Araştırma Makalesi / Research Article ESTU R 9(2), 2026, sy(243-264) DOI: 10.32569/resilience.1677230

RESILIENCE
e-ISSN: 2602-4667

Eskişehir Teknik Üniversitesi

Resilience

https://dergipark.org.tr/tr/pub/resilience

Siber Güvenlikte Dayanıklılık: Uluslararası Çerçevelerin değerlendirilmesi ve Yalın Uygulama Modeli Önerisi

Resilience in Cyber Security: Examining the International Frameworks and Basic Implementation Model Proposal

Füsun YAVUZER ASLAN[1], Bora ASLAN[1,*]

ORCİD 0000-0001-7096-3425
ORCİD 0000-0002-8069-8204

[1]*Kırklareli Üniversitesi, Mühendislik Fakültesi, Yazılım Mühendisliği 39750, Kırklareli, Türkiye*

Öne Çıkanlar / Highlights

- Siber dayanıklılık, sadece saldırıları önleme değil; hazırlık, müdahale ve toparlanma süreçlerini içeren bütüncül bir güvenlik yaklaşımı olarak ele alınmıştır.
- NIST, ENISA, ISO/IEC 27001, COBIT ve ITIL gibi uluslararası çerçeveler incelenmiş; bu yapılardan hareketle on temel sistem özelliği yapılandırılmıştır.
- Kısıtlı kurumsal kapasiteye sahip kuruluşlar için altı stratejik adıma dayanan yalın ve uygulanabilir bir siber dayanıklılık çerçevesi önerilmiştir.
- Cyber resilience is addressed as a holistic security approach that includes not only prevention, but also preparation, response, and recovery processes.
- International frameworks such as NIST, ENISA, ISO/IEC 27001, COBIT, and ITIL were examined, and ten key system characteristics were derived from them.
- A simplified and applicable cyber resilience framework consisting of six strategic steps is proposed for organizations with limited institutional capacity.

Makale Bilgisi / *Article Info*

Gönderim / Received: 15/04/2025
Kabul / Accepted: 11/12/2025
Online Erişim / Available online: 06/02/2026

Anahtar Kelimeler

Siber Güvenlik
Dayanıklılık
Güvenlik Standartları
Çerçeve Önerisi

Keywords

Cyber Security
Resilience
Safety Standards
Frame Proposal

Özet

Dijitalleşmenin hızla arttığı günümüzde, kurumların yalnızca siber tehditleri önlemeye değil aynı zamanda bu tehditlere karşı dayanıklılığını sürdürülebilir biçimde artırmaya yönelik bütüncül stratejiler geliştirmesi gerekmektedir. Bu çalışma siber güvenlikte dayanıklılık kavramını merkezine alarak modern bilgi sistemlerinin saldırılara karşı yalnızca korunmasını değil aynı zamanda saldırı anında işlevselliğini sürdürebilmesini ve sonrasında hızla toparlanabilmesini sağlayacak yapısal ve yönetsel özellikleri incelemektedir. Çalışma kapsamında öncelikle NIST, ENISA, ISO/IEC 27001, COBIT ve ITIL gibi uluslararası düzeyde kabul görmüş çerçeve ve standartlar analiz edilmiş ardından bu yapılar temel alınarak belirlenen on sistem özelliği açıklanmıştır. Buna ek olarak bu çerçeveleri uygulayacak kurumsal kapasiteye sahip olmayan küçük ve orta ölçekli organizasyonlar için altı stratejik adımdan oluşan sadeleştirilmiş bir yalın dayanıklılık çerçevesi önerilmiştir. Önerilen bu çerçeve kurumsal düzeyde kritik varlıkların belirlenmesi güvenli mimari ve segmentasyon, yedeklilik, sürekli izleme, yama yönetimi ve acil durum planlaması gibi adımlarla kurumların asgari düzeyde dayanıklı bir dijital yapı inşa etmesine olanak sağlamaktadır. Çalışma hem teorik hem de uygulamalı katkılarıyla siber dayanıklılığın farklı kurumsal düzeylerde nasıl geliştirilebileceğine dair kapsamlı bir bakış sunmaktadır.

Abstract

In today's rapidly digitalizing world, organizations must develop not only preventive measures against cyber threats but also comprehensive strategies to enhance their resilience in a sustainable manner. This study centers on the concept of cyber resilience, examining the

*Corresponding author, e-mail: bora.aslan@klu.edu.tr

structural and managerial attributes that enable modern information systems not only to be protected against attacks but also to maintain functionality during incidents and recover swiftly afterwards. Within the scope of the study, internationally recognized frameworks and standards such as NIST, ENISA, ISO/IEC 27001, COBIT, and ITIL are first analyzed. Subsequently, ten core system characteristics derived from these frameworks are identified and discussed. Additionally, for small and medium-sized organizations that may lack the capacity to fully implement these frameworks, a simplified Basic Resilience Framework consisting of six strategic steps is proposed. This model includes steps such as the identification of critical assets, secure architecture and segmentation, redundancy, monitoring, patch management, and emergency response planning enabling organizations to establish a minimum level of cyber resilience. The study offers a comprehensive perspective on how cyber resilience can be developed across various organizational levels, providing both theoretical insights and practical applications.

1. GİRİŞ / INTRODUCTION

Bilişim teknolojilerinin hayatın tüm alanlarında etkin bir şekilde kullanılmasıyla siber güvenlik ve dayanıklılık kavramları günümüzde giderek daha fazla önem kazanmaktadır. Eğitimden sağlığa, ulaşımdan finansal hizmetlere kadar hemen her sektör, dijital altyapılar üzerinden faaliyet göstermektedir. Kamu kurumları, özel işletmeler ve son kullanıcı olarak bireyler bilgi sistemlerine bağımlı hale gelmişlerdir. Bu dijitalleşme süreci bir yandan iş süreçlerinin hızlanmasını, karar verme mekanizmalarının iyileştirilmesini ve veriye dayalı yönetim anlayışının güçlenmesini sağlarken diğer yandan siber tehditlerin etkilerinin daha yaygın ve yıkıcı olmasına neden olmaktadır (Möller, 2023). Özellikle enerji, sağlık, bankacılık, ulaşım, telekomünikasyon ve su yönetimi gibi kritik altyapılar, ulusal güvenlik ve toplumsal düzen açısından hayati önem taşımakta ve bu sistemlerin herhangi bir siber saldırı karşısında çalışamaz hale gelmesi, sadece ekonomik kayıplara değil, aynı zamanda kamu güvenliğini tehdit eden sonuçlara da yol açabilmektedir. Bu nedenle, bilişim teknolojilerine bağımlılığın artmasıyla birlikte, bu sistemlerin yalnızca korunması değil, aynı zamanda saldırı durumunda işlevselliğini sürdürebilmesi ve hızlıca toparlanabilmesi de stratejik bir gereklilik haline gelmiştir. Siber güvenlik politikalarının yanı sıra, teknolojik sistemlerin dayanıklı bir yapıya kavuşturulması hem kamu hem de özel sektör için öncelikli gündem maddesi halindedir.

Günümüz dünyasında finans sistemleri kurumsal veya ulusal bilgi sistemleri gibi kritik altyapılar siber saldırılara açık hale gelmiş olup bu tür saldırıların sadece teknik güvenlik açıklarından değil aynı zamanda kurumsal hazırlık eksikliklerinden ve zayıf organizasyonel yapıdan da kaynaklandığı görülmektedir (Lehto, 2022). Siber saldırılar artık sadece sistemlerin çalışamaz hale gelmesiyle sınırlı kalmamakta; veri sızıntısı, hizmet kesintisi, itibar kaybı ve hatta ekonomik krizlere yol açabilecek boyutlara ulaşmaktadır. Özellikle kamu hizmetleri, dijital ödeme altyapıları ve sağlık sistemleri gibi yüksek bağımlılıkla çalışan yapılar, bir saldırı anında geniş kitleleri etkileyebilecek potansiyele sahiptir. Bu nedenle, siber güvenlikte yalnızca tehditleri önlemeye odaklanan klasik yaklaşımlar yetersiz kalmakta, bu sistemlerin saldırı öncesinde hazırlıklı olması, saldırı anında işlevselliğini sürdürebilmesi ve sonrasında hızla toparlanarak normale dönebilmesi önem kazanmaktadır. Dayanıklılık kavramı bu noktada devreye girerek, güvenlik politikalarının ötesinde, süreçlerin sürekliliğini sağlayacak stratejileri ve organizasyonel esnekliği içeren çok katmanlı, bütünsel bir bakış açısı sunar. Bu bağlamda siber güvenlikte dayanıklılık teknik altyapıların dayanıklılığı kadar, insan faktörü, kriz yönetimi kapasitesi ve kurum kültürü gibi unsurların da dahil olduğu bütünleşmiş bir güvenlik anlayışını zorunlu kılmaktadır.

Dayanıklılık sistemlerin, kuruluşların veya toplumların beklenmedik olaylar karşısında temel işlevlerini koruyarak hızla toparlanabilme yeteneğidir. Siber güvenlik bağlamında dayanıklılık, bir organizasyonun veya sistemin siber saldırılara rağmen temel işlevlerini sürdürebilme ve hızlı şekilde toparlanabilme yeteneğini ifade eder (Araujo vd., 2024). IBM siber dayanıklılığı bir kuruluşun siber olayları önleme, bunlara dayanma ve sonrasında iyileşme becerisi olarak tanımlamaktadır (IBM, 2020). Benzer şekilde NIST (ABD Ulusal Standartlar ve Teknoloji Enstitüsü) siber dayanıklılığı, sistemlerin olumsuz koşulları, saldırıları veya ihlalleri sezme, bunlara karşı koyma, bunlardan kurtulma ve yeni durumlara uyum sağlama kabiliyetini geliştirmek olarak ele almaktadır (Ross vd., 2021). Dayanıklılık kavramı, klasik siber güvenlik önlemlerini iş sürekliliği ve felaket sonrası toparlanma perspektifiyle birleştirir.

Bu nedenle dayanıklılık, yalnızca bir saldırıyı engellemeye değil, aynı zamanda saldırı gerçekleştiğinde hizmetlerin kesintiye uğramamasına veya en az kesintiyle devam etmesine odaklanır.

Siber saldırılar son yıllarda artan dijitalleşme ile hem ölçek hem de etki açısından daha karmaşık ve yıkıcı bir boyuta ulaşmıştır. Ülkeler, kurumlar ve kuruluşlar iş sürekliliğini sağlamak, finansal kayıpları ve itibar zararını azaltmak için dayanıklılığı stratejik bir hedef haline getirmektedirler. 2024 yılı, küresel ve ulusal düzeyde siber saldırıların hem sayısal artış gösterdiği hem de ekonomik etkilerinin ciddi boyutlara ulaştığı bir dönem olmuştur. IBM'in yayımladığı "Cost of a Data Breach 2024" raporuna göre, dünya genelinde bir veri ihlalinin ortalama maliyeti 4,88 milyon dolar seviyesine ulaşmıştır. Bu artış, yapay zeka gibi teknolojilerin siber saldırganlar tarafından daha etkin kullanılmasıyla ilişkilendirilmiştir (IBM, 2024). Küresel ölçekte, siber saldırıların toplam ekonomik maliyetinin 2024 yılında 9 trilyon doları aştığı tahmin edilmektedir. Bu rakamın 2025 yılında 10,5 trilyon dolara ulaşması beklenmektedir. Sadece Almanya'da siber saldırıların yol açtığı ekonomik zarar 266 milyar euro olarak rapor edilmiştir. Bazı örnek siber olaylar aşağıda verilmiştir:

- 10 Mart 2025 tarihinde sosyal medya platformu X (eski adıyla Twitter), Dark Storm Team adlı bir grup tarafından gerçekleştirilen koordineli DDoS (servis dışı bırakma) saldırısına maruz kalmıştır. Söz konusu saldırı neticesinde platform, 24 saat içinde üç kez hizmet dışı kalmıştır. Platformun sahibi Elon Musk, saldırının büyük olasılıkla bir devlet destekli yapı tarafından gerçekleştirildiğini ifade etmiştir. Bu saldırı, sosyal medya altyapılarının ne denli kırılgan olduğunu ve kamusal bilgi akışının kesintiye uğratılmasının potansiyel sosyopolitik etkilerini bir kez daha ortaya koymuştur (Hay Newman, 2025).
- Aralık 2024'te, Türkiye'de PTT'nin Hızlı Geçiş Sistemi ve Anadolu Sigorta'nın "Sigortam Cepte" adlı mobil uygulamaları, siber saldırganlar tarafından hedef alınmıştır. Saldırganlar, bu uygulamaların bildirim servislerine yetkisiz erişim sağlayarak kullanıcılara küfürlü mesajlar göndermiş ve belirli bir Bitcoin adresine ödeme yapılmaması halinde kullanıcı verilerinin ifşa edileceği tehdidinde bulunmuşlardır. Saldırının, OneSignal adlı bildirim altyapısının API anahtarlarının ele geçirilmesiyle mümkün olduğu belirlenmiştir (Dünya Gazetesi, 2024).
- 2024 yılının son çeyreğinde, ABD'de faaliyet gösteren SRP Federal Credit Union, yaklaşık 240.000 üyesinin kişisel ve finansal verilerinin sızdırıldığı ciddi bir veri ihlali yaşamıştır. Saldırganlar, 5 Eylül ile 4 Kasım 2024 tarihleri arasında kurumun sistemlerine yetkisiz erişim sağlayarak ad, doğum tarihi, sosyal güvenlik numarası, ehliyet bilgileri ve banka hesap numaraları gibi hassas verileri ele geçirmiştir. Saldırının sorumluluğunu, 650 GB'lık veri çaldığını iddia eden Nitrogen adlı bir fidye yazılımı grubu üstlenmiştir. SRP, etkilenen bireylere kimlik hırsızlığına karşı koruma hizmeti sunarken, olayın ardından toplu dava süreçleri de başlatılmıştır (Daniel, 2024).
- Hindistan merkezli internet servis sağlayıcısı Hathway, Ocak 2024'te yaklaşık 4 milyon kullanıcının etkilendiği bir veri ihlali yaşamıştır. Saldırganlar, şirketin içerik yönetim sistemindeki bir güvenlik açığını istismar ederek kullanıcıların KYC (Müşterini Tanı) bilgilerine erişim sağlamışlardır. Sızdırılan veriler arasında adlar, adresler, telefon numaraları ve e-posta adresleri yer almaktadır (Waqas, 2024).
- 2024 yılının Kasım ayında Amazon çalışanlarına ait iletişim bilgilerinin bir siber suç forumunda yayımlandığını doğrulamıştır. Bu veri sızıntısı şirkette kullanılan MOVEit dosya transfer yazılımındaki bir güvenlik açığından kaynaklanmıştır (Dobberstein, 2024).
- Starbucks 2024 yılının Kasım ayında, tedarik zinciri yönetimi yazılımı sağlayıcısı Blue Yonder'a yönelik bir fidye yazılımı saldırısının dolaylı etkileriyle karşı karşıya kalmıştır. Bu saldırı, Starbucks'ın çalışanlarının vardiya planlaması ve çalışma saatlerinin takibi gibi arka uç operasyonlarını sekteye uğratmış, şirketin manuel yöntemlere başvurmasına neden olmuştur (Baran, 2024).

