Bölüm 8

Bankacılık Sektöründe Siber Güvenlik: Tehditler, Riskler ve Düzenleyici Yaklaşımlar

Zeyno Konca[1]

Özet

Finansal hizmetlerde dijital dönüşümün hız kazanması, bankacılık faaliyetlerinin kapsamını ve erişimini genişletirken siber risklere olan maruziyeti de önemli ölçüde artırmıştır. Dijital kanallar üzerinden yürütülen işlemlerin yaygınlaşması, siber riskleri teknik bir güvenlik sorununun ötesine taşıyarak finansal istikrarı ve kullanıcı güvenini etkileyebilen bir tehdit alanı hâline getirmiştir. Bu çalışmada siber risk, siber tehdit ve siber güvenlik kavramları finansal sistem perspektifinden ele alınmakta; özellikle bankacılık sektöründe karşılaşılan siber tehdit türleri ve bu tehditlerin doğurduğu riskler kavramsal bir çerçevede incelenmektedir. Çalışma, siber tehditlerin bankacılık sektöründe operasyonel süreklilik, veri bütünlüğü ve ödeme sistemleri üzerindeki etkilerini ortaya koymakta; siber güvenliğin finansal sistemin güvenilirliği açısından taşıdığı önemi tartışmaktadır. Ayrıca uluslararası kuruluşlar tarafından geliştirilen siber güvenlik ve siber dayanıklılık odaklı düzenleyici yaklaşımlar ile bu yaklaşımların Türkiye'de bankacılık sektörüne yönelik ulusal düzenlemelere yansımaları değerlendirilmektedir. Bulgular, siber güvenliğin yalnızca finansal kurumların düzenleyici uyum alanı olarak değil, dijital finansal hizmetleri kullanan bireyler ve işletmeler açısından doğrudan sonuçlar doğuran bir güven unsuru olarak ele alınması gerektiğini göstermektedir.

1. Giriş

Dijitalleşme, bankacılık sektöründe yalnızca hizmet sunum biçimlerini değil, riskin doğasını ve finansal istikrarın kırılganlık kanallarını da köklü biçimde dönüştürmektedir. Bu dönüşümle birlikte siber güvenlik, bankacılık sektörü açısından yalnızca teknik bir bilişim meselesi olmaktan çıkarak, bir yönetişim ve operasyonel dayanıklılık alanına dönüşmüştür.

1 Öğr. Gör. Dr., Sivas Cumhuriyet Üniversitesi, Zara Veysel Dursun UBYO. Finans ve Bankacılık Bölümü, zeynokonca@cumhuriyet.edu.tr, 0000-0003-2303-322X

https://doi.org/10.58830/ozgur.pub1070.c4229

Büyük veri analitiği ve yapay zekâ temelli dijital teknolojilerdeki hızlı gelişmelerle birlikte kullanımı giderek yaygınlaşan dijital bankacılık faaliyetleri, rekabet gücünü korumak ve müşteri hizmet etkinliğini artırmak isteyen bankaları kapsamlı bir dijital dönüşüm ve sürekli yenilik sürecine yöneltmektedir. Ödeme hizmetleri, fon transferleri, kredi süreçleri ve müşteri etkileşimleri giderek dijital kanallar, bulut bilişim altyapıları ve uygulama programlama arayüzleri (API) üzerinden yürütülmekte; bu durum bankacılık faaliyetlerinin hızını ve erişilebilirliğini artırmaktadır. Bununla birlikte dijital dönüşüm, bankacılık faaliyetlerinin saldırı yüzeyini genişleterek bankaları daha karmaşık siber risklere maruz bırakmakta; bilgi sistemlerine yönelik tehditler stratejik bir risk unsuru hâline gelmektedir (Gai vd., 2018).

Dijital dönüşüm, bankaların operasyonel verimliliğini artırarak fiziksel şubelere bağımlılığı azaltmakta ve gelişmiş veri analitiği sayesinde risklerin daha erken tespit edilmesine olanak tanımaktadır. Bununla birlikte bankaların iş modelleri ve örgütsel yapılarında ortaya çıkan bu dönüşüm, iç kontrol mekanizmaları ve kurumsal yönetişim açısından yeni belirsizlikleri de beraberinde getirmektedir. Bu durum uyum maliyetleri ve batık yatırımlar yoluyla risk maruziyetini artırabilmektedir. Dijital dönüşüm, bankacılık sektöründe riskleri eş zamanlı olarak sınırlayan ve yeniden üreten çift yönlü bir süreç olarak değerlendirilmektedir (Chen vd., 2023).

