e-imza ve e-belge hizmetleri*. https://kamusm.bilgem.tubitak.gov.tr
31. **Kara, M.** (2021). *Kurumsal bilgi güvenliği yönetim sistemlerinde risk değerlendirme modelleri* (Yüksek lisans tezi). İstanbul Teknik Üniversitesi.
32. **Karakaya, A., & Aydın, A.** (2021). Türkiye'de e-devlet hizmetlerinin bilgi güvenliği yönünden değerlendirilmesi. Bilişim Teknolojileri Dergisi, 14(1), 15–24.

33. **Kişisel Verileri Koruma Kurumu (KVKK).** (2020). *Veri güvenliğine yönelik teknik ve idari tedbirler rehberi*. https://www.kvkk.gov.tr
34. **Marhad, S. S., Abd Goni, S. Z., & Abdullah Sani, M. K. J.** (2024). Implementation of information security management systems for data protection in organizations: A systematic literature review. European Journal of Business and Management Research, 9(18), 54–83.
35. **Marhad, M. R. A. R., Abd Goni, A. M., & Abdullah Sani, M. F.** (2024). Deepfake threats and ethical governance in digital environments. Journal of Information Ethics, 33(1), 12–24.
36. **Martin, A., Gupta, S., & Sanders, B.** (2017). The Equifax breach: An examination of failures. Journal of Cybersecurity Policy, *2*(3), 45–56.
37. **Microsoft.** (2020). *Zero trust security model whitepaper*. https://learn.microsoft.com/en-us/security/zero-trust/
38. **Mayo Clinic.** (2021). *Privacy and security practices in patient care systems*. https://www.mayoclinic.org/
39. **National Institute of Standards and Technology (NIST).** (2020). *Framework for improving critical infrastructure cybersecurity*. https://www.nist.gov/cyberframework
40. **Ponemon Institute.** (2019). *Cost of a data breach report*. IBM Security. https://www.ibm.com/security/data-breach
41. **Rani, M., Kumar, V., & Singh, A.** (2021). User behavior analytics for cybersecurity using machine learning. Cybersecurity Advances, *4*(3), 35–50.
42. **Sadeghi, A., Wachsmann, C., & Waidner, M.** (2020). Security and privacy challenges in Industrial Internet of Things. In Proceedings of the Design, Automation & Test in Europe Conference & Exhibition 1230–1235.

43. **SANS Institute.** (2016). *Security awareness planning kit*. https://www.sans.org/security-awareness-training/

44. **Schein, E. H.** (2010). *Organizational culture and leadership* (4th ed.). Jossey-Bass.

45. **Sipahi, M., & Kalkan, A.** (2022). Risk yönetimi ve bilgi güvenliği stratejileri. In A. Demir & B. Kaya (Eds.), *Bilgi teknolojilerinde güvenlik yaklaşımları* 45–78. Nobel Akademik Yayıncılık.

46. **Smith, J. L.** (2020). *Strategic risk management in information security systems* (Unpublished master's thesis). University of California, Berkeley.

47. **Tikk, E., Kaska, K., & Vihul, L.** (2010). *International cyber incidents: Legal considerations*. Cooperative Cyber Defence Centre of Excellence.

48. **Tuygun, M.** (2019). *ISO 27001 bilgi güvenliği yönetim sistemi standardının kamu kurumlarına uygulanabilirliğinin araştırılması: Ankara ili örneği* (Yüksek lisans tezi). Gazi Üniversitesi, Bilişim Enstitüsü.

49. **TÜBİTAK.** (2023). *Türkiye'de bilgi güvenliği yönetim sistemlerinin mevcut durumu ve öneriler*. https://www.tubitak.gov.tr/tr/raporlar/bilgi-guvenligi-raporu-2023.pdf

50. **TÜBİTAK BİLGEM.** (2021). *Kamu kurumlarında bilgi güvenliği yönetimi rehberi*. https://bilgem.tubitak.gov.tr

51. **Ulaştırma ve Altyapı Bakanlığı.** (2021). *Dijital Türkiye raporu*. https://www.uab.gov.tr

52. **Weill, P., & Ross, J. W.** (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business School Press.

53. **Whitman, M. E., & Mattord, H. J.** (2022). *Principles of information security* (7th ed.). Cengage Learning.