Siber saldırıların tamamen engellenemeyebileceği dijital çağın kaçınılmaz bir gerçeğidir. Gelişen tehdit ortamında saldırganlar giderek daha farklı yöntemler kullanmakta sıfır gün açıkları, sosyal mühendislik teknikleri ve yapay zeka destekli otomasyonlarla güvenlik sistemlerini aşabilmektedir (Ali vd., 2023). Bu nedenle, yalnızca saldırıları önlemeye odaklanmak yeterli değildir. Bunun yerine, saldırının

gerçekleşmesi durumunda sistemlerin işlevselliğini sürdürebilmesi, zararın sınırlanması ve en kısa sürede toparlanma sağlanması temel hedef olmalıdır. İşte bu noktada iyi yapılandırılmış bir siber dayanıklılık stratejisi devreye girerek, olası kesintilerin operasyonel, finansal ve itibari etkilerini asgariye indirir. Bu strateji önleyici güvenlik önlemlerini kriz yönetimi, iş sürekliliği planlaması ve olay sonrası iyileşme süreçleriyle bütünleştirerek bütüncül bir yaklaşım sunar. Dolayısıyla, siber dayanıklılık yalnızca bir güvenlik önlemi değil aynı zamanda modern işletmeler için sürdürülebilirlik, rekabet avantajı ve müşteri güvenini pekiştirme açısından da stratejik bir gerekliliktir (AL-Hawamleh, 2024). Kurumlar bu farkındalıkla dayanıklılık kapasitelerini artırmalı ve siber tehditlere karşı daha dayanıklı bir dijital altyapı inşa etmelidir.

Bu çalışma siber güvenlikte dayanıklılık kavramını merkeze alarak modern organizasyonların yalnızca saldırılara karşı korunmasını değil, aynı zamanda bu saldırılar karşısında işlevselliğini sürdürebilmesini ve sonrasında hızlı bir şekilde toparlanabilmesini sağlayacak bütüncül yapıları incelemektedir. Çalışmanın 2.bölümünde NIST, ENISA, ISO/IEC 27001 gibi uluslararası geçerliliğe sahip dayanıklılık çerçeveleri ele alınmıştır. Bu çerçevelerden türetilen on temel sistem özelliği detaylandırılmış ve 3.bölümde sunulmuştur. Ayrıca kurumsal kapasitesi sınırlı olan küçük ve orta ölçekli kuruluşlar için altı stratejik adımdan oluşan yalın bir yalın dayanıklılık çerçevesi 4. bölümde önerilmiştir. Böylece hem yüksek düzey standartlara dayalı hem de uygulanabilir düzeyde çözümler sunularak, kurumsal düzeyde siber dayanıklılığın nasıl inşa edilebileceğine dair yapısal ve yönetsel bir yol haritası ortaya konmuştur.

2. SİBER DAYANIKLILIK ÇERÇEVELERİ VE STANDARTLARI / CYBER RESILIENCE FRAMEWORKS AND STANDARDS

Siber dayanıklılık, kritik altyapı sistemlerinin siber tehditlere karşı korunma, hazırlık, müdahale ve iyileşme yetenekleri sayesinde saldırı anında kesintisiz çalışmayı sürdürebilme, zararları en aza indirme ve hızlı şekilde toparlanabilme kapasitesidir(Lubis vd., 2025). Siber dayanıklılık kavramı yalnızca bilgi güvenliğini sağlamaya yönelik önlemlerle sınırlı kalmamakta aynı zamanda organizasyonların saldırılar öncesinde hazırlıklı olmasını, saldırılar sırasında işlevselliğini sürdürebilmesini ve saldırı sonrasında hızlı ve etkili biçimde toparlanabilmesini sağlayan bütüncül bir yaklaşımı temsil etmektedir. Bu yaklaşımın sistematik biçimde hayata geçirilebilmesi ise belirli çerçeve modellerin ve uluslararası standartların rehberliğinde mümkün olmaktadır. Çerçeve organizasyonların mevcut durumu değerlendirmesi, zaafiyetleri tespit etmesi ve öncelikli iyileştirme adımlarını planlaması için yapılandırılmış yol haritasıdır.
Başta NIST Siber Güvenlik Çerçevesi, ISO/IEC 27001 ve ENISA Dayanıklılık Kılavuzları olmak üzere birçok kurumsal ve teknik belge siber dayanıklılık süreçlerini planlama, uygulama, izleme ve sürekli iyileştirme döngüsüne oturtan yapılandırılmış yaklaşımlar sunmaktadır. Bu bölümde mevcut siber dayanıklılık çerçeveleri ve ilgili standartlar ele alınmaktadır. Bu yapıların temel prensipleri, bileşenleri ve uygulama alanları verilerek kurumların hangi çerçeveleri neden ve nasıl benimseyebileceği açıklığa kavuşturulmakta ve siber dayanıklılığın kurumsal bir yetkinliğe dönüştürülmesine yönelik yöntemsel bir zemin sunulmaktadır.

2.1 NIST Siber Güvenlik Çerçevesi / NIST Cyber Security Framework

NIST Siber Güvenlik Çerçevesi NIST tarafından ilk olarak 2014 yılında geliştirilmiş olup, özellikle kritik altyapıların siber tehditlere karşı korunmasını desteklemek amacıyla oluşturulmuştur (NIST, 2024). 2024 yılında yayımlanan CSF (Siber Güvenlik Çerçevesi) 2.0 versiyonu ile çerçeve özel sektör, kamu kurumları ve farklı büyüklükteki kuruluşlar için daha kapsamlı ve ölçeklenebilir hale getirilmiştir. Çerçeve kuruluşların siber güvenlik risklerini tanımlamasını, yönetmesini ve azaltmasını sağlayan sistematik bir yapı sunmaktadır ve bu yönüyle siber dayanıklılık stratejilerinin temelini oluşturmaktadır. Kurulan yapı Tablo 1'de verildiği gibi yönetişim, tanımlama, koruma, tespit, yanıt ve toparlanma olmak üzere altı temel fonksiyona ve alt kategorilere dayalıdır. Bu fonksiyonlar bir kuruluşun tehditlere karşı hazırlıklı olmasını, saldırı anında müdahale kapasitesini sürdürmesini ve olay sonrasında hizmet sürekliliğini sağlayacak şekilde toparlanabilmesini mümkün kılmaktadır. Her fonksiyon, daha ayrıntılı kategoriler ve alt kontroller aracılığıyla kuruluşların güvenlik süreçlerini değerlendirmesine ve geliştirmesine yardımcı olmaktadır.

Tablo 1. *NIST Temel Fonksiyon ve Alt Kategorileri*

Fonksiyon	Kategori
Yönetişim (GV)	Kurumsal Bağlam
	Risk Yönetim Stratejisi
	Roller, Sorumluluklar ve Yetkiler
	Politika
	Gözetim
	Siber Güvenlik Tedarik Zinciri Risk Yönetimi
Tanımlama (ID)	Varlık Yönetimi
	Risk Değerlendirme
	İyileştirme
Koruma (PR)	Kimlik Yönetimi, Kimlik Doğrulama ve Erişim Kontrolü
	Farkındalık ve Eğitim
	Veri Güvenliği
	Platform Güvenliği
	Teknoloji Altyapısı Direnci
Tespit (DE)	Sürekli İzleme
	Olumsuz Olay Analizi
Yanıt (RS)	Olay Yönetimi
	Olay Analizi
	Olay Yanıtı Raporlama ve İletişim
	Olay Azaltımı
Toparlanma (RC)	Olay Sonrası Toparlanma Planının Uygulanması
	Toparlanma Süreci İletişimi

Çerçeve teknolojik önlemlerin yanı sıra yönetişim, politika oluşturma, çalışan farkındalığı ve tedarik zinciri güvenliği gibi operasyonel ve kurumsal boyutları da kapsamaktadır. Bu çok katmanlı yaklaşım, siber güvenliğin sadece bilişim teknolojileri departmanlarıyla sınırlı kalmamasını, organizasyonun tüm birimlerinin güvenlik sorumluluğuna dahil edilmesini sağlamaktadır. Çerçeve ISO/IEC 27001 gibi diğer uluslararası standartlarla uyumlu olacak biçimde tasarlandığı için entegre yönetim sistemlerine kolayca adapte edilebilmektedir. Uygulama açısından esnek bir yapıya sahip olan çerçeve, organizasyonların kendi risk düzeylerine, sektörel bağlamlarına ve olgunluk seviyelerine göre özelleştirilebilmektedir. Ayrıca, sürekli iyileştirme ve geri bildirim mekanizmaları sayesinde, tehdit ortamındaki değişimlere karşı adaptif bir güvenlik kültürünün gelişmesine katkı sunmaktadır. Bu bağlamda, NIST Siber Güvenlik Çerçevesi hem stratejik yönetim düzeyinde hem de operasyonel uygulamalarda proaktif, ölçülebilir ve dayanıklı bir siber güvenlik yaklaşımı sağlamaktadır.

NIST Siber Güvenlik Çerçevesinin kurumsal düzeyde uygulanabilmesi için öncelikle organizasyonun mevcut güvenlik durumunun değerlendirilmesi ve buna uygun bir profil oluşturulması gerekmektedir. Bu kapsamda kurum, hem mevcut durumunu yansıtan bir "mevcut profil" hem de ulaşmak istediği hedef durumu temsil eden bir "hedef profil" tanımlamalıdır. Bu iki profil arasındaki farklar, kurumsal güvenlik açıklarının ve iyileştirme alanlarının sistematik şekilde tespit edilmesini sağlamaktadır. Böylelikle, çerçevenin uygulanması yalnızca teknik düzeyde değil, aynı zamanda stratejik karar alma süreçleriyle entegre bir biçimde başlatılabilmektedir. İkinci aşamada, organizasyonun karşı karşıya olduğu siber riskler belirlenmeli ve önceliklendirilmelidir. Kurumun iş süreçleri, varlık envanteri, dış tehdit ortamı ve içsel zafiyetleri analiz edilerek, risk temelli bir yaklaşım çerçevesinde tehdit senaryoları oluşturulmaktadır. Bu analiz, hangi güvenlik kontrollerinin ne ölçüde etkili olduğu ve hangi alanlarda daha fazla yatırım yapılması gerektiği konularında karar vericilere yön göstermektedir. Bu doğrultuda, çerçevenin risk odaklı yapısı, kaynakların etkili kullanılmasını ve yüksek öncelikli güvenlik açıklarına odaklanılmasını mümkün kılmaktadır. Üçüncü olarak, çerçevenin beş temel fonksiyonu esas alınarak kurumsal bir açıklık analizi yapılmalıdır. Bu analiz sayesinde, mevcut sistemlerin ve politikaların çerçevenin öngördüğü yapılarla ne ölçüde örtüştüğü değerlendirilmektedir. Örneğin, tanımla fonksiyonu kapsamında varlık yönetimi ve risk değerlendirme mekanizmaları incelenmekte; koru fonksiyonu kapsamında erişim kontrolleri, veri güvenliği ve kullanıcı eğitimi gibi kontroller analiz edilmektedir. Bu süreç, çerçevenin uygulanmasında hangi alanların öncelikli olduğunu belirlemek açısından önemli bir referans sunmaktadır. Açıklık analizinin ardından kısa, orta ve uzun vadeli hedefleri içeren kapsamlı bir

uygulama planı oluşturulmalıdır. Bu yol haritası teknolojik altyapı yatırımlarını, güncellenmesi gereken politika ve prosedürleri, organizasyonel yapıdaki iyileştirmeleri ve çalışanlara yönelik eğitim programlarını kapsamalıdır. Çerçevenin modüler yapısı sayesinde bu uygulama planı kurumun ölçeğine, sektörel ihtiyaçlarına ve kaynak kapasitesine göre esnek biçimde uyarlanabilmektedir. Böylelikle uygulama süreci, kurumsal gerçekliklerle uyumlu, adım adım ilerleyen ve ölçülebilir hedeflere dayalı bir şekilde kurgulanmaktadır. Son olarak, çerçevenin etkinliğinin sürdürülebilirliğini sağlamak amacıyla sürekli izleme ve gözden geçirme süreçleri hayata geçirilmelidir. Bu kapsamda, güvenlik kontrollerinin performansı ölçülmekte, yeni ortaya çıkan tehditler doğrultusunda profiller güncellenmekte ve elde edilen bulgular ışığında iyileştirici aksiyonlar alınmaktadır. Ayrıca iç denetimlerin ve dış değerlendirme mekanizmalarının uygulanması, güvenlik olgunluğunun periyodik olarak ölçülmesini ve kurumsal dayanıklılığın zamanla gelişmesini desteklemektedir.

Bu aşamalar bütüncül olarak ele alındığında NIST Siber Güvenlik Çerçevesi yalnızca teknik güvenlik uygulamalarını değil aynı zamanda organizasyonel yönetişim yapısını da güçlendiren, kuruma özel bir siber dayanıklılık çerçevesi sunmaktadır. Kurumlar bu yapı sayesinde, değişen tehdit ortamına karşı hazırlıklı olabilmekte, saldırılara etkili biçimde yanıt verebilmekte ve operasyonel sürekliliklerini güvence altına alabilmektedir.

2.2 ENISA Siber Dayanıklılık Kılavuzu / ENISA Cyber Resilience Guide

ENISA (Avrupa Birliği Siber Güvenlik Ajansı) Avrupa genelinde dijital altyapıların ve hizmetlerin güvenliğini artırmak amacıyla kapsamlı stratejik ve teknik rehberler yayımlamakta ve üye ülkelerin siber dayanıklılık kapasitelerini geliştirmelerini desteklemektedir. ENISA'nın siber dayanıklılık yaklaşımı, yalnızca bilgi teknolojileri düzeyinde değil, aynı zamanda kurumsal yönetişim, kriz yönetimi ve sektörler arası iş birliği gibi çok boyutlu bir yapıyı kapsamaktadır (ENISA, 2024). Kurum, Avrupa Birliği çapında ortak siber güvenlik standartlarının ve iyi uygulama örneklerinin oluşturulmasına öncülük etmekte; böylece sınır ötesi dijital hizmetlerin güvenliğini kolektif bir dayanıklılık perspektifiyle ele almaktadır.

Avrupa Komisyonu 15 Eylül 2022 tarihinde CRA'yı (Siber Dayanıklılık Yasası) yayınlamıştır. Bu kapsamda ENISA tarafından yayımlanan rehberlerde, özellikle kritik altyapı sektörleri öncelikli olarak ele alınmakta ve bu sektörlerde faaliyet gösteren aktörlerin olası siber tehditlere karşı hazırlıklı olmalarını sağlamak için çeşitli kontrol mekanizmaları önerilmektedir. Yayınlanan rehberler hem stratejik düzeyde hem de operasyonel düzeyde uygulanabilir bir yapı sunmaktadır. Ayrıca ENISA tehdit istihbaratı paylaşımı, kamu-özel sektör iş birliği modelleri ve güvenlik kültürünün kurumsallaştırılması gibi alanlarda da referans çerçeveler geliştirmektedir. Buna ek olarak ENISA çerçevesi ürün geliştirme, teslimat, bakım, güncelleme ve ürünün ömrünün sonlandırılması gibi tüm yaşam döngüsü evrelerinde güvenliğin nasıl sağlanacağını açıklamakta ve ürün bazlı risk analizi, gömülü güvenlik önlemleri, veri gizliliği ve bütünlüğü, erişim kontrolleri, olay kayıt mekanizmaları, otomatik güncelleme sistemleri ve zafiyet yönetimi gibi kapsamlı kriterler ortaya koymaktadır. ENISA'nın katkısı sadece standart eşlemesiyle sınırlı kalmamakta aynı zamanda geliştirme öncesi güvenlik gerekliliklerinin tanımlanması, güvenli tasarım ilkeleri, kullanım sonrası güncelleme ve raporlama süreçleri gibi kritik unsurları da içermektedir.

ENISA 2025 sonrası için Avrupa genelinde yüksek düzeyde ortak bir siber güvenlik seviyesi sağlama hedefi doğrultusunda yeni stratejisini yayımlamıştır. Bu strateji Avrupa'nın dijital altyapılarını hem günümüz hem de gelecekteki siber tehditlere karşı dayanıklı hale getirmeyi amaçlayan Tablo 2'de verilen yedi ana hedef etrafında şekillendirilmektedir. Bu strateji özellikle AB üyesi ülkelerdeki hem kamu kurumları hem özel sektör hem de bireysel kullanıcılar için daha dirençli bir dijital Avrupa oluşturmayı hedeflemektedir.

Tablo 2. *ENISA Hedefleri*

No	Hedef	Açıklama
1	Güçlendirilmiş Topluluklar ve Katılımcı Bir Siber Ekosistem	ENISA, kamu ve özel sektör temsilcilerinden oluşan çok paydaşlı yapılar aracılığıyla dayanıklı ve bilinçli siber güvenlik toplulukları oluşturmayı hedeflemektedir.

2	Gelecek Odaklı ve Erken Uyarı Temelli Yaklaşım	Gelişen ve gelecekteki siber güvenlik tehditlerine karşı öngörü geliştirme ve proaktif stratejiler oluşturma.
3	Avrupa Genelinde Paylaşılan Siber Güvenlik Bilgisi	Bilgi ve tehdit istihbaratının sınırlar ötesi paylaşımını teşvik ederek, AB içinde ortak bir güvenlik anlayışı geliştirmek.
4	AB Siber Güvenlik Politikalarının Tutarlı Biçimde Uygulanmasına Destek	ENISA, NIS2, CRA ve diğer düzenleyici yapıların hayata geçirilmesinde üye ülkelere rehberlik sunmayı sürdürecektir.
5	Siber Olaylar ve Krizlere Karşı AB Düzeyinde Güçlü Hazırlık	ENISA, ortak tatbikatlar ve müdahale rezervleri gibi girişimlerle kriz yönetim kapasitesini artıracaktır.
6	AB'de Siber Güvenlik Kapasitesinin Geliştirilmesi	Kurumsal, teknik ve insan kaynağı boyutlarında kapasite geliştirme faaliyetleri ile tüm paydaşların olgunluk düzeyi artırılacaktır.
7	Güvenli Dijital Çözümlere Olan İnancın Artırılması	Avrupa dijital pazarının güvenliğini artıracak teknik standartlar, sertifikasyon süreçleri ve kullanıcı güveni odaklı uygulamalar yaygınlaştırılacaktır.

ENISA'nın CRA tabanlı yaklaşımının kurumsal düzeyde uygulanabilmesi çok aşamalı ve bütüncül bir güvenlik yönetim sürecini gerektirmektedir. İlk olarak kurumun CRA kapsamına giren ürünlerini tanımlaması gerekmektedir. Bu kapsamda, ürünlerin dijital unsur içerip içermediği, ağ bağlantılı olup olmadığı ve hedef pazarlarda nasıl konumlandığı gibi faktörler dikkate alınarak kapsam belirleme süreci yürütülmelidir. Ürünlerin fonksiyonel sınırlarının ve kullanım senaryolarının belirlenmesi, sonraki adımların sağlıklı bir şekilde planlanmasını sağlamaktadır. Bu aşamada ürünler sadece kurumun ürettiği cihazları değil aynı zamanda verileri veya hizmetleri de kapsamaktadır. İkinci aşamada ürünün tüm yaşam döngüsünü kapsayan risk temelli bir güvenlik analizi gerçekleştirilmelidir. ENISA'nın yaklaşımına göre güvenlik yalnızca ürünün piyasaya sunulmasıyla sınırlı kalmamakta; tasarım, üretim, dağıtım, bakım ve kullanım sonrası dönemleri de kapsamaktadır. Bu çerçevede güvenlik gereksinimleri erken aşamalarda tanımlanmakta ve "güvenli tasarım" ile "varsayılan güvenli yapılandırma" ilkeleri doğrultusunda sistematik olarak entegre edilmektedir. Bu yaklaşım, güvenliğin ürün tasarımının temel bir bileşeni haline gelmesini sağlamaktadır. Üçüncü adımda ürün güvenliğiyle ilgili belirlenen gereksinimler, ENISA'nın önerdiği uluslararası standartlarla eşleştirilmelidir. ISO/IEC 27001, 27002, 27701, IEC 62443 ve ETSI EN 303 645 gibi standartlar doğrultusunda, kimlik doğrulama, erişim kontrolleri, yama ve güncelleme yönetimi, zafiyet tarama politikaları, veri gizliliği ve olay kayıt sistemleri gibi güvenlik alanlarında ayrıntılı teknik ve yönetsel önlemler belirlenmelidir. Bu standart eşlemesi hem regülasyonlara uyumu kolaylaştırmakta hem de güvenliğin evrensel kabul görmüş çerçevelere dayanmasını sağlamaktadır. Dördüncü aşamada her bir güvenlik gereksinimi için uygun teknik ve organizasyonel kontroller geliştirilerek detaylı bir dokümantasyon yapılmalıdır. Bu kapsamda güvenli yazılım geliştirme döngüsü belgeleri, zafiyet yönetim prosedürleri, yazılım bileşenlerinin tam listesini içeren belgeleri ve kullanıcıya yönelik bilgilendirme ile güncelleme mekanizmalarına ilişkin planlamalar oluşturulmalıdır. Bu belgeler ürünün tüm yaşam döngüsünde izlenebilirlik ve hesap verebilirlik sağlayarak denetim süreçlerine zemin oluşturmaktadır. Beşinci adım ürünün pazara sunulmasından sonraki dönemleri kapsamaktadır. Bu noktada güvenliğin sürekliliğini sağlamak adına otomatik veya manuel güncelleme sistemleri kurulmalı zafiyetlerin bildirimi için şeffaf ve erişilebilir iletişim kanalları oluşturulmalıdır. Ayrıca düzenli olarak penetrasyon testleri ve güvenlik denetimleri yapılmalı ve kullanıcılar için anlaşılır güncelleme notları yayımlanmalıdır. Bu uygulamalar kullanıcı güvenini artırmakta ve regülasyonlara uyumu sürdürülebilir kılmaktadır. Son olarak ürünün CRA kapsamındaki uyum düzeyini göstermek üzere uygun bir değerlendirme ve sertifikasyon sürecine tabi tutulması gerekmektedir. ENISA dokümanı ürünün risk profiline göre üreticinin kendi kendine değerlendirmesi, standartlara uygunluk beyanı veya üçüncü taraf denetimi ve sertifikasyonu şeklinde üç farklı uyum yöntemi önermektedir. Özellikle yüksek riskli ürünler için bağımsız denetim ve akredite kurumlarca verilen sertifikasyonlar önerilmektedir. Bu süreç yalnızca yasal bir gerekliliği karşılamakla kalmayıp aynı zamanda ürünün güvenilirliğini belgeleyen kurumsal bir itibara da katkı sağlamaktadır.

ENISA'nın siber dayanıklılık rehberleri, Avrupa Komisyonu'nun NIS2 gibi dijital dayanıklılık politikaları ile uyumlu olacak şekilde güncellenmekte ve ülkelerin mevzuat yapılarıyla bütünleşmiş biçimde uygulanabilirlik göstermektedir. Rehberlerde önerilen iyi uygulamalar, teknik kontrollerin ötesinde kurum içi organizasyonel kapasitenin geliştirilmesini, eğitim programlarının yaygınlaştırılmasını ve sektörel koordinasyonun artırılmasını da kapsamaktadır. Bu yönüyle ENISA,

yalnızca rehber yayımlayan bir kurum olmanın ötesinde, Avrupa çapında siber dayanıklılık ekosisteminin şekillendirilmesinde aktif bir koordinasyon rolü üstlenmektedir.

2.3 ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi / ISO/IEC 27001 Information Security Management System

ISO/IEC 27001 standardı, bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini sistematik ve sürdürülebilir bir biçimde korumayı amaçlayan uluslararası geçerliliğe sahip bir Bilgi Güvenliği Yönetim Sistemi çerçevesi sunmaktadır. ISO (Uluslararası Standardizasyon Örgütü) ve IEC (Uluslararası Elektroteknik Komisyonu) tarafından geliştirilen bu standart, organizasyonların bilgi güvenliğini bir yönetim sistemi yaklaşımıyla ele almasını sağlamaktadır. Bu sistem, yalnızca teknik kontrollerin uygulanmasını değil, aynı zamanda politika geliştirme, risk değerlendirme, sürekli iyileştirme ve insan faktörünün yönetimini de kapsamaktadır. ISO/IEC 27001 standardı, organizasyonların işleyişine entegre edilebilecek esnek bir yapı sunmakta ve bilgi güvenliği risklerinin değerlendirilmesi, önceliklendirilmesi ve kontrol altına alınmasını sağlayan bir çerçeve oluşturmaktadır. Bu kapsamda, risk değerlendirme süreçleri, güvenlik kontrollerinin seçimi ve uygulanması, farkındalık eğitimleri, iç denetimler ve yönetim gözden geçirme mekanizmaları standardın temel yapı taşlarını oluşturmaktadır. ISO/IEC 27001 ayrıca, kuruluşların yasal ve sözleşmesel yükümlülüklerini karşılamalarına yardımcı olmakta; dış denetim ve sertifikasyon süreçleriyle birlikte güvenlik uygulamalarının bağımsız olarak doğrulanabilmesini mümkün kılmaktadır.

Siber dayanıklılık açısından değerlendirildiğinde, ISO/IEC 27001 organizasyonların yalnızca saldırıları önlemeye değil, aynı zamanda olaylara hazırlıklı olmaya, etkili şekilde müdahale edebilmeye ve olay sonrası toparlanma süreçlerini yapılandırmaya da katkı sunmaktadır. Standardın içerdiği sürekli PUKÖ (Planla–Uygula–Kontrol Et–Önlem Al) döngüsü, güvenlik uygulamalarının tehdit ortamındaki değişimlere karşı uyarlanabilir olmasını teşvik etmektedir. Bu sayede ISO/IEC 27001, teknik, yönetsel ve insan kaynaklı boyutları kapsayan bütünsel bir bilgi güvenliği yaklaşımı sağlayarak kurumların siber dayanıklılık kapasitesini kurumsallaştırmalarına olanak tanımaktadır.

ISO/IEC 27001'in içeriğinde yer alan kontrol maddeleri, hem erişim denetimleri, kriptografik kontroller, yedekleme ve loglama gibi teknik önlemler hem de güvenlik politikaları, bilinçlendirme eğitimleri, olay yönetimi süreçleri gibi organizasyonel ve insan faktörü temelli önlemler aracılığıyla kurumsal güvenlik kültürünü bütüncül biçimde oluşturmaktadır. Bu kontroller kurumun sadece güvenliğini artırmakla kalmamakta; aynı zamanda bir siber olay gerçekleştiğinde olay müdahale planlarının, raporlama prosedürlerinin ve iletişim mekanizmalarının önceden tanımlı ve test edilmiş olmasını garanti altına almaktadır. Ayrıca ISO/IEC 27001 iş sürekliliği planlaması, felaket kurtarma ve olağanüstü durum hazırlığı gibi dayanıklılık odaklı uygulamaları doğrudan destekleyen yapılar içermektedir. Bu sayede, bir saldırı veya kesinti durumunda kurumun kritik operasyonlarını asgari düzeyde etkilenecek şekilde sürdürmesi mümkün olmaktadır. Standardın öngördüğü periyodik iç denetim süreçleri, yönetim gözden geçirme toplantıları ve sürekli iyileştirme döngüsü (PDCA) aracılığıyla, organizasyonun güvenlik olgunluğu zamanla artmakta ve değişen tehdit ortamına karşı adaptasyon yeteneği güçlenmektedir. ISO/IEC 27001'in bir diğer önemli katkısı ise uyum ve şeffaflık ilkelerini güçlendirmesidir. Kurumlar bu standarda göre sertifikalandırıldıklarında, yalnızca iç güvenlik yapılarının sağlamlığını belgelemekle kalmamakta; aynı zamanda müşterilerine, iş ortaklarına ve düzenleyici kurumlara karşı güven telkin eden, sürdürülebilir ve hesap verebilir bir güvenlik yönetimi yürüttüklerini göstermektedirler. Bu yönüyle ISO/IEC 27001, kurumsal güvenin tesis edilmesinde, paydaşlar arası güvenlik taahhütlerinin yerine getirilmesinde ve organizasyonun güçlü bir siber dayanıklılık temeline sahip olduğunu kanıtlamasında stratejik bir rol üstlenmektedir.

2.4 COBIT Bilişim Teknolojileri Yönetişimi ve Siber Dayanıklılık Yaklaşımı / COBIT Information Technology Governance and Cyber Resilience Approach

COBIT (Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri), kurumsal düzeyde bilgi teknolojilerinin yönetişimi ve yönetimi için ISACA tarafından geliştirilen kapsamlı bir çerçeve olup, organizasyonların bilişim teknolojileri süreçlerini stratejik hedeflerle ilişkilendirerek güvenli, ölçülebilir ve hesap verebilir bir yapıya kavuşturmayı amaçlamaktadır (ISACA, 2019). COBIT yalnızca teknik altyapının kontrolünü değil aynı zamanda kurumsal yönetişim, performans yönetimi, risk kontrolü ve yasal uyum gibi stratejik

alanları da kapsamakta ve bu yönüyle siber dayanıklılık kapasitesinin bütüncül olarak yönetilmesini mümkün kılmaktadır. Özellikle COBIT 2019 versiyonu ile birlikte çerçeve dijital dönüşüm, siber güvenlik ve sürdürülebilir bilişim teknolojileri hizmetleri gibi alanlara daha esnek ve modüler çözümler sunmaktadır.

Tablo 3. *COBIT Süreç Alanları*

Kod	Adı	İçeriği
EDM	Değerlendir, Yönlendir ve İzle (Evaluate, Direct and Monitor)	Bilişim teknolojileri yönetişimi çerçevesinde kurumsal hedeflerle uyumu sağlamak, stratejik kararları yönlendirmek ve performansı üst düzeyde izlemeyi kapsamaktadır.
APO	Hizala, Planla ve Organize Et (Align, Plan and Organize)	Bilişim teknolojileri stratejilerinin planlanması, organizasyonel yapıların kurulması ve risk yönetimi dahil olmak üzere tüm yönetsel hazırlık süreçlerini kapsamaktadır.
BAI	İnşa Et, Edin ve Uygula (Build, Acquire and Implement)	Bilgi sistemlerinin geliştirilmesi, dış kaynakların edinilmesi ve yeni çözümlerin güvenli şekilde devreye alınmasını içermektedir.
DSS	Teslimat, Servis ve Destek (Deliver, Service and Support)	Bilişim teknolojileri hizmetlerinin sunumu, olay yönetimi, erişim kontrolleri ve kullanıcı destek hizmetlerinin güvenli ve kesintisiz şekilde yürütülmesini kapsamaktadır.
MEA	İzle, Değerlendir ve Ölç (Monitor, Evaluate and Assess)	Bilişim teknolojileri süreçlerinin performansını ve uygunluğunu izlemek, denetlemek ve sürekli iyileştirme için ölçülebilir çıktılar üretmek amacıyla uygulanmaktadır.

COBIT bilgi sistemlerinin değer üretimini desteklerken, aynı zamanda potansiyel risklerin ve dışsal tehditlerin kontrol altına alınmasını sağlayacak bir denetim ve yönetişim mekanizması kurmaktadır. Bu çerçevede tanımlanan ve Tablo 3'de verilen beş süreç alanı sayesinde bilişim teknolojisi süreçlerinin kurumsal hedeflerle nasıl ilişkilendirileceği ve yönetileceği açık bir biçimde ortaya konmaktadır. Bu alanlardan özellikle DSS ve MEA, siber olaylara hazırlık, müdahale, toparlanma ve sürekli iyileştirme mekanizmalarının işleyişine doğrudan katkı sağlamaktadır. Siber dayanıklılık bağlamında COBIT risk temelli yaklaşımı ve ölçülebilir performans göstergeleri ile kuruma özel güvenlik politikalarının geliştirilmesini, uygulanmasını ve sürekli gözden geçirilmesini teşvik etmektedir. Ayrıca organizasyonun yönetim, bilişim departmanı, iç denetim birimi, iş birimleri gibi farklı seviyelerinde görev ve sorumlulukların net şekilde tanımlanmasına olanak tanımaktadır. Bu da kriz anlarında daha koordineli ve hızlı müdahale edilebilir bir yapı sağlamaktadır. COBIT'in, ISO/IEC 27001, NIST CSF ve ITIL gibi diğer çerçevelerle uyumlu olarak çalışabilmesi, hibrit bir güvenlik ve dayanıklılık yönetimi oluşturmak isteyen kurumlar açısından da önemli bir avantaj sunmaktadır. Bu yönüyle COBIT sadece teknik kontrollerin uygulanmasına değil, kurumsal yönetişimin stratejik düzeyde güvenliğe entegre edilmesine katkı sunmakta ve siber dayanıklılığın karar alma süreçlerinin ayrılmaz bir parçası haline gelmesini sağlamaktadır. Kurumların sürdürülebilir güvenlik performansı ve uyum kapasitesi oluşturmasında COBIT, etkili bir yönetim mimarisi ve denetim altyapısı sunarak kritik bir rol üstlenmektedir.

2.5 ITIL Siber Dayanıklılık Yaklaşımı / ITIL Cyber Resilience Approach

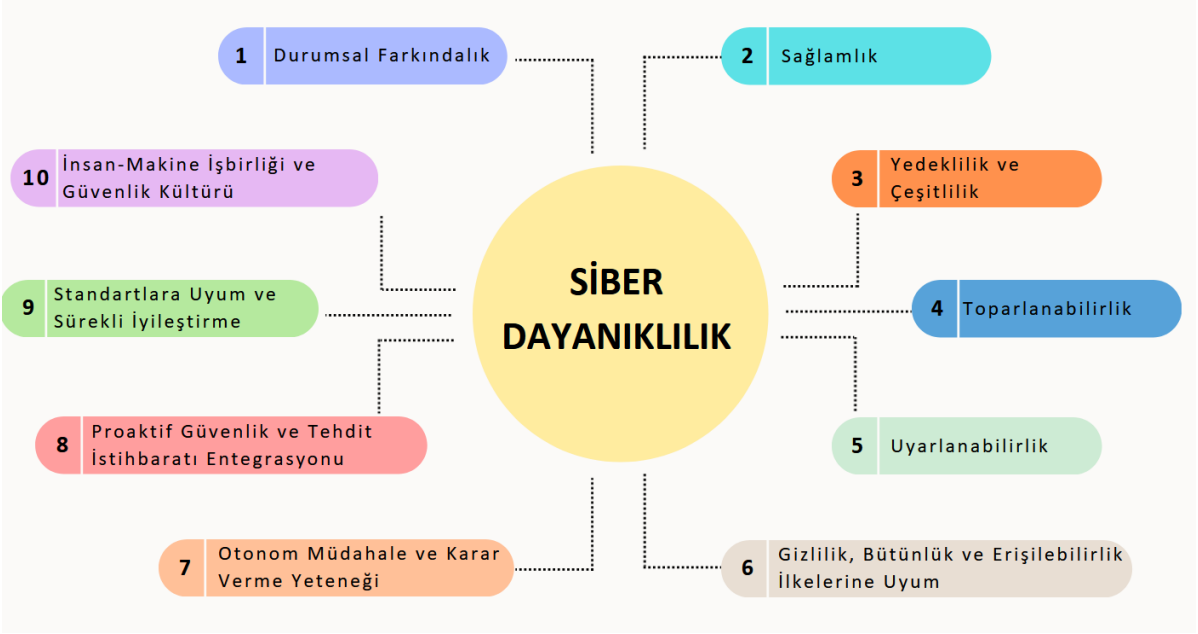
ITIL (Bilgi Teknolojileri Altyapı Kütüphanesi), bilgi teknolojileri hizmet yönetimi alanında dünya genelinde yaygın biçimde benimsenen bir çerçeve olup bilişim teknolojileri hizmetlerinin tasarımı, sunumu, yönetimi ve sürekli iyileştirilmesi süreçlerini sistematik hale getirmektedir (Axelos, 2019). ITIL kuruluşların teknolojik altyapılarını yalnızca operasyonel düzeyde değil stratejik planlama, müşteri odaklılık ve risk yönetimi perspektifiyle yönetmelerini sağlayan süreç tabanlı bir yaklaşım sunmaktadır. Bu yönüyle ITIL çerçevesi siber dayanıklılığın operasyonel kapasitesini güçlendirmekte ve bilişim teknolojileri hizmetlerinin güvenli, sürdürülebilir ve esnek biçimde sunulmasına katkı sağlamaktadır. ITIL bilgi teknolojileri hizmet yönetimine daha çevik, değer odaklı ve bütüncül bir yaklaşım kazandırmak amacıyla yeniden yapılandırılmıştır. Bu kapsamında Genel Yönetim Uygulamaları, Hizmet Yönetimi Uygulamaları ve Teknik Yönetim Uygulamaları olmak üzere üç temel uygulama alanı tanımlamakta ve bu alanlar aracılığıyla hizmet yönetimi süreçlerini yönetişimden operasyona kadar bütünleştirmektedir. ITIL'de tanımlanan üç temel domain yalnızca hizmet yönetimini değil, aynı zamanda stratejik yönetişimden teknik uygulamaya kadar tüm katmanlarda siber dayanıklılığı kurumsallaştıran bir yapı sunmaktadır. Bu yapılar, kurumların bilişim teknolojileri hizmetlerini sadece etkili değil, aynı zamanda güvenli ve sürdürülebilir biçimde sunmalarını mümkün kılmaktadır.

İlk olarak "Genel Yönetim Uygulamaları" alanı organizasyonun stratejik planlama, yönetişim, risk yönetimi ve sürekli iyileştirme süreçlerini kapsamaktadır. Bu uygulama grubu, aynı zamanda bilgi güvenliği yönetimi, mevzuat uyumu ve organizasyonel değişim yönetimi gibi yapısal konuları da içermektedir. Siber dayanıklılık açısından bakıldığında, bu alan tehditleri önceden öngörmeye, güvenlik politikalarının geliştirilmesine ve dayanıklılığı destekleyen yönetim mekanizmalarının kurumsal düzeyde yerleşmesine olanak tanımaktadır. Ayrıca sürekli iyileştirme kültürünün teşvik edilmesi sayesinde, kurumların değişen tehdit ortamına daha hızlı uyum sağlayabilmeleri sağlanmaktadır. İkinci domain olan "Hizmet Yönetimi Uygulamaları" ITIL'in geleneksel güçlü yönünü oluşturan süreç tabanlı hizmet yönetimi yaklaşımını temsil etmektedir. Bu kapsamda olay yönetimi, problem yönetimi, değişiklik kontrolü, hizmet düzeyi yönetimi ve iş sürekliliği yönetimi gibi süreçler yer almaktadır. Bu domain siber dayanıklılık bağlamında kritik öneme sahiptir çünkü sistem kesintileri, siber saldırılar veya diğer hizmet aksaklıkları durumunda etkili bir müdahale ve toparlanma süreci yürütülmesini mümkün kılmaktadır. Olayların kök nedenlerine ulaşılması, tekrarının önlenmesi ve hizmet kalitesinin sürdürülebilir şekilde iyileştirilmesi, bu domainin siber tehditlere karşı güçlü bir savunma hattı oluşturmasına katkı sağlamaktadır. Son olarak "Teknik Yönetim Uygulamaları" domaini bilişim teknolojileri altyapısı ve uygulama ortamlarının sürdürülebilir şekilde yönetilmesine odaklanmaktadır. Altyapı ve platform yönetimi, yazılım geliştirme ve dağıtımı gibi teknik süreçleri içeren bu domain, sistem mimarilerinin güvenli şekilde kurulmasını, yazılımların güncel tutulmasını ve operasyonel teknolojilerin güvenliğini sağlamaktadır. Siber dayanıklılık açısından bu alan, özellikle güvenlik açıklarının yönetimi, sistem yedekleme, erişim kontrolleri ve teknik konfigürasyonların sağlamlığı gibi konularda doğrudan katkı sunmaktadır. Bu teknik altyapı güvenliği, hizmetlerin hem saldırıya karşı korunmasında hem de olay sonrası toparlanmasında belirleyici rol oynamaktadır.

Siber dayanıklılık bağlamında, ITIL'in olay yönetimi, problem yönetimi, değişiklik yönetimi ve hizmet sürekliliği yönetimi gibi süreçleri organizasyonların kriz anlarında etkili yanıt verebilmesini ve sistematik biçimde toparlanabilmesini mümkün kılmaktadır. Bu süreçler yalnızca teknik düzeyde aksaklıkları gidermeyi değil, aynı zamanda olayların kök nedenlerini analiz etmeyi, önleyici tedbirler geliştirmeyi ve kullanıcı deneyimini korumayı da hedeflemektedir. ITIL'in kurumsal yapıya entegre edilmesi BT hizmetleriyle ilgili rollerin ve sorumlulukların açık biçimde tanımlanmasına yardımcı olmakta güvenlik ve dayanıklılık politikalarının operasyonel uygulamalarla uyumlu hale gelmesini sağlamaktadır. Ayrıca ITIL ISO/IEC 20000 ve 27001 gibi hizmet yönetimi standartlarıyla uyumlu yapısıyla denetlenebilir ve belgelendirilebilir bir bilişim teknolojileri hizmet yönetim ortamı oluşturmaktadır. Bu yönüyle ITIL yalnızca hizmet kalitesini artırmakla kalmamakta aynı zamanda siber saldırılara, operasyonel kesintilere ve teknolojik değişimlere karşı kurumsal adaptasyon ve toparlanma kabiliyetini sistematik biçimde güçlendirmektedir. Bu nedenle ITIL siber dayanıklılık stratejilerinin operasyonel temelini oluşturan, uygulama odaklı ve sürdürülebilir bir model sunmaktadır.

3. SİBER SALDIRILARA KARŞI DİRENÇLİ SİSTEMLERİN ÖZELLİKLERİ / CHARACTERISTICS OF SYSTEMS RESISTANT TO CYBER ATTACKS

Siber saldırıların sıklığı, karmaşıklığı ve etkisi giderek artarken, yalnızca güvenlik önlemleriyle tehditleri önlemek yeterli olmamaktadır. Bu nedenle, sistemlerin saldırı öncesinde hazırlıklı olması, saldırı anında temel işlevlerini sürdürebilmesi ve saldırı sonrasında hızlıca toparlanabilmesi için dayanıklılık kavramı ön plana çıkmaktadır. Dayanıklı bir sistem sadece saldırıları engellemekle kalmaz, aynı zamanda bu saldırılara karşı dayanıklı, uyarlanabilir ve sürdürülebilir bir yapıya sahiptir (Abdelkader vd., 2024). Çalışmanın 2. bölümündeki uluslararası standartlarda ve güvenlik çerçevelerinde tanımlandığı üzere, siber saldırılara karşı dayanıklı sistemler, birtakım evrensel özellikleri bünyesinde barındırmaktadır. Bu bölümde, siber dayanıklılığın temel yapı taşlarını oluşturan söz konusu sistem özellikleri başlıklar halinde ele alınmakta ve her biri kısa açıklamalarla değerlendirilmektedir. Bu özellikler, siber dayanıklılık kavramının bütüncül yapısını yansıtmakta olup, sistemlerin saldırı öncesi hazırlık, saldırı anında işlevsellik ve saldırı sonrası toparlanma kapasitelerini birlikte ele almaktadır. Şekil 1'de, siber saldırılara karşı dayanıklı sistemlerin sahip olması gereken temel 10 özellik görsel olarak sunulmuştur.



Şekil 1: *Siber Saldırılara Karşı Dayanıklı Sistemlerin Özellikleri*

3.1 Durumsal Farkındalık / Situational Awareness

Durumsal farkındalık, bir sistemin ya da organizasyonun kendi iç süreçlerini ve çevresel tehdit ortamını gerçek zamanlı olarak algılayabilme, anlayabilme ve bu bilgileri karar alma süreçlerine entegre edebilme kapasitesidir. Siber dayanıklılık bağlamında durumsal farkındalık, yalnızca mevcut sistem bileşenlerinin durumunu izlemekle sınırlı değildir; aynı zamanda ağ trafiği, kullanıcı davranışları, dış tehdit istihbaratı ve operasyonel anormallikler gibi çok katmanlı verilerin analizini içeren dinamik bir süreçtir (Franke & Brynielsson, 2014). Bu yetenek, özellikle hızlı değişen tehdit ortamlarında, saldırıların erken aşamada tespit edilmesi ve etkili müdahale stratejilerinin geliştirilmesi açısından kritik öneme sahiptir. Durumsal farkındalık algılama, anlama ve öngörü olmak üzere üç temel bileşenden oluşur. Algılama aşamasında, sistem içerisindeki ve çevresindeki olaylara dair loglar, ağ trafiği, kullanıcı aktiviteleri gibi veriler toplanır. Anlama aşamasında bu veriler bir bağlama oturtularak yorumlanır, örneğin bu aşamada bir kullanıcı davranışının olağandışı olup olmadığı analiz edilir. Son aşamada ise mevcut durumdan hareketle yakın gelecekte ne tür tehditlerin gelişebileceği öngörülmeye çalışılır. Bu sayede yalnızca tepkisel değil, proaktif güvenlik yaklaşımları geliştirilebilir.

Durumsal farkındalık yalnızca teknik bir yetkinlik olarak değil aynı zamanda organizasyonel bir kabiliyet olarak da değerlendirilmelidir. Bu kapsamda, güvenlik operasyon merkezlerinin tehdit istihbaratı ekiplerinin ve sistem yöneticilerinin koordineli çalışması gerekir. Ayrıca görselleştirme araçları, SIEM (Güvenlik Bilgi ve Olay Yönetimi) sistemleri ve yapay zeka destekli analiz platformları, bu farkındalığın artırılmasına katkı sunan önemli bileşenlerdir. Etkili bir durumsal farkındalık, yalnızca saldırılara karşı hızlı yanıt vermeyi değil, aynı zamanda organizasyonun genel güvenlik duruşunu sürekli iyileştirmesini de sağlar. Bu nedenle, siber dayanıklı sistemlerin tasarımında ve operasyonel yönetiminde durumsal farkındalık, temel bir ön koşul olarak ele alınmalıdır.

3.2 Sağlamlık / Robustness

Sağlamlık bir sistemin siber saldırı, teknik arıza, kullanıcı hatası veya beklenmeyen dışsal etkiler gibi olumsuz durumlar karşısında temel işlevlerini sürdürebilme kapasitesini ifade eder. Siber güvenlik bağlamında sağlamlık, sistemlerin tehditlere karşı kırılganlığının düşük, dayanıklılığının ise yüksek olması anlamına gelir (M. M. Saeed & Alsharidah, 2024). Sağlam bir sistem, bir bileşeninin başarısızlığa uğraması durumunda dahi genel hizmet sürekliliğini koruyabilecek şekilde tasarlanmıştır. Bu bağlamda sağlamlık, siber dayanıklılığın en temel yapı taşlarından biridir ve saldırıların operasyonel süreçlere minimum etkiyle yansımasını sağlar.

Teknik açıdan sağlamlık, sistem mimarisinde çok katmanlı güvenlik prensibinin uygulanması, kritik bileşenlerin izole edilmesi, erişim denetimlerinin sıkılaştırılması ve ağ segmentasyonu gibi önlemlerle güçlendirilir. Aynı zamanda, yazılım ve donanım bileşenlerinin hata toleranslı olacak şekilde yapılandırılması, sistemin herhangi bir zafiyeti saldırganın yayılma alanına dönüştürmesini engeller. Örneğin, bir ağ segmentinde gerçekleşen saldırı, diğer segmentlere sıçramadan lokalize edilebilir; ya da bir hizmette yaşanan kesinti, yedek sistemlerin otomatik devreye girmesiyle kullanıcıya yansıtılmadan telafi edilebilir.

Sağlamlığın yüksek olduğu bir sistem aynı zamanda tek nokta hatası barındırmaz yani herhangi bir bileşenin çökmesi tüm sistemin durmasına yol açmaz. Bu tür bir tasarım yaklaşımı, özellikle kritik altyapılarda büyük önem taşır. Ayrıca, sağlamlık sadece fiziksel sistem düzeyinde değil, uygulama ve hizmet düzeyinde de geçerlidir. Web uygulamalarında kullanıcı giriş verinin doğrulanması, hata yönetimi veya güvenli kodlama gibi saldırıya dayanıklı yazılım geliştirme ilkeleri bu kapsamda değerlendirilir. Sağlamlık özelliği, bir sistemin yalnızca saldırıya karşı dayanma değil, aynı zamanda saldırının etkisini sınırlama kapasitesini de ifade eder. Bu özellik, diğer dayanıklılık bileşenleriyle birlikte düşünüldüğünde, kurumların siber tehditlere karşı sadece savunma değil, aynı zamanda süreklilik odaklı bir güvenlik anlayışını benimsemelerine katkı sağlar.

3.3 Yedeklilik ve Çeşitlilik / Redundancy and Diversity

Yedeklilik ve çeşitlilik, sistemlerin beklenmedik durumlar ve saldırılar karşısında işlevselliğini sürdürebilmesini sağlayan tamamlayıcı özelliklerdir. Yedeklilik bir sistemdeki kritik bileşenlerin veya hizmetlerin yedek kopyalarının bulunması anlamına gelirken çeşitlilik ise aynı işlevi yerine getiren sistem bileşenlerinin farklı mimari, yazılım ya da üretici kaynaklarına dayanarak oluşturulmasıdır (Troubitsyna, 2023). Bu iki kavram, birlikte uygulandığında hem sistemin hata toleransını artırmakta hem de saldırı yüzeyini farklılaştırarak tehdit aktörlerinin başarı şansını azaltmaktadır.

Yedeklilik özellikle yüksek erişilebilirlik gerektiren sistemlerde, hizmet sürekliliğini sağlamak adına kritik öneme sahiptir. Örneğin, bir veri merkezinde kullanılan sunucular, ağ cihazları ya da veri tabanları; aktif-pasif veya aktif-aktif konfigürasyonlarla yedeklenerek, herhangi bir arıza ya da saldırı durumunda devreye girecek alternatif yapılarla güçlendirilir. Bu sayede bir bileşenin işlev dışı kalması, sistem genelinde kesintiye yol açmaz. Aynı şekilde, bulut tabanlı mimarilerde coğrafi olarak dağıtılmış veri yedekleri hem doğal afetlere hem de hedefli saldırılara karşı koruma sağlar. Çeşitlilik ise, sistemin homojenliğinden kaynaklanan yapısal zafiyetleri azaltma amacına hizmet eder. Örneğin, tüm sunucuların aynı işletim sistemine sahip olması durumunda, bu işletim sistemine yönelik bir zafiyetin tüm yapıyı etkileme riski oldukça yüksektir. Benzer şekilde bazı saldırılar belirli donanım üreticilerine yönelik olabilmektedir. Farklı üreticilerden gelen donanımlar, değişik işletim sistemleri veya alternatif yazılım çözümleri kullanılarak oluşturulan heterojen yapılar, saldırıların yayılımını sınırlandırır. Bu bağlamda çeşitlilik, sistem içi teknolojik tekilleşmenin önüne geçerek, saldırıların domino etkisiyle sistem genelini etkilemesini zorlaştırır.

Yedeklilik ve çeşitlilik yalnızca donanımsal değil, aynı zamanda yazılımsal, ağ mimarisi ve insan kaynağı düzeyinde de uygulanabilir. Örneğin, ağ trafiğinin farklı rotalardan programlanarak yönlendirilmesi, alternatif kimlik doğrulama mekanizmalarının bulunması ya da güvenlik operasyonlarının farklı ekipler tarafından çapraz denetlenmesi, bu yaklaşımın farklı katmanlarda uygulanabilirliğini gösterir. Yedeklilik ve çeşitlilik ilkeleri, sistemin tek nokta zafiyetlerini azaltarak ve operasyonel esneklik kazandırarak, siber saldırıların etkisini sınırlayan, toparlanma süresini kısaltan ve genel dayanıklılık kapasitesini artıran çok katmanlı bir savunma yaklaşımı sunar. Bu nedenle, özellikle yüksek öneme sahip altyapılarda bu ilkelerin sistem tasarımı ve güvenlik politikalarına entegre edilmesi, bilimsel ve uygulamalı birçok çalışmada öncelikli bir strateji olarak önerilmektedir.

3.4 Toparlanabilirlik / Recoverability

Toparlanabilirlik bir sistemin siber saldırı, donanım arızası, veri ihlali veya başka herhangi bir kesinti sonrası işlevsel durumuna yeniden ve sürdürülebilir bir şekilde dönebilme yeteneğini ifade eder. Siber dayanıklılık bağlamında toparlanabilirlik, sadece verilerin geri yüklenmesi değil aynı zamanda sistemlerin, süreçlerin ve hizmetlerin minimum kayıpla, mümkün olan en kısa sürede yeniden devreye

alınması anlamına gelir (Beretas, 2024). Bu kavram, özellikle iş sürekliliği ve felaket kurtarma planlamalarının merkezinde yer almakta olup, saldırıya uğramış sistemlerin etkili bir şekilde yeniden yapılandırılmasını ve operasyonel stabilitenin sağlanmasını hedefler.

Toparlanabilirliğin temel bileşenleri arasında veri yedekleme stratejileri, otomatik kurtarma prosedürleri, felaket senaryolarına dayalı önceden tanımlanmış eylem planları ve düzenli test edilen kurtarma tatbikatları yer almaktadır. Kritik sistemlerin günlük, haftalık ya da gerçek zamanlı yedeklerinin alınması, bu yedeklerin fiziksel olarak ayrı ve güvenli ortamlarda saklanması, fidye yazılımı gibi saldırı türleri karşısında veri bütünlüğünün korunmasını sağlar. Ayrıca, değiştirilemez yedekleme teknolojileri, saldırganın yedekleri şifreleyerek erişimi engelleme girişimlerini geçersiz kılar. Toparlanabilirlik yalnızca teknik altyapı düzeyinde değil, organizasyonel ve yönetsel boyutlarda da ele alınmalıdır. Bir kurumun toparlanabilirliği bilgi teknolojileri ekibinin müdahale hızına, iletişim stratejilerine, iç koordinasyon yapısına ve üst yönetimin karar alma yetkinliğine doğrudan bağlıdır. Bu nedenle kurumsal düzeyde müdahale ve iş sürekliliği planlarının oluşturulması, tüm paydaşların rollerini bildiği, önceden tanımlı senaryolara uygun olarak hızlı aksiyon alınmasını sağlar. Ayrıca, saldırı sonrası yapılacak analizler ve etki çalışmaları gelecekteki toparlanma kabiliyetini geliştirmek açısından kritik rol oynayacaktır. Literatürde toparlanabilirlik, sıklıkla MTTR (Toparlanıncaya Kadar Geçen Ortalama Süre) ve RPO (Kurtarma Noktası Hedefi) gibi metriklerle ölçülmektedir (Maglaras, 2022). MTTR, sistemin normal çalışmasına dönmesi için geçen süreyi ifade ederken RPO ise veri kaybı açısından kabul edilebilir zaman aralığını tanımlar. Bu metriklerin düşük tutulması yüksek toparlanabilirlik seviyesine işaret eder. Kurumların bu hedefleri karşılayabilmesi için sistematik testler, sürekli izleme araçları ve otomasyon tabanlı kurtarma sistemlerine yatırım yapmaları gerekmektedir.

Toparlanabilirlik, dayanıklı sistem mimarilerinin saldırıya uğrama ihtimalini tamamen ortadan kaldırmasa da saldırı sonrası etkilerin sınırlandırılması ve organizasyonun normal faaliyetlerine dönebilmesi açısından hayati bir savunma katmanıdır. Bu özellik, siber dayanıklılığı sürdürülebilir kılmak ve kurumsal itibar ile iş sürekliliğini korumak açısından stratejik bir öneme sahiptir.

3.5 Uyarlanabilirlik / Adaptability

Uyarlanabilirlik bir sistemin ya da organizasyonun siber tehdit ortamındaki değişimlere yanıt verebilme, yeni koşullara göre kendini yapılandırabilme ve saldırılar sonrasında daha dayanıklı bir duruma evrilebilme yeteneğini ifade eder. Siber dayanıklılık bağlamında bu kavram, sadece mevcut saldırılara tepki vermekle sınırlı olmayan, aynı zamanda gelecekteki tehditlere karşı hazırlık kapasitesini sürekli geliştirmeye yönelik dinamik bir güvenlik anlayışını temsil eder (Munusamy & Khodadi, 2023). Uyarlanabilirlik, özellikle siber tehditlerin karmaşık, belirsiz ve sürekli evrimleşen doğası karşısında, organizasyonların öğrenen sistemler haline gelmelerini zorunlu kılar.

Bu yetenek hem teknik sistem mimarilerinde hem de kurumsal süreçlerde uygulanabilir. Teknik düzeyde uyarlanabilirlik, yapay zeka destekli tehdit algılama sistemlerinin yeni saldırı kalıplarını öğrenmesi, güvenlik politikalarının koşullara göre otomatik güncellenmesi ve sistem konfigürasyonlarının dinamik biçimde yeniden yapılandırılması gibi özelliklerle somutlaşır. Örneğin, bir ağ segmentinde alışılmadık bir davranış tespit edildiğinde sistemin otomatik olarak erişim kurallarını sıkılaştırması ya da anomaliye göre güvenlik duvarı yapılandırmasını güncellemesi, uyarlanabilirliğin teknik bir yansımasıdır.

Kurumsal düzeyde ise uyarlanabilirlik siber olayların ardından yapılan olay sonrası analizlerinin, iş süreçlerinin yeniden düzenlenmesine ve güvenlik politikalarının güncellenmesine entegre edilmesini içerir. Bu noktada edinilen dersler döngüsünün aktif biçimde işletilmesi, organizasyonun tehditlere karşı bağışıklık geliştirmesine olanak tanır. Ayrıca regülasyonlar, sektörel tehdit istihbaratı ve paydaş geri bildirimleri doğrultusunda siber güvenlik stratejilerinin periyodik olarak güncellenmesi, uyarlanabilirlik kapasitesinin kurumsallaşmasını sağlar.

Uyarlanabilirliğin önemli bir bileşeni de esneklik ile birlikte düşünülmesidir. Esnek sistemler, yalnızca bir duruma uyum sağlamakla kalmaz, aynı zamanda farklı senaryolar için alternatif çözüm yollarını barındırır. Bu bağlamda, çoklu savunma katmanları, modüler sistem tasarımları ve alternatif operasyonel senaryolar, uyarlanabilirliğin teknik temelini oluşturur. Literatürde uyarlanabilirlik çoğu

zaman CRMM (Siber Esneklik Olgunluk Modelleri) kapsamında değerlendirilmekte ve organizasyonların tehditlere karşı reaktiften proaktife, oradan da öngörücü seviyeye geçiş kapasitesi ile ilişkilendirilmektedir (Shaked vd., 2021). Bu doğrultuda, yüksek uyarlanabilirlik düzeyi, yalnızca olaylara hızlı yanıt verebilme değil, aynı zamanda gelecekteki riskleri önceden tahmin ederek stratejik hazırlık yapabilme becerisi olarak da tanımlanır.

3.6 Gizlilik, Bütünlük ve Erişilebilirlik İlkelerine Uyum / Compliance with Confidentiality, Integrity and Accessibility Principles

Siber dayanıklı sistemlerin temelinde, bilgi güvenliğinin evrensel ilkeleri olarak kabul edilen gizlilik, bütünlük ve erişilebilirlik yer almaktadır (Whitman & Mattord, 2011). Bu üç ilkeye uyum, bir sistemin sadece saldırılara karşı korunmasını değil, aynı zamanda bilgi varlıklarının güvenliğini sürdürülebilir biçimde yönetebilmesini sağlamaktadır. Dayanıklılık bağlamında bu ilkeler sistemin normal işleyişini sürdürebilmesi, güvenilir bilgi üretmesi ve kritik verilere sadece yetkili kullanıcıların zamanında erişebilmesini teminat altına alır.

Gizlilik, yetkisiz erişimlerin önlenmesini ve verilerin yalnızca yetkili kişi ya da sistemler tarafından görüntülenebilmesini ifade etmektedir. Bu doğrultuda, erişim kontrolü, şifreleme, çok faktörlü kimlik doğrulama ve veri sınıflandırma politikaları, gizliliği sağlamaya yönelik temel önlemler arasında yer alır. Siber saldırılarda sıklıkla hedef alınan kişisel verilerin ve kurumsal sırların korunması, özellikle KVKK (Kişisel Verileri Koruma Kanunu), GDPR(Genel Veri Koruma Tüzüğü) gibi düzenlemelere uyum açısından da kritik öneme sahiptir. Bütünlük, verilerin izinsiz değiştirilmesini, silinmesini ya da bozulmasını önlemeyi amaçlamaktadır. Bu kapsamda kullanılan dijital imzalar, bütünlük kontrolü algoritmaları ve log kayıtlarının güvenli yönetimi, sistemin olaylardan sonra güvenilir veri üretmeye devam etmesini mümkün kılmaktadır. Özellikle finansal sistemlerde ve kritik altyapılarda bütünlük ihlalleri, doğrudan operasyonel ve hukuki riskleri beraberinde getirdiği için dayanıklı sistemlerde bu ilkeye sıkı bağlılık gerektirmektedir. Erişilebilirlik ise bilginin ve hizmetlerin ihtiyaç duyulan anda, yetkili kullanıcılar tarafından erişilebilir olmasını ifade etmektedir. DDoS saldırıları, sistem arızaları ya da doğal afetler gibi kesinti yaratabilecek durumlara karşı yedeklilik, felaket kurtarma planları ve yük dengeleme çözümleri erişilebilirliği garanti altına almaktadır. Dayanıklı sistemler bu ilkeye uyumu sadece fiziksel düzeyde değil aynı zamanda mantıksal erişim stratejileri ve kullanıcı deneyimini koruyarak da sağlamaktadır.

Bu üç ilkeye uyum yalnızca teknik sistem tasarımında değil aynı zamanda kurumsal politika, risk yönetimi, kullanıcı eğitimleri ve mevzuat uyum süreçlerinde de bütüncül olarak uygulanmalıdır. Hem bireysel hem de kurumsal düzeyde siber güvenlik stratejilerinin ölçütlerini belirleyen bu ilkeler siber dayanıklılık çerçevesinde vazgeçilmez olarak kabul edilmelidir.

3.7 Otonom Müdahale ve Karar Verme Yeteneği / Autonomous Intervention and Decision Making Capability

Otonom müdahale ve karar verme yeteneği, siber dayanıklı sistemlerin hızla gelişen tehdit ortamına karşı insan müdahalesine ihtiyaç duymadan gerçek zamanlı tepki verebilmesini sağlayan ileri düzey bir özelliktir (Dehghantanha vd., 2023). Günümüzde saldırılar 7/24 şekilde ve milisaniyeler içinde gerçekleşebildiğinden, geleneksel manuel güvenlik yanıt mekanizmaları çoğu durumda yetersiz kalmaktadır. Bu bağlamda, yapay zeka, makine öğrenmesi ve davranışsal analiz teknolojileri ile entegre edilen sistemler olağandışı aktiviteleri tespit ederek proaktif savunma önlemlerini devreye alabilmektedir. Bu yetenek yalnızca saldırıların erken aşamalarda etkisiz hale getirilmesini sağlamakla kalmamakta aynı zamanda olayın yayılma potansiyelini sınırlandırarak sistem bütünlüğünün korunmasına da katkı sunmaktadır.

Otonom sistemler tehdit algılama/sınıflandırma süreçlerini büyük ölçüde otomatikleştirmekte ve zararlı etkinlikleri tanımladıktan sonra erişim kısıtlama, ağ izolasyonu, kullanıcı oturumu sonlandırma veya şüpheli süreçleri durdurma gibi müdahaleleri doğrudan ve gecikmesiz gerçekleştirebilmektedir. Bu tür sistemler özellikle yüksek hacimli ve karmaşık ağ ortamlarında, bilişim uzmanlarının gözünden kaçabilecek saldırıları yüksek doğrulukla belirleyebilmektedir. Ayrıca, tehdit istihbarat kaynakları ile

sürekli senkronize edilerek kendini güncel tutmakta ve yeni saldırı tekniklerine karşı savunma katmanlarını dinamik biçimde yeniden yapılandırabilmektedir.

Siber dayanıklılık perspektifinden bakıldığında, otonom karar verme mekanizmaları, organizasyonun saldırı anındaki operasyonel sürekliliğini sağlamaktadır. Bu yetenek olay müdahale süresini önemli ölçüde kısaltmakta, insan hatasını azaltmakta ve kaynakların daha stratejik alanlara yönlendirilmesine olanak tanımaktadır. Ek olarak olay sonrası elde edilen verilerin analizi sayesinde bu sistemler zamanla daha etkin hale gelmekte ve organizasyonun genel güvenlik duruşunu güçlendirmektedir. Otonom müdahale ve karar verme kapasitesi, yalnızca teknolojik bir avantaj olarak değil, aynı zamanda kritik hizmetlerin sürekliliğini teminat altına alan bir dayanıklılık mekanizması olarak değerlendirilmektedir. Bu nedenle, modern siber güvenlik mimarilerinde otonom sistemlerin entegrasyonu, stratejik öncelik haline gelmektedir.

3.8 Proaktif Güvenlik ve Tehdit İstihbaratı Entegrasyonu / Proactive Security and Threat Intelligence Integration

Proaktif güvenlik ve tehdit istihbaratı entegrasyonu, siber dayanıklılığı artırma hedefi doğrultusunda, yalnızca gerçekleşmiş saldırılara tepki vermekle sınırlı kalmayan aynı zamanda olası tehditleri önceden tespit etmeye ve engellemeye yönelik ön alıcı yaklaşımlar benimseyen bir güvenlik anlayışını temsil etmektedir (S. Saeed vd., 2023). Bu yaklaşım kapsamında, saldırganların taktikleri, teknikleri ve prosedürleri, açık kaynaklardan, ticari istihbarat sağlayıcılarından veya güvenlik topluluklarından elde edilen verilerle sürekli olarak analiz edilmekte ve sistem savunmaları bu bilgiler ışığında güncellenmektedir. Bu sayede organizasyonlar, yalnızca pasif savunma yapmak yerine, dinamik tehdit ortamına uyum sağlayan ve değişken risklere karşı dayanıklı yapılar geliştirmektedir.

Tehdit istihbaratı, zararlı yazılımların imzaları, güvenliği ihlal edilmiş IP adresleri, zafiyet bilgileri ve saldırgan altyapılarına dair göstergeleri içermekte ve bu göstergeler, güvenlik bilgi ve olay yönetim sistemleri, güvenlik yönetim platformları ile entegre edilmektedir. Bu entegrasyon güvenlik ekiplerinin karar alma süreçlerini iyileştirmekte ve müdahale sürelerini minimize etmektedir. Ayrıca, makine öğrenimi tabanlı korelasyon motorları sayesinde bu veriler otomatik biçimde analiz edilmekte ve normal sistem davranışlarından sapmalar daha hassas şekilde belirlenebilmektedir.

Proaktif güvenlik stratejileri kapsamında zafiyet taramaları, sızma testleri, saldırı yüzeyi analizi ve tehdit modelleme teknikleri düzenli olarak uygulanmaktadır. Bu uygulamalar sayesinde sistemdeki potansiyel güvenlik açıkları saldırganlar bunları istismar etmeden önce belirlenmektedir. Ayrıca, honeypot ve deception teknolojileri gibi savunma yöntemleri de saldırgan davranışlarını gözlemleyerek tehdit istihbaratının daha zengin hale gelmesini sağlamaktadır. Bu bağlamda, proaktif güvenlik ve tehdit istihbaratı entegrasyonu, kurumların siber tehditlere karşı yalnızca reaktif değil, stratejik olarak hazırlıklı ve öngörülü bir konumda bulunmasını mümkün kılmaktadır.

3.9 Standartlara Uyum ve Sürekli İyileştirme / Compliance with Standards and Continuous Improvement

Standartlara uyum ve sürekli iyileştirme siber dayanıklılığın sürdürülebilirliğini sağlamada kritik rol oynayan iki tamamlayıcı unsuru oluşturmaktadır. ISO/IEC 27001, NIST Siber Güvenlik Çerçevesi, ISO 27001 gibi uluslararası kabul görmüş standartlara uyum sağlamak kurumların bilgi güvenliği, iş sürekliliği ve risk yönetimi süreçlerini sistematik bir yapıya kavuşturmaktadır. Bu standartlar yalnızca minimum güvenlik gereksinimlerini tanımlamakla kalmamakta aynı zamanda organizasyonların siber tehditlere karşı dayanıklılığını ölçebilir, denetlenebilir ve geliştirilebilir hale getirmektedir. Uyum süreçleri, kurumların güvenlik politikalarını, prosedürlerini ve kontrollerini belirli aralıklarla gözden geçirmesini ve dış denetimlerle olgunluk seviyelerini değerlendirmesini mümkün kılmaktadır. Sürekli iyileştirme bu standartlara uyumun statik bir hedef değil, dinamik bir gelişim süreci olduğunu vurgulamaktadır. Kurumlar düzenli iç denetimler, olay sonrası analizler, performans göstergeleri ve kullanıcı geri bildirimleri aracılığıyla mevcut güvenlik yapılarını değerlendirmekte ve bu değerlendirmelere dayalı olarak politikalarını, süreçlerini ve teknolojik altyapılarını güncellemektedir. Özellikle değişen tehdit peyzajı, yeni regülasyonlar ve teknolojik gelişmeler karşısında, sürekli

iyileştirme kültürünün benimsenmesi, güvenlik seviyesinin zaman içinde zayıflamasını engellemektedir.

Siber olay müdahale süreçlerinden elde edilen bulguların kurumsal bilgiye dönüştürülmesi aynı tür saldırılara karşı daha hazırlıklı olunmasını sağlamaktadır. Kurumlar bu doğrultuda PUKÖ döngüsünü uygulayarak siber dayanıklılık kapasitesini sürekli geliştirmektedir. Standartlara uyum ve sürekli iyileştirme, böylece yalnızca mevzuata uygunluğu değil, aynı zamanda organizasyonun siber olgunluk seviyesinin yükseltilmesini ve tehdit ortamına stratejik uyum sağlanmasını mümkün kılmaktadır.

3.10 İnsan-Makine İşbirliği ve Güvenlik Kültürü / Human-Machine Cooperation and Safety Culture

İnsan-makine işbirliği ve güvenlik kültürü siber dayanıklı sistemlerin yalnızca teknik altyapıya değil aynı zamanda insan faktörüne ve organizasyonel davranışlara dayandığını ortaya koymaktadır. Günümüz siber güvenlik ortamında otomatik sistemler ve yapay zeka destekli çözümler yüksek doğrulukta tehdit tespiti ve müdahale imkanı sunmaktadır. Buna rağmen bu teknolojilerin etkinliği insan uzmanlığının gözetimi, değerlendirmesi ve yönlendirmesi ile anlam kazanmaktadır. Bu kapsamda güvenlik operasyon merkezlerinde görev yapan analistler ile otonom sistemler arasında kurulan etkileşimli işbirliği hem saldırıların daha isabetli şekilde sınıflandırılmasını hem de uygun müdahale stratejilerinin geliştirilmesini mümkün kılmaktadır.

İnsan-makine işbirliği yalnızca güvenlik uzmanları düzeyinde değil tüm çalışanları kapsayan bir güvenlik farkındalığı kültürü ile desteklenmektedir. Bu kültür çalışanların bilgi güvenliği politikalarına uymasını teşvik etmekte, şüpheli aktiviteleri raporlamalarını kolaylaştırmakta ve sosyal mühendislik gibi insan odaklı saldırı türlerine karşı savunma hattı oluşturmaktadır. Eğitim programları, simülasyonlar ve düzenli güvenlik tatbikatları güvenlik kültürünün kurumsal bellekte yer edinmesini sağlamaktadır. Aynı zamanda bu farkındalık çalışmaları insan kaynağının yalnızca zayıf halka olma ihtimalini azaltmamakta aksine güvenliğin aktif bir bileşeni haline gelmesini teşvik etmektedir. Güvenlik kültürü yönetim desteği, sürekli iletişim, açık geri bildirim mekanizmaları ve davranışsal güvenlik metrikleri ile kurumsallaştırılmaktadır. İnsan-makine işbirliği ise yalnızca iş yükünü bölüştürmekle kalmamakta aynı zamanda karmaşık ve çok katmanlı tehdit ortamına karşı daha esnek, öğrenebilen ve karar verme yeteneği yüksek sistemlerin oluşmasını desteklemektedir. Bu bütüncül yaklaşım siber dayanıklılığı sadece teknolojik değil, aynı zamanda sosyoteknik bir sistem olarak ele almayı mümkün kılmaktadır.

4. KURUMLAR İÇİN YALIN DİRENÇLİLİK ÇERÇEVESİ ÖNERİSİ/ BASIC RESILIENCE FRAMEWORK PROPOSAL FOR ORGANISATIONS

Siber saldırıların artan karmaşıklığı, akıllı üretim ortamlarında kapsamlı bir siber güvenlik stratejisi, risk değerlendirmesi, standartların uygulanması ve sürekli izleme gerekliliğini ortaya koymaktadır. Her sektörün kendi operasyonel yapısına göre uyarlanmış bir güvenlik yaklaşımı geliştirmesi, olası tehdit senaryolarına karşı dayanıklılığı artırarak operasyonel kesintileri ve veri kayıplarını önlemeye yardımcı olur (Meagher & Dhirani, 2024). Siber dayanıklılığa yönelik uluslararası standart ve çerçeveler kapsamlı rehberlik sağlasa da her kurum bu yapıları uygulayacak kapasiteye veya kaynağa sahip olmayabilir. Bu noktada, temel düzeyde uygulanabilir, yalın ve etkili dayanıklılık stratejilerinin hayata geçirilmesi kritik önem taşımaktadır. Bu bölümde çerçevelere tam uyum sağlayamayan kurumlar için temel düzeyde uygulanabilecek stratejik adımlar bütünsel bir yaklaşımla sunulmaktadır. Sunulan çerçevenin temel yapısı Tablo 4'te verilmiştir. Önerilen çerçevenin oluşturulmasında çalışmanın önceki bölümlerinde analiz edilen NIST CSF, ENISA rehberleri, ISO/IEC 27001, COBIT ve ITIL çerçevelerinin ortak prensipleri karşılaştırmalı olarak incelenmiş ve özellikle küçük ve orta ölçekli kurumların uygulayabileceği minimum gereksinimler temel alınmıştır. Her adım için odak alanı, kurumsal hedef ve üretilmesi gereken belge türleri, ilgili standartlardaki karşılıklarıyla eşleştirilerek tablo formatına dönüştürülmüştür. Bu yaklaşım önerilen çerçevenin hem bilimsel temellere dayalı hem de uygulanabilir niteliğe sahip olmasını sağlamaktadır.

Kritik Varlıkların Belirlenmesi ve Önceliklendirilmesi (KVBO) adımı, kurumun siber dayanıklılık kapasitesini temellendiren en önemli stratejik aşamalardan biridir. Bu adımda, kurumun işleyişi açısından kritik olan sistem, süreç, donanım ve veri varlıklarının sistematik biçimde envanteri çıkarılmakta ve bu varlıkların güvenlik, süreklilik ve etki düzeyine göre önceliklendirilmesi sağlanmaktadır. Örneğin bir elektrik şebekesinde güç üretim kontrol sistemleri, bir hastanede hayat destek cihazları veya bir finans kuruluşunda müşteri verilerinin bulunduğu veri tabanları bu kapsamda değerlendirilebilecek başlıca varlıklardır. CISA (ABD Siber Güvenlik ve Altyapı Güvenliği Ajansı) tarafından önerilen CRR (Siber Dayanıklılık İncelemesi) uygulamaları da bu aşamada rehberlik sağlayan yöntemler arasında yer almaktadır. Bu çalışmalar sayesinde, kısıtlı kaynaklar maksimum etki yaratacak alanlara tahsis edilmekte, korunması gereken öncelikli bileşenler belirlenmektedir. Kritik varlıkların envanteri yalnızca fiziksel sistemler veya donanımlarla sınırlı tutulmamalıdır. Günümüz dijital ekosisteminde veri, çoğu zaman en değerli varlık konumundadır. Bu nedenle kurum bünyesindeki tüm veri türlerinin sınıflandırılması ve korunması gereken bilgi varlıklarının ISO/IEC 27001 gibi standartlara uygun şekilde güvenlik düzeylerine göre kategorize edilmesi gerekmektedir. Veri envanteri, veri sınıflandırma dokümanı ve risk değerlendirme raporları bu aşamanın temel çıktı belgeleri arasında yer almaktadır. Böylelikle kurumun hangi varlıklarının daha sıkı korunması gerektiği belirlenmekte; izinsiz erişim, veri kaybı veya hizmet kesintisi gibi olaylara karşı daha dayanıklı bir yapı oluşturulmaktadır.

Tablo 4. *Önerilen Yalın Siber Güvenlik Dayanıklılık Çerçevesi*

Kod	Strateji	Odak Alanı	Hedef	Çıktı Belgeleri
KVBO	Kritik Varlıkların Belirlenmesi ve Önceliklendirilmesi	Varlık envanteri, veri sınıflandırma	En kritik işlev ve varlıkları tanımlayarak koruma önceliklerini belirlemek	Varlık Envanteri, Risk Değerlendirme Raporu, Veri Sınıflandırma Dokümanı
GMS	Güvenli Mimari ve Segmentasyon	Sistem mimarisi, ağ güvenliği	Saldırı yüzeyini küçültmek ve yayılmayı sınırlamak	Ağ Topolojisi Haritası, Segmentasyon Planı, Güvenlik Yapılandırma Raporu
YC	Yedeklilik ve Çeşitlilik	Sistem yedekleme, donanım-yazılım çeşitliliği	Hizmet sürekliliği sağlamak ve tekil arızalara karşı direnç oluşturmak	Yedekleme Politikası, Donanım/Platform Envanteri, Süreklilik Test Kayıtları
SITI	Sürekli İzleme ve Tehdit İstihbaratı	Anomali tespiti, olay izleme, bilgi paylaşımı	Tehditleri erken aşamada fark etmek ve proaktif savunma geliştirmek	İzleme Raporları, Tehdit Bültenleri, Log Kayıtları, SOME Protokolleri
BYG	Bakım, Yamalar ve Güncellemeler	Yama yönetimi, zafiyet tarama	Sistemleri güncel tutarak bilinen açıklara karşı koruma sağlamak	Yama Takip Listesi, Zafiyet Taraması Raporları, Güncelleme Planları
OADP	Olay ve Acil Durum Planları	Olay müdahale, kriz yönetimi, tatbikat	Saldırı sonrası toparlanmayı hızlandırmak ve koordinasyonu sağlamak	Olay Müdahale Planı, Tatbikat Raporları, İyileştirme Aksiyon Planları, İletişim Planı

Güvenli Mimari ve Segmentasyon (GMS), kurumsal siber dayanıklılık stratejisinde saldırı yüzeyini azaltma, sistemler arası izolasyonu sağlama ve ihlallerin yayılmasını sınırlama amacıyla kritik bir rol oynamaktadır. Bu strateji kapsamında, kurumun tüm ağ topolojisi ve bilgi sistemleri detaylandırılmakta; operasyonel, yönetimsel ve kullanıcı düzeyindeki ağlar arasındaki ilişkiler analiz edilerek segmentasyon ilkelerine dayalı bir ağ mimarisi oluşturulmaktadır. Bu yapı sayesinde, örneğin operasyonel teknolojilere bağlı endüstriyel kontrol sistemleri ile kurumsal ofis ağı birbirinden ayrılarak, bir ağda gerçekleşen güvenlik ihlalinin diğer ağ segmentine sıçraması önlenmektedir. Bu ayrım, özellikle enerji, sağlık ve üretim gibi sektörlerde güvenlik olaylarının etkisini lokalize etmek açısından hayati öneme sahiptir. Katmanlı savunma stratejileriyle birlikte geliştirilen bu mimari yapı, yalnızca erişimlerin sınırlandırılmasını değil, aynı zamanda güvenlik yapılandırmalarının merkezi biçimde yönetilmesini ve saldırılara karşı sistematik yanıt mekanizmalarının kurulmasını da sağlamaktadır. Segmentasyon,

saldırıların yatay hareket kabiliyetini azaltmakta, saldırganların sistemler arasında yayılmasını engelleyerek riskin etkili biçimde sınırlanmasına katkı sunmaktadır. Ayrıca bu yapı, saldırı sonrası hasar tespitinin hızlıca yapılmasını ve etkilenen varlıkların doğru biçimde tanımlanmasını kolaylaştırmakta; olay müdahale süreçlerinin başarısını doğrudan etkilemektedir. Bu stratejinin çıktı belgeleri arasında, ağ topolojisi haritaları, segmentasyon politikaları, sistemler arası erişim matrisleri ve güvenlik yapılandırma dokümantasyonu yer almaktadır. Bu belgeler hem sistem mimarisinin sürdürülebilirliğini hem de dış denetimlerde şeffaflık ve hesap verebilirliği desteklemektedir. Kurumlar bu yapı sayesinde, güvenlik ihlallerine karşı daha dayanıklı, izlenebilir ve yönetilebilir bir dijital altyapı inşa etmiş olmaktadır.

Yedeklilik ve Çeşitlilik (YYC), kurumların siber dayanıklılık kapasitesini artırmak için kritik altyapılarda uygulanması gereken temel stratejilerden biridir. Bu yaklaşım, hem sistemlerin saldırı veya arıza sonrası hızlı toparlanabilmesini hem de tekil zafiyet noktalarının sistem bütünlüğünü tehdit etmesini önlemeyi hedeflemektedir. Yedeklilik, bir sistem bileşeninin arızalanması durumunda aynı işlevi üstlenecek yedeğinin hazırda bulunmasını ifade eder. Örneğin, kurumsal veri sunucularının farklı coğrafi bölgelerde konumlandırılması veya bir telekomünikasyon sisteminde ana yönlendiricinin arızalanması durumunda yedek donanımın devreye alınması, hizmet sürekliliğini garanti altına almaktadır. Bu yapı, afet durumlarında olduğu kadar siber saldırılar sonrasında da operasyonların aksamadan sürdürülebilmesini sağlamaktadır. Çeşitlilik ise aynı işlevi gören sistemlerin veya bileşenlerin farklı üreticilerden, teknolojilerden ya da yazılımlardan seçilmesini içermektedir. Özellikle belirli marka veya yazılım sürümlerine yönelik siber saldırıların yaygınlaştığı günümüzde, tek bir ürün ya da tedarikçiye bağımlı kalmak kurumsal riskleri artırmaktadır. Bu nedenle çeşitlilik, sistemin tek bir zafiyetten tamamen etkilenmesini önleyerek arızaya karşı güvenli bir yapı oluşturmaktadır. Elektrik şebekelerinde alternatif güç kaynaklarının veya yük paylaşımı sağlayan sistemlerin devreye alınması, bu stratejinin fiziksel altyapı örnekleri arasında yer almaktadır. Yedeklilik ve çeşitlilik stratejisi uygulandığında, kurumsal yapının operasyonel süreklilik, toparlanabilirlik ve hizmet güvenliği alanlarındaki dayanıklılığı güçlenmektedir. Bu stratejinin çıktı belgeleri arasında; yedekleme politikaları, donanım/yazılım çeşitlilik envanteri, felaket kurtarma planları, toparlanma süreleri belgeleri ve test senaryoları yer almaktadır. Bu belgeler, sistemlerin kesintisiz ve güvenli şekilde işlemesini sağlarken, aynı zamanda olası zafiyetlerin etkisinin sınırlandırılmasını mümkün kılmaktadır. Kurumlar böylelikle tekil arızalardan etkilenmeyen, esnek ve toparlanabilir bir sistem mimarisi inşa etmiş olmaktadır.

Sürekli İzleme ve Tehdit İstihbaratı (SITI), kurumsal siber dayanıklılık stratejisinin tehditleri erken aşamada tespit etmeye ve savunma kapasitesini proaktif biçimde artırmaya yönelik bileşenidir. Kritik altyapıların korunmasında 7/24 çalışacak şekilde yapılandırılmış gerçek zamanlı izleme sistemlerinin kurulması temel bir gereklilik olarak öne çıkmaktadır. Bu sistemler; ağ trafiğini, kullanıcı davranışlarını, sistem erişimlerini ve işlem hacmini sürekli izleyerek potansiyel tehdit belirtilerini anında tespit edebilecek şekilde yapılandırılmaktadır. Özellikle anomali tespit sistemleri, endüstriyel kontrol sistemlerinin normal operasyonel davranışlarını öğrenmekte ve bu davranışlardan sapmaları alarm üretecek şekilde analiz etmektedir. İzleme faaliyetlerinin yalnızca kurum içi değil, aynı zamanda sektörel düzeyde tehdit istihbaratı paylaşımıyla desteklenmesi de büyük önem taşımaktadır. Enerji, sağlık, finans ve ulaşım gibi yüksek etki potansiyeline sahip sektörlerde ISAC (Information Sharing and Analysis Center) benzeri yapılar aracılığıyla edinilen istihbaratın paylaşılması, tüm sektörel savunma kapasitesini güçlendirmektedir. Ülkemizde de benzer şekilde, Siber Olaylara Müdahale Ekipleri (SOME) kurularak kurumların iç tehditlere karşı hızlı yanıt verebilmesi ve bilgi güvenliği olaylarını Ulusal Siber Olaylara Müdahale Merkezi (USOM) gibi otoritelere bildirmesi yasal bir yükümlülük haline getirilmiştir. Ayrıca 6698 sayılı Kişisel Verilerin Korunması Kanunu gibi düzenlemeler, ihlallerin raporlanmasını ve kayıt altına alınmasını da zorunlu kılmaktadır. Bu stratejinin çıktı belgeleri arasında; izleme politikaları, tehdit istihbarat raporları, alarm ve olay kayıtları, anlık bildirim protokolleri ve SOME görev tanımları yer almaktadır. Ayrıca penetrasyon testleri, log analizi ve olay korelasyonu çalışmaları bu stratejiyi destekleyen uygulamalardır. Sürekli izleme ve tehdit istihbaratının güçlü bir yapıya kavuşturulması, kurumların yalnızca gerçekleşen saldırılara yanıt vermesini değil, aynı zamanda gelişen tehditleri öngörmesini ve önleyici güvenlik mimarileri geliştirmesini de mümkün kılmaktadır. Bu yönüyle SITI, kurumsal siber dayanıklılığın en dinamik ve proaktif bileşenlerinden biridir.

Bakım, Yamalar ve Güncellemeler (BYG) stratejisi, kurumsal sistemlerin güncel tehditlere karşı korunmasını sağlayan en temel operasyonel dayanıklılık bileşenlerinden biridir. Kritik altyapılarda kullanılan yazılım ve donanımlar, zaman içinde güvenlik açıklarına maruz kalabilmekte ve bu açıkların giderilmesi için üreticiler tarafından düzenli olarak güvenlik yamaları ve sistem güncellemeleri yayımlanmaktadır. Ancak bu güncellemelerin uygulanması, birçok durumda kurumların operasyonel planlamasına ve kaynak yönetimine bağlı olduğundan, özellikle eski sistemlerde güncellemelerin ertelenmesi ya da atlanması sıkça karşılaşılan bir zafiyet oluşturmaktadır. Bu durum, sistemlerin saldırılara açık hale gelmesine neden olmakta ve saldırganlar tarafından hedeflenen ilk savunma noktalarından biri haline gelmektedir. Bu nedenle kurumsal düzeyde yapılandırılmış bir yama yönetimi politikası geliştirilmesi ve bu politikanın düzenli denetimlerle desteklenmesi kritik öneme sahiptir. Bu kapsamda, her bileşenin güncelleme döngüsü takip edilmeli, güncellenemeyen veya üretici desteği sona ermiş sistemler için alternatif güvenlik önlemleri uygulanmalıdır. Ayrıca sistemler üzerinde periyodik olarak gerçekleştirilecek zafiyet taramaları, mevcut açıkların önceden tespit edilerek sömürülmeden önce kapatılmasına imkan tanımaktadır. Bu proaktif yaklaşım, siber saldırılara karşı savunma reflekslerini güçlendirmekte ve saldırganların hareket kabiliyetini sınırlamaktadır. Bu stratejinin çıktı belgeleri arasında; yama yönetim prosedürü, güncelleme takvimi, zafiyet tarama raporları, risk azaltım planları ve donanım-yazılım envanter belgeleri yer almaktadır. Ayrıca dış bağımlılık içeren sistemler için üçüncü taraf üretici uyumluluk belgeleri de sürecin parçası olmalıdır. Etkin bir bakım ve güncelleme politikası uygulayan kurumlar, yalnızca saldırılara karşı daha dayanıklı olmakla kalmaz; aynı zamanda mevzuat uyumu, operasyonel sürdürülebilirlik ve sistem güvenilirliği açısından da önemli bir avantaj elde etmektedir. Bu nedenle BYG stratejisi hem önleyici hem de destekleyici nitelikleriyle kurumsal siber dayanıklılık modelinin vazgeçilmez bir bileşenidir.

Olay ve Acil Durum Planları (OADP), kurumsal siber dayanıklılık stratejisinin müdahale ve toparlanma yetkinliğini oluşturan kritik bileşenidir. Bu strateji kapsamında olası siber olaylara, altyapı kesintilerine veya kriz senaryolarına karşı önceden hazırlanmış müdahale planlarının oluşturulması, belgelenmesi ve düzenli aralıklarla test edilmesi gerekmektedir. Siber olayların etkileri hizmet kesintisi, veri kaybı veya fiziksel altyapıya zarar gibi sonuçlar doğurabilmekte ve çoğu zaman yangın, sel veya deprem gibi fiziksel afetlerle benzer düzeyde zararlara yol açabilmektedir. Bu nedenle, siber olaylara ilişkin müdahale planlarının kurumsal afet ve acil durum yönetim planlarıyla bütünleşmiş biçimde ele alınması gereklidir. Hazırlanan planların etkinliğinin sağlanması için, masaüstü senaryolar, teknik tatbikatlar ve simülasyonlar yoluyla düzenli testler gerçekleştirilmelidir. Örneğin bir fabrika tesisinde endüstriyel kontrol sistemine yönelik bir siber saldırı senaryosu kapsamında bilişim departmanı, operasyon ve iletişim birimlerinin katılımıyla yürütülen masaüstü tatbikatlar, gerçek zamanlı reaksiyon kabiliyetini artırmakta, birimler arası koordinasyonu test etmekte ve olay anında alınacak aksiyonların doğruluğunu değerlendirmeye olanak tanımaktadır. Bu uygulama, yalnızca sistemsel tepki süresini değil, aynı zamanda insan faktörü kaynaklı eksiklikleri ve iletişim zafiyetlerini de ortaya çıkarmaktadır. Tatbikatlar sonrası yapılan değerlendirmelerle planların yetersiz kalan yönleri güncellenmekte, bu sayede sürekli iyileştirme döngüsü işletilmektedir. OADP stratejisine ait çıktı belgeleri arasında; olay müdahale planları, acil durum iletişim protokolleri, tatbikat senaryo raporları, kritik karar alma akışları ve iyileştirme eylem planları yer almaktadır. Bu belgeler hem iç denetim süreçlerinde hem de dış paydaşlarla güven temelli iş birliği süreçlerinde kurumsal dayanıklılığın kanıtı olarak işlev görmektedir. Dolayısıyla, olay ve acil durum planları, yalnızca bir müdahale aracı değil; aynı zamanda siber dayanıklılığın sürekliliğini ve operasyonel güvenliğini garanti altına alan stratejik bir zorunluluktur.

5. SONUÇLAR / CONCLUSIONS

Siber güvenliğin yalnızca savunma odaklı önlemlerle sınırlandırılamayacağı günümüzde, dayanıklılık kavramı kurumların dijital varlıklarını sürdürülebilir biçimde koruyabilmesi için kritik bir gereklilik haline gelmiştir. Artan siber saldırı sıklığı, karmaşıklığı ve etkisi; bilgi sistemlerinin yalnızca korunmasını değil, aynı zamanda kesintilere karşı dayanıklı, esnek ve toparlanabilir biçimde yapılandırılmasını zorunlu kılmaktadır. Bu bağlamda siber dayanıklılık, klasik güvenlik yaklaşımlarının ötesine geçen bütüncül ve çok katmanlı bir güvenlik perspektifi sunmaktadır.

Çalışmada öncelikle, kurumsal dayanıklılığı artırmak amacıyla geliştirilen başlıca uluslararası çerçeveler detaylı biçimde ele alınmıştır. NIST Siber Güvenlik Çerçevesi, ENISA Siber Dayanıklılık Rehberleri, ISO/IEC 27001 standardı, COBIT ve ITIL gibi çerçeveler; organizasyonların tehditleri öngörebilmesi, güvenlik kontrollerini sistematikleştirmesi ve iyileştirme döngülerini sürdürebilmesi açısından yapılandırılmış birer rehber işlevi görmektedir. Bu yapılar arasında hedef, kapsam ve uygulama düzeyi açısından farklılıklar olsa da hepsi kurumsal kapasitenin artırılmasını hedeflemektedir.

Bu çerçevelerden elde edilen ilkelere dayanarak, siber saldırılara karşı dayanıklı sistemlerin sahip olması gereken evrensel özellikler ortaya konmuştur. Durumsal farkındalık, sağlamlık, toparlanabilirlik, otonom müdahale yeteneği, tehdit istihbaratı entegrasyonu ve insan-makine iş birliği gibi on temel özellik, dayanıklı sistemlerin yapı taşlarını oluşturmaktadır. Bu özellikler, yalnızca teknolojik altyapı değil aynı zamanda organizasyonel yapı, kurumsal kültür ve süreç yönetimiyle birlikte ele alınmalıdır.

Çalışmanın önemli katkılarından biri, özellikle sınırlı kaynaklara sahip küçük ve orta ölçekli kurumlar için uygulanabilir nitelikte yalın ve sistematik bir model olan kurumlar için yalın siber güvenlik dayanıklılık çerçevesinin geliştirilmiş olmasıdır. Bu çerçeve kurumsal altyapının en kritik bileşenlerinin belirlenmesinden başlayarak, güvenli mimari tasarımı, yedeklilik ve çeşitlilik, sürekli izleme ve tehdit istihbaratı, sistemlerin güncel tutulması ve olay müdahale planlarının yapılandırılması gibi altı temel stratejik adımdan oluşmaktadır. Her adım için hedeflenen amaçlar, odak alanları ve üretilecek çıktı belgeler tanımlanarak, kurumların kendi bağlamlarına uyarlanabilir bir yol haritası sunulmuştur. Bu yapı sayesinde, uluslararası standartlara tam uyum sağlayamayan kurumlar dahi siber dayanıklıklarını kurumsal düzeyde yapılandırabilecek kapsayıcı bir modelle desteklenmektedir. Böylelikle çalışma, yalnızca teorik bir katkı sunmakla kalmamış, aynı zamanda uygulamaya dönük somut bir öneri de geliştirmiştir.

Siber dayanıklılık alanı sürekli değişen tehdit ortamı ve teknolojik gelişmeler doğrultusunda dinamik biçimde evrilmektedir. Bu nedenle gelecekte yapılacak araştırmalar, yalnızca mevcut çerçevelerin etkinliğini değerlendirmekle sınırlı kalmamalı, aynı zamanda yeni nesil tehditlere karşı dayanıklılık kapasitesinin nasıl geliştirileceğine odaklanmalıdır. Öncelikle yapay zeka destekli saldırılara karşı otonom karar alma sistemlerinin güvenilirliği, etik sınırları ve müdahale kabiliyetleri daha ayrıntılı biçimde incelenmelidir. Aynı şekilde, durumsal farkındalık ve tehdit istihbarat sistemlerinin yapay öğrenme ve büyük veri analitiğiyle nasıl daha etkin entegre edilebileceği, araştırma gündeminin ön sıralarında yer almalıdır. Buna ek olarak çok sektörlü (enerji, sağlık, finans, üretim vb.) ve çok aktörlü (kamu, özel sektör, tedarikçiler, kullanıcılar) yapılar arasında dayanıklılık paylaşımı ve koordinasyonunu destekleyecek modellerin geliştirilmesi önem kazanmaktadır. Dayanıklılık olgunluk modellerinin sektörel adaptasyonu, küçük ve orta ölçekli işletmelere özel ölçeklenebilir çerçeve tasarımları ve kriz senaryolarına dayalı simülasyon çalışmalarının yaygınlaştırılması da gelecek araştırmaların odak noktaları arasında yer almalıdır. Son olarak siber dayanıklılığın sadece teknik değil yönetişim, yasal uyum, kullanıcı eğitimi ve kurumsal kültür gibi çok boyutlu yönleriyle de ele alınacağı disiplinlerarası çalışmaların artırılması gerekmektedir. Bu bağlamda, teorik modellerin saha verisiyle desteklenmesi ve uygulama örnekleriyle test edilmesi, siber dayanıklılık literatürüne önemli katkılar sağlayacaktır.

KAYNAKLAR / REFERENCES

Abdelkader, S., Amissah, J., Kinga, S., Mugerwa, G., Emmanuel, E., Mansour, D.-E. A., Bajaj, M., Blazek, V., & Prokop, L. (2024). Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks. *Results in Engineering*, *23*, 102647. https://doi.org/10.1016/j.rineng.2024.102647

AL-Hawamleh, A. M. (2024). Securing the Future: Framework Fundamentals for Cyber Resilience in Advancing Organizations. *Journal of System and Management Sciences*. https://doi.org/10.33168/JSMS.2024.1008

Ali, A., Khan, M. A., Farid, K., Akbar, S. S., Ilyas, A., Ghazal, T. M., & Al Hamadi, H. (2023). The Effect of Artificial Intelligence on Cybersecurity. *2023 International Conference on Business*

Analytics for Technology and Security (ICBATS), 1-7. https://doi.org/10.1109/ICBATS57792.2023.10111151

Araujo, M. S. de, Machado, B. A. S., & Passos, F. U. (2024). Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance. *Applied Sciences*, *14*(5), 2116. https://doi.org/10.3390/app14052116

Axelos. (2019). *ITIL 4: The Framework for the Management of IT-Enabled Services*.

Baran, G. (2024, Kasım). Starbucks Hit by Ransomware Attack Via Third-party Software Supplier. *Cyber Security News*.

Beretas, C. (2024). Information Systems Security, Detection and Recovery from Cyber Attacks. *Universal Library of Engineering Technology*, *01*(01), 27-40. https://doi.org/10.70315/uloap.ulete.2024.0101005

Daniel, L. (2024, Aralık). Data Breach—240,000 Credit Union Members Exposed. *Forbes*. https://www.forbes.com/sites/larsdaniel/2024/12/20/data-breach-240000-credit-union-members-exposed/

Dehghantanha, A., Yazdinejad, A., & Parizi, R. M. (2023). Autonomous Cybersecurity: Evolving Challenges, Emerging Opportunities, and Future Research Trajectories. *Proceedings of the Workshop on Autonomous Cybersecurity*, 1-10. https://doi.org/10.1145/3689933.3690832

Dobberstein, L. (2024, Kasım). Amazon confirms employee data exposed in leak linked to MOVEit vulnerability. *The Register*. https://www.theregister.com/2024/11/12/amazon_moveit_breach/

Dünya Gazetesi. (2024, Aralık). *Türkiye, PTT ve Anadolu Sigorta 'hack'leriyle sarsıldı: Siber saldırıların perde arkasında ne var?* https://www.dunya.com/gundem/turkiye-ptt-ve-anadolu-sigorta-hackleriyle-sarsildi-siber-saldirilarin-perde-arkasinda-ne-var-haberi-756506

ENISA. (2024). *Cyber Resilience Act Requirements Standards Mapping*.

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness – A systematic review of the literature. *Computers & Security*, *46*, 18-31. https://doi.org/10.1016/j.cose.2014.06.008

Hay Newman, L. (2025, Mart 11). *What Really Happened With the DDoS Attacks That Took Down X*. Wired. https://www.wired.com/story/x-ddos-attack-march-2025/

IBM. (2020). *What is cyber resilience?* https://www.ibm.com/think/topics/cyber-resilience

IBM. (2024). *Cost of a Data Breach Report 2024*. https://www.ibm.com/reports/data-breach

ISACA. (2019). *COBIT 2019 Framework: Introdcution and Methodology*.

Lehto, M. (2022). *Cyber-Attacks Against Critical Infrastructure* (ss. 3-42). https://doi.org/10.1007/978-3-030-91293-2_1

Lubis, M., Safitra, M. F., Fakhrurroja, H., & Muttaqin, A. N. (2025). Guarding Our Vital Systems: A Metric for Critical Infrastructure Cyber Resilience. *Sensors*, *25*(15), 4545. https://doi.org/10.3390/s25154545

Maglaras, L. (2022). From Mean Time to Failure to Mean Time to Attack/Compromise: Incorporating Reliability into Cybersecurity. *Computers*, *11*(11), 159. https://doi.org/10.3390/computers11110159

Meagher, H., & Dhirani, L. L. (2024). Cyber-Resilience, Principles, and Practices. Içinde *Cybersecurity Vigilance and Security Engineering of Internet of Everything* (ss. 57-74). https://doi.org/10.1007/978-3-031-45162-1_4

Möller, D. P. F. (2023). *Cybersecurity in Digital Transformation* (ss. 1-70). https://doi.org/10.1007/978-3-031-26845-8_1

Munusamy, T., & Khodadi, T. (2023). Building Cyber Resilience: Key Factors for Enhancing Organizational Cyber Security. *Journal of Informatics and Web Engineering*, *2*(2), 59-71. https://doi.org/10.33093/jiwe.2023.2.2.5

NIST. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. https://doi.org/10.6028/NIST.CSWP.29

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). *Developing cyber-resilient systems: A Systems Security Engineering Approach*. https://doi.org/10.6028/NIST.SP.800-160v2r1

Saeed, M. M., & Alsharidah, M. (2024). Security, privacy, and robustness for trustworthy AI systems: A review. *Computers and Electrical Engineering*, *119*, 109643. https://doi.org/10.1016/j.compeleceng.2024.109643

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. *Sensors*, *23*(16), 7273. https://doi.org/10.3390/s23167273

Shaked, A., Tabansky, L., & Reich, Y. (2021). Incorporating Systems Thinking Into a Cyber Resilience Maturity Model. *IEEE Engineering Management Review*, *49*(2), 110-115. https://doi.org/10.1109/EMR.2020.3046533

Troubitsyna, E. (2023). *Utilising Redundancy to Enhance Security of Safety-Critical Systems* (ss. 188-196). https://doi.org/10.1007/978-3-031-40953-0_16

Waqas, A. (2024, Ocak). Indian ISP Hathway Data Breach: Hacker Leaks 4 Million Users, KYC Data. *Hackread*. https://hackread.com/indian-isp-hathway-data-breach-user-data-kyc-leak/

Whitman, M. E., & Mattord, H. J. (2011). *Principles of Information Security* (7. bs). Course Technology Press.