Bankacılıkta dijital dönüşüm, kredi öncesi, kredi süreci ve kredi sonrası aşamalarda otomasyon ve veri temelli karar mekanizmaları aracılığıyla risk yönetimi maliyetlerini önemli ölçüde azaltmakta; gelişmiş kredi değerlendirme sistemleri, erken uyarı mekanizmaları ve dijital tahsilat platformları sayesinde operasyonel verimliliği artırmaktadır. Bu gelişmeler, bankaların riskleri daha hassas biçimde ölçmesine ve daha dengeli bir risk alma yaklaşımı benimsemesine imkân tanırken, dijital teknolojilerin iş büyümesi ve süreç inovasyonu amacıyla kullanımı ticari bankaları diğer finansal sektörlere kıyasla daha yüksek ve çeşitlenen risklerle karşı karşıya bırakmaktadır. Nitekim literatür, bankacılıkta dijitalleşmenin risk alma davranışı üzerindeki etkisinin tek yönlü olmadığını; dijitalleşmenin bilanço içi faaliyetlerde riskleri azaltırken, servet yönetimi ürünleri ve diğer bilanço dışı işlemler yoluyla, özellikle fiyat rekabeti ve uzun vadeli ürünler üzerinden risk alma eğilimini artırabildiğini ortaya koymaktadır. Bu bulgular, bankaların dijital dönüşüm sürecinde yalnızca bilanço içi risklere değil, bilanço dışı risklerin izlenmesine de odaklanması gerektiğini; düzenleyici otoritelerin ise dijitalleşmeyle birlikte ortaya çıkan yeni risk türlerini kapsayan, daha güncel ve kapsamlı bir gözetim çerçevesi geliştirmesinin zorunlu olduğunu göstermektedir (Wang vd., 2024).

Siber güvenlik, dijital sistemlerin, ağların ve verilerin gizlilik, bütünlük ve erişilebilirliğini koruyan temel bir unsur olarak günümüz dijital dünyasında kritik bir konuma sahiptir. Toplumun teknolojilere olan yüksek bağımlılığı ve bulut bilişim, mobilite, e-ticaret ve çevrimiçi hizmetler gibi dijital teknolojilerin yaygın biçimde benimsenmesi, büyük hacimli hassas verilerin korunmasını zorunlu kılmakta ve güçlü siber güvenlik çözümlerine olan ihtiyacı artırmaktadır. Bununla birlikte siber güvenlik, yalnızca bireysel verilerin korunmasıyla sınırlı olmayıp, ulusal ekonomilerin güvenliği ve istikrarı ile de doğrudan ilişkilidir. Siber suçların giderek daha karmaşık hale gelmesi, bu tehditle ancak sistemler, kurumlar ve toplumlar arasındaki kolektif bir yaklaşımla mücadele edilebileceğini ortaya koymaktadır. Tanımlama, tespit etme ve iyileştirme süreçlerinin uyum içinde işlediği kapsamlı bir siber güvenlik mimarisinin tesis edilmesi son derece önemlidir (Mahato vd., 2024).

Bu çalışmanın amacı, bankacılık faaliyetleri çerçevesinde siber risklerin taşıdığı niteliği ortaya koymak ve siber güvenlik ile siber dayanıklılık kavramlarını ortak bir analitik çerçeve içinde değerlendirmektir. Bu kapsamda, bankacılık faaliyetlerinin dijitalleşmesiyle birlikte belirginleşen siber tehditler ele alınmakta; uluslararası standartlar ve ulusal uygulamalar doğrultusunda bankalar açısından etkili bir siber dayanıklılık yaklaşımının hangi unsurlar üzerine inşa edildiği incelenmektedir. Çalışma, teknik ayrıntılara odaklanan bir siber güvenlik rehberi sunmaktan ziyade, bankacılık faaliyetleri ve finansal istikrar perspektifinden kavramsal ve analitik bir değerlendirme ortaya koymayı hedeflemektedir.

2. Siber Risk Kavramı ve Finansal Etkileri

Siber risk, bilgi ve teknoloji varlıklarına yönelik operasyonel riskler olarak tanımlanmakta ve bu risklerin bilgi ile bilgi sistemlerinin gizliliği, bütünlüğü ve erişilebilirliği üzerinde sonuçlar doğurduğu kabul edilmektedir. Siber riskler yalnızca hedef alınan kurumu değil, aynı zamanda karşı tarafları ve üçüncü tarafları da etkileyebilmekte; çoğu durumda küçük ve bağımsız kayıplar şeklinde gerçekleşse de bazı senaryolarda düşük olasılıklı ancak yüksek etkili sistem kesintilerine yol açabilmektedir. Ayrıca siber riskler her zaman kötü niyetli saldırılardan kaynaklanmamakta; yazılım güncellemeleri, sistem arızaları veya doğal afetler gibi dışsal şoklar da iş sürekliliğini bozarak siber riskin gerçekleşmesine neden olabilmektedir. Bu tür kesintiler, sisteme karşı güvensizliği tetikleyerek kısa vadede bulaşıcı etkilere sebep olabilmekte ve finansal istikrar üzerinde olumsuz sonuçlar yaratabilmektedirler (Bouveret, 2018).

Siber risklerin ortaya çıkmasında teknik zafiyetler veya dış tehditlerin yanı sıra işletme içi yönetsel karar süreçleri de belirleyici olmaktadır. Chen vd. (2024), ABD'de faaliyet gösteren firmalar üzerinde yaptıkları kapsamlı çalışmada, yöneticilerin kısa vadeli finansal hedeflere odaklanmalarının siber güvenlik riskini anlamlı biçimde artırdığını ortaya koymaktadır. Çalışma bulguları, araştırma-geliştirme, yazılım, bakım ve çalışan eğitimi gibi takdire bağlı harcamalarda yapılan olağandışı kesintilerin, veri ihlali yaşanma olasılığını yükselttiğini göstermektedir. Anderson vd. (2012), siber suçların ekonomik etkisinin yalnızca doğrudan parasal kayıplarla sınırlı olmadığını; savunma harcamaları, işlem hacmindeki daralma ve güven kaybı gibi dolaylı unsurlar aracılığıyla finansal sistem üzerinde daha geniş ve kalıcı sonuçlar doğurduğunu ifade etmektedir.

Siber risklerin etkisinin en yoğun yaşandığı kurumlardan olan bankaların geleneksel şube merkezli faaliyet yapısının mobil ve internet bankacılığı odaklı bir modele evrilmesiyle birlikte suistimale açık yeni süreç ve hizmet alanları ortaya çıkmıştır. Bankacılık faaliyetleri hem müşteri güvenliği hem de kurumsal güvenlik açısından her geçen gün farklılaşan ve karmaşıklaşan risklerle karşı karşıya kalmaktadır. Bu yeni risk unsurlarının yarattığı kırılganlıklar, siber risk kavramı çerçevesinde ele alınmakta ve bilgi sistemleri ile teknolojik varlıkları etkileyen risklerin finansal ve itibari sonuçlarıyla birlikte değerlendirilmesini gerekli kılmaktadır. (Bouveret, 2018).

Bankacılık faaliyetleri çerçevesinde siber riskler, sistemlere izinsiz erişim yoluyla ya da meşru görünen bilgi parçalarının birleştirilmesi yoluyla ortaya çıkabilmektedir. Banka hesap numaraları tek başına doğrudan fon transferine imkân vermese de finansal kurum adı veya yönlendirme numarası gibi tamamlayıcı bilgilerle birlikte kullanıldığında, sahte ödeme talimatları oluşturma, yetkisiz otomatik transfer girişimleri ve sahte çek düzenleme gibi çok çeşitli dolandırıcılık faaliyetlerine zemin hazırlayabilmektedir. Bu durum, bankacılık faaliyetlerinde siber risklerin tekil bilgi ihlalinden ziyade bilgi kümelenmesi yoluyla arttığını göstermektedir (ITRC, 2025).

Siber riskin finansal sistem üzerinde yarattığı kırılganlıklar, bu riskin kaynağında yer alan tehdit türleri dikkate alınmadan tam olarak anlaşılmamaktadır. Bu nedenle siber riskin oluşumunda belirleyici rol oynayan siber tehditlerin yapısının ve yaygınlık düzeyinin incelenmesi önem arz etmektedir.

3. Bankacılık Sektörünün Maruz Kaldığı Siber Tehditler

Siber tehditler, bilgisayar ağları ve bilgi sistemlerine yönelik olarak verilerin yok edilmesi, bozulması veya yetkisiz biçimde ele geçirilmesini

amaçlayan kötü niyetli girişimler olarak tanımlanmakta; bu tehditler web siteleri, bilgisayar sistemleri ve çevrimiçi platformlar gibi farklı kaynaklardan ortaya çıkabilmektedir. Bu tehditlerin temel amacı, çevrimiçi kanallar aracılığıyla hassas bilgilerin izinsiz biçimde elde edilmesidir (Sekhar ve Kumar, 2023). Finansal kurumlar, müşteri kazanımı, işlem gerçekleştirme ve düzenleyici uyum gibi temel operasyonlarını giderek artan ölçüde dijital altyapılar üzerinden yürüttükçe, gelişmiş siber tehditlere karşı daha kırılgan hâle gelmektedir (Katuri, 2025).

Bilgi teknolojilerinin finansal sistem faaliyetlerinin merkezine yerleşmesi, bu sistemleri siber tehditlere karşı daha hassas bir yapıya dönüştürmüştür. OFR (2025) raporu, özellikle büyük ölçekli veri ihlalleri ve sistem kesintileri gibi siber olayların, finansal istikrar üzerinde hem operasyonel aksaklıklar hem de güven kaybı yoluyla belirgin etkiler yarattığını ortaya koymaktadır. Raporda, finansal sistemin kesintisiz işleyişinin doğrudan teknoloji altyapısının güvenilirliğine bağlı olduğu vurgulanmakta; geniş çaplı siber saldırılar veya teknik arızaların, yalnızca ilgili kurumun faaliyetlerini sekteye uğratmakla kalmayıp, ödeme sistemleri, fon transfer ağları ve piyasa işleyişi üzerinde zincirleme etkiler doğurabildiği belirtilmektedir. Bu sebeple finansal istikrarın korunması açısından siber risklerin yönetiminde teknik savunma önlemlerinin yanı sıra, saldırı sonrası süreçlerin hızla ve güvenli biçimde normale döndürülebilmesini ifade eden operasyonel dayanıklılığın da artırılması gerekmektedir (OFR,2025).

Finans sektörü dijital teknolojilerdeki hızlı gelişmelere paralel olarak çevrimiçi bankacılık uygulamaları, dijital ödeme sistemleri ve fintek tabanlı çözümlerin yaygınlaştığı kapsamlı bir dönüşüm yaşamaktadır. Bu dönüşüm, işlemlerin hızını ve hizmetlere erişimi artırırken; aynı zamanda finansal altyapıların gizlilik, bütünlük ve sürekliliğini hedef alan siber tehditlerin artmasına neden olmuştur. Avrupa Birliği Siber Güvenlik Ajansı (European Union Agency for Cybersecurity-ENISA), finans sektörünün yüksek hacimli finansal ve kişisel veri işlemesi nedeniyle siber saldırganlar açısından yüksek değerli hedef konumunda bulunduğunu ve bu nedenle söz konusu tehditlerin hem operasyonel riskler hem de finansal istikrar açısından önemli sonuçlar yaratabileceğini vurgulamaktadır. Kurum tarafından hazırlanan ve Avrupa finans sektörüne yönelik siber tehditlerin ele alındığı Threat Landscape: Finance Sector 2024 raporunda, finans sektörünü hedef alan başlıca tehditler aşağıdaki gibi sıralanmıştır:

1- Dağıtık Hizmet Engelleme (DDoS) Saldırıları: DDoS saldırıları, hedeflenen sistemin hizmet verme kapasitesini aşırı talep ile baskılayarak finansal hizmetlere erişimi kesintiye uğratmayı amaçlayan saldırı türleridir.

Bu saldırılar özellikle yoğun trafik oluşturarak sunucuların çökmesine veya yanıt veremez hâle gelmesine neden olur ve bankacılık işlemlerinin sürekliliğini riske sokar.

2-Veri ile İlişkili Tehditler: Veri ile ilişkili tehditler, hassas finansal ve kişisel veri varlıklarının açığa çıkmasına, ele geçirilmesine veya kötüye kullanılmasına yol açan olayları kapsar. Bu tehditler, siber suçlular tarafından finansal çıkarlar için istismar edilmekte ve bankaların müşteri güvenini zedeleme potansiyeli taşımaktadır.

3-Sosyal Mühendislik Saldırıları: Sosyal mühendislik tehditleri, kullanıcıları manipüle ederek gizli bilgilerin açıklanmasını veya yetkisiz işlem yapılmasını sağlamaya çalışan yöntemleri içerir.

4-Dolandırıcılık (Fraud): Dolandırıcılık temelli tehditler, siber saldırganların finansal kazanç elde etmek amacıyla kimlik veya banka bilgilerini kötüye kullanmalarını ifade eder.

5-Fidye Yazılımı (Ransomware): Fidye yazılımları, sistem veya verileri şifreleyerek erişimi engelleyen ve şifre çözümü için fidye talep eden kötü amaçlı yazılım saldırılarını kapsar.

6-Zararlı Yazılımlar (Malware): Malware, bankacılık sistemlerine ve kullanıcı cihazlarına zarar verebilen, bilgi çalabilen veya kontrolü ele geçirebilen kötü amaçlı yazılımları ifade eder.

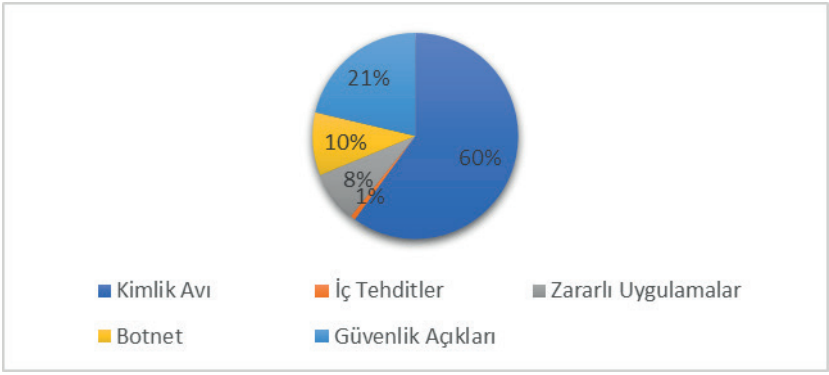
7-Tedarik Zinciri Saldırıları: Tedarik zinciri saldırıları, bankaların kritik hizmetlerini sağlayan üçüncü tarafların sistemlerine yöneliktir ve bu zafiyetlerin istismarı yoluyla daha geniş bankacılık altyapılarına erişim sağlanabilir.

8-Diğer Tehditler: Raporun kapsamına giren diğer tehditler, yukarıdaki kategorilere doğrudan uymayan ancak finansal sistemlere zarar verebilecek teknik ve taktikleri içermektedir (ENISA, 2024).

ENISA tarafından Temmuz 2024–Haziran 2025 döneminde gerçekleşen yaklaşık 4.900 seçilmiş ve doğrulanmış olaya dayanarak hazırlanan bir diğer raporda Avrupa Birliği genelinde siber tehdit ortamının giderek daha karmaşık, çok aktörlü ve politik bağlamdan etkilenen bir yapıya dönüştüğü görülmektedir. Rapora göre siber saldırılarda en sık kullanılan ve şekil 1'de yer alan ilk sızma yöntemi olan kimlik avı-oltalama (phishing), kötü amaçlı e-postalar (malspam), sesli dolandırıcılık (vishing) ve kötü amaçlı reklamlar (malvertising) dâhil olmak üzere vakaların yaklaşık %60'ını oluşturarak baskın ilk sızma vektörü olmuştur. Güvenlik açıklarının istismarı ise ilk erişim vektörlerinin %21,3'ünü oluşturmuş; bu vakaların %68'inde zararlı yazılım

(malware) kullanımı gerçekleşmiştir. Diğer yandan 2024 yılı içinde Avrupa Birliği'nin ağ ve bilgi sistemlerinin güvenliğini artırmaya yönelik temel siber güvenlik düzenlemesi olan NIS Direktifi kapsamında raporlanan yüksek etkili olayların %11'inin finans sektöründe gerçekleştiği belirtilmektedir. Bu bulgular, finansal altyapının siber olaylar açısından sistemik önem taşıyan bir alan olduğunu göstermektedir. Finans sektörü içinde ise saldırıların büyük ölçüde bankacılık alt sektöründe yoğunlaştığı, bankacılık sektörüne yönelik saldırıların finans sektöründeki toplam olayların %21,6'sını oluşturduğu raporlanmıştır (ENISA, 2025).

Şekil 1: Siber Saldırılarda En Sık Kullanılan İlk Sızma Yöntemleri



Kaynak: ENISA, (2025). *Threat landscape: Finance sector 2025*. Publications Office of the European Union.

Darem vd. (2023), bankacılık ve finans sektörünü hedef alan siber risklerin analizine yönelik olarak kapsamlı bir siber tehdit çerçevesi ortaya koymuştur. Bu çerçeve, siber tehditlerin finansal kurumlar üzerindeki etkisini, tehditlerin doğasını ve temel özelliklerini dikkate alarak yapılandırılmıştır. Çerçeve kapsamında siber tehditler, sınıflandırma ölçütlerine bağlı olarak teknik tehditler ve teknik olmayan tehditler olmak üzere iki ana grupta ele alınmaktadır. Bunun yanında, siber tehditlere karşı geliştirilen karşı önlemler çerçevenin tamamlayıcı bir bileşeni olarak tanımlanmakta; bu önlemler teknik kontrollerin yanı sıra hukuki ve düzenleyici düzenlemeler ile örgütsel ve yönetsel uygulamaları da kapsamaktadır.

Finans sektörü içinde siber tehditlerin en çok etkilediği alan olan bankacılık sektöründe siber güvenlik tehditleri hem teknik altyapıdan hem de kullanıcı etkileşimlerinden kaynaklanan riskleri içermektedir. Dijital bankacılıkta siber tehdit, hesap sahibinin bilgisi veya onayı olmaksızın

sistemlere erişmeyi hedefleyen her türlü kötü niyetli faaliyeti kapsamaktadır. Bu tehditlerin başında, verilerin şifrelenmeden saklanması veya iletilmesi gelmekte olup, açık biçimde bulunan veriler siber saldırganlar tarafından kolaylıkla ele geçirilebilmekte ve ciddi güvenlik ihlallerine yol açabilmektedir. Bunun yanı sıra, kullanıcı cihazları üzerinden gerçekleştirilen dijital işlemler sırasında bulaşabilen zararlı yazılımlar, ağ üzerinden aktarılan hassas bilgileri hedef alarak dijital bankacılık sistemlerinin bütünlüğünü tehdit etmektedir. Bankaların hizmet çeşitliliğini artırmak amacıyla yararlandığı üçüncü taraf hizmet sağlayıcılar, ATM şifresi, CVV veya tek kullanımlık şifre gibi bilgilerin paylaşımı yoluyla dolandırıcılık ve yetkisiz erişim risklerini artırmakta; sahtecilik (spoofing) ve kimlik avı saldırıları ise banka web sitelerini taklit eden platformlar ile e-posta, telefon ve kısa mesaj gibi iletişim kanalları üzerinden hassas finansal bilgilerin ele geçirilmesine olanak tanımaktadır. Mevcut bulgular, siber suçların önemli bir bölümünün ATM, banka kartı ve internet bankacılığı işlemleriyle ilişkili olduğunu gösterirken, büyük ölçekli bankalarda dahi izinsiz para transferlerinin gerçekleştiğine işaret etmektedir (Sekhar ve Kumar, 2023).

Siber saldırılarda kullanılan bir diğer yöntem de sıfır tıklama (zero-click) saldırıları olup, kullanıcıdan herhangi bir işlem gerektirmeden, uygulama ve işletim sistemi zafiyetlerinin istismarı yoluyla gerçekleştirilebilmesi nedeniyle bankacılık açısından niteliksel bir risk artışını temsil etmektedir. Bu tür saldırılar, mobil bankacılık uygulamalarının çalıştığı uç cihazların kullanıcı farkındalığına dayalı güvenlik varsayımlarını geçersiz kılabildiğini göstermektedir. Bu durum, bankacılıkta siber güvenliğin yalnızca kimlik doğrulama ve kullanıcı davranışına odaklanan bir çerçevede ele alınamayacağını; uç cihaz güvenliği, uygulama katmanı izolasyonu ve saldırı sonrası tespit kapasitesini içeren daha bütünleşik bir siber dayanıklılık yaklaşımını zorunlu kılmaktadır (Nisha ve Kulkarni, 2022).

Dijitalleşmenin hız kazanmasıyla birlikte siber saldırıların operasyonel süreklilik, veri bütünlüğü ve finansal istikrar üzerindeki potansiyel etkileri daha belirgin hâle gelmiş; bu durum koruyucu, önleyici ve iyileştirici mekanizmaların önemini artırmıştır. Siber tehditlerin çeşitlenmesi ve karmaşıklaşması, finansal kurumların bu tehditlerin etkilerini sınırlandırmaya yönelik sistematik yaklaşımlar geliştirilmesini de zorunlu kılmaktadır. Ortaya çıkan siber tehdit profili karşısında finansal kurumların siber güvenliği kurumsal düzeyde yapılandırılmış bir risk yönetimi yaklaşımıyla ele alması gerekmektedir.

4. Bankacılık Sektöründe Siber Güvenlik Yaklaşımları

Siber güvenlik, bilgisayar ve elektronik iletişim sistemleri ile bu sistemler üzerinden üretilen ve iletilen bilgilerin kullanılabilirlik, bütünlük, gizlilik, kimlik doğrulama ve inkâr edilemezlik ilkeleri doğrultusunda korunmasına, muhtemel zararların önlenmesine, sınırlandırılmasına ve giderilmesine yönelik tedbirler bütününü ifade etmektedir (NIST,2021).

Dijital kanalların kullanımının her geçen gün artmasından kaynaklı olarak siber güvenliğin kurumsal ve sistemik düzeyde taşıdığı önem, özellikle finansal kuruluşların maruz kaldığı siber olayların sıklığı ve yol açtığı ekonomik kayıplar üzerinden daha açık biçimde ortaya çıkmaktadır. Siber güvenlik olaylarının yaklaşık beşte biri finansal kuruluşlar tarafından raporlanmış ve önemli düzeyde doğrudan kayıplar bildirmiştir. Bu kayıplar 2004-2024 yılları arasında yaklaşık 12 milyar ABD düzeyine ulaşmıştır (IMF,2024). Kimlik Hırsızlığı Kaynak Merkezi (Identity Theft Resource Center -ITRC) tarafından yayımlanan 2025 yılı ilk yarı veri ihlali raporuna göre, söz konusu dönemde toplam 1.732 veri ihlali raporlanmış olup, bunların 387'si finansal hizmetler sektöründe gerçekleşmiştir. Bu bulgu, bankacılık ve finansal kurumların siber saldırılar açısından en yüksek risk altında bulunan sektörler arasında yer aldığını göstermektedir (ITRC, 2025).

Siber güvenlik ihlallerinin etkileri, yalnızca ihlale uğrayan firmayla sınırlı kalmayıp aynı sektördeki diğer kuruluşlara da yansıyabilmektedir. Islam ve arkadaşları (2022), bir firmada gerçekleşen siber ihlalin, rakip firmalar açısından yatırımcı belirsizliğini artırarak piyasa tepkilerine yol açabildiğini ve bu etkinin yönetsel yapılarla ilişkili olduğunu ortaya koymaktadır. Benzer şekilde, Kelton ve Yang (2024) yatırımcıların bu tür ihlalleri değerlendirirken davranışsal sezgilere başvurduğunu ve özellikle finansal olarak kırılgan firmalar için bulaşıcılık etkilerinin daha güçlü olduğunu göstermektedir.

Finansal sistemin etkin ve istikrarlı işleyişi bakımından önem arz eden siber güvenlik tehditlerinin yönetimi, Merkez Bankaları ve denetleyici otoritelerin gözetim ve düzenleme yetkileri kapsamında kilit bir sorumluluk alanı olarak öne çıkmaktadır. Bu otoritelerin rolü; tekil finansal kuruluşların güvenliği ve sağlamlığı ile finansal altyapıların ve finansal piyasaların gözetimini kapsamaktadır. Siber güvenliğin risk açısından artan önemi, finans sektöründeki kuruluşlar tarafından dijital teknolojilerin giderek daha fazla benimsenmesinin ve dijital altyapıların genişlemesiyle eş zamanlı olarak finansal ürün ve hizmetlerin dijitalleşmesinin bir yansımasıdır. Finans sektörünü hedef alan siber saldırıların sayısındaki ve karmaşıklığındaki artış, bu risklerin kritik niteliğini güçlü biçimde ortaya koymakta; özellikle siber uzayda meydana gelen tekil bir başarısızlığın zincirleme etkiler yaratarak

finansal istikrarı olumsuz etkileyebilmesi olasılığına, yani sistemik siber risk olaylarına odaklanılmasına yol açmaktadır (Forscey vd., 2022)

Günümüzde finans ve bankacılık hizmetlerinin ve bilgilerin büyük ölçüde bulut ortamında yer alması nedeniyle, kritik finansal verilerin yapay zekâ tabanlı, ölçeklenebilir ve esnek bir erişim kontrol sistemi ile korunması gerekmektedir. Finansal kuruluşlar, şifreleme, iki faktörlü kimlik doğrulama ve yetkilendirme gibi yerleşik güvenlik özelliklerine sahip sistemler kullanabilmektedir. Ancak tüketici ve kurum bilgilerini korumada erişim kontrolleri, altyapı ve fiziksel varlıklardan daha büyük bir öneme sahiptir. FinTech'in gelişimi ile Nesnelerin İnterneti (IoT), Büyük Veri, blokzincir, yapay zekâ ve makine öğrenmesi gibi diğer teknolojiler, bankacılık ve finansal hizmetler sektöründe eş zamanlı olarak gelişmektedir Modern bankacılığın en zorlayıcı sorunlardan biri, müşteri verilerinin güvenliğinin sağlanması olmuştur. Finans sektöründe siber saldırılar giderek daha ciddi bir hâl almaktadır. Siber güvenlik ve siber suç kavramları birbiriyle ilişkilidir. Sahip oldukları bilgilere nasıl erişildiğine ya da bu bilgilerin nasıl değiştirildiğine bağlı olarak bilgisayarlar hem hedef hem de araç rolü üstlenebilmektedir. Teknolojik gelişmeler bankacılık işlemlerinin kolaylığını büyük ölçüde artırmış olsa da, aynı zamanda çok sayıda yeni siber güvenlik sorunu da ortaya çıkmış ve bu sorunlar en üst seviyeye ulaşmıştır. Her ne kadar bu suçlarla mücadele etmek için çeşitli prosedürler uygulanıyor olsa da, tüm bilgi sistemlerinde hâlen çok sayıda zayıflık bulunmaktadır. Finansal kurumların, siber suçlarla mücadelede kullanılabilecek tahmin modelleri geliştirmesi gerekmektedir. Kötü niyetli faaliyetleri tespit edebilmek için sistemlerin sürekli, etkin şekilde izlenmesi, işletilmesi ve işlemlerin takip edilmesi zorunludur. Bu durum, ancak bilgi güvenliğini sağlamak amacıyla siber dayanıklılığa sahip gelişmiş teknolojilerin kullanılmasıyla mümkün olmaktadır (Khan vd.,2023).

Yapay zekâ, milyonlarca olayı kısa sürede analiz edebilmesi ve çok çeşitli siber tehditleri eş zamanlı olarak izleyebilmesi sayesinde, sürekli evrilen siber saldırılara karşı öngörüye dayalı analitik ve istihbarat üretme kapasitesine sahip bir teknoloji olarak öne çıkmaktadır. Bu özellikleri sayesinde, potansiyel tehditlerin gerçekleşmeden önce tespit edilmesine ve uygun karşı önlemlerin zamanında devreye alınmasına imkân tanımaktadır. Yapay zekâ