54. **Yalçın, A.** (2020). Bilgi güvenliği yönetim sistemi (BGYS) standartlarının Türkiye'deki kamu kurumlarında uygulanabilirliği. Savunma Bilimleri Dergisi, 19(1), 1–21.
55. **Yıldırım, H., & Demir, E.** (2023). Siber güvenlik risklerinin analizi: Türkiye'de kamu kurumları üzerine bir çalışma. Siber Güvenlik ve Yönetim, 5(1), 45–67.
56. **Yılmaz, E., & Yıldırım, B.** (2020). Bilgi güvenliği risk yönetimi ve ISO 27001 uygulamaları üzerine bir değerlendirme. Bilgi Ekonomisi ve Yönetimi Dergisi, 15(1), 45–64.

ÖZET

Günümüzün hızla dijitalleşen dünyasında bilgi güvenliği, yalnızca teknik bir zorunluluk olmanın ötesine geçerek; kurumsal sürdürülebilirliğin sağlanması, itibarı koruma ve rekabet üstünlüğü elde etme açısından stratejik bir öncelik haline gelmiştir. Artan siber tehditler, veri ihlalleri, mevzuatlara uyum gereklilikleri ve kamuoyunun güven beklentisi, kurumların bilgi varlıklarını sistematik biçimde korumasını her zamankinden daha kritik bir gereklilik haline getirmiştir. Bu nedenle, bilgi güvenliği sistemleri ile risk yönetimi süreçlerinin entegre ve stratejik bir yaklaşımla ele alınması zorunlu hale gelmiştir.

Bu çalışma, bilgi güvenliği sistemleri kapsamında risk yönetiminin hem yapısal hem de stratejik boyutlarını ayrıntılı biçimde ele almayı amaçlamaktadır. Riskin tanımlanması, analiz edilmesi, kontrol altına alınması ve düzenli olarak izlenmesi gibi süreçler; bilgi güvenliğinin temel ilkeleri olan gizlilik, bütünlük ve erişilebilirlik ekseninde değerlendirilmiştir. Aynı zamanda, uluslararası düzeyde kabul görmüş ISO/IEC 27001 standardı, NIST ve ENISA rehberleri ile 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ve Genel Veri Koruma Tüzüğü (GDPR) gibi yasal düzenlemeler doğrultusunda kurumların güvenlik politikalarını nasıl oluşturmaları gerektiği ele alınmıştır.

Çalışmada, kamu ve özel sektöre ait çeşitli vaka analizleri üzerinden başarılı ve başarısız uygulamalar karşılaştırmalı biçimde incelenmiştir. Elde edilen bulgular, bilgi güvenliği risk yönetiminin yalnızca teknik kontrollerle sınırlı kalmadığını; bunun ötesinde kurumsal liderlik, güçlü bir güvenlik kültürü, çalışan farkındalığı ve stratejik planlama gibi unsurlarla doğrudan ilişkili olduğunu ortaya koymaktadır. Bu yönüyle

çalışma, bilgi güvenliği yönetişimini bütüncül ve stratejik bir bakış açısıyla ele almak isteyen uygulayıcılara ve karar vericilere kapsamlı bir rehber sunmayı hedeflemektedir.

Anahtar Kelimeler: Bilgi Güvenliği, Risk Yönetimi, Stratejik Yönetişim, Veri Koruma Mevzuatı, ISO/IEC 27001

ABSTRACT

In today's rapidly digitalizing world, information security has evolved beyond being a mere technical necessity and has become a strategic priority for ensuring organizational sustainability, protecting corporate reputation, and gaining competitive advantage. The increasing prevalence of cyber threats, data breaches, regulatory compliance requirements, and public trust expectations have made it more critical than ever for organizations to systematically protect their information assets. Consequently, integrating information security systems with risk management processes through a strategic and holistic approach has become indispensable.

This study aims to examine both the structural and strategic dimensions of risk management within the scope of information security systems. The processes of risk identification, analysis, mitigation, and continuous monitoring are evaluated within the framework of the fundamental principles of information security: confidentiality, integrity, and availability. Furthermore, international standards such as ISO/IEC 27001, NIST, and ENISA guidelines, as well as national and international legal regulations like the Turkish Personal Data Protection Law (KVKK) and the General Data Protection Regulation (GDPR), are discussed in relation to how organizations should formulate their security policies.

The study also presents a comparative analysis of successful and unsuccessful practices based on case studies from both public and private sectors. The findings reveal that information security risk management extends beyond technical controls and is closely linked to corporate leadership, a strong security culture, employee awareness, and strategic planning. In this context, the study aims to provide practitioners and decision-

makers with a comprehensive guide for adopting a strategic and integrated perspective on information security governance.

Key Words: Information Security, Risk Management, Strategic Governance, Data Protection Regulation, ISO/IEC 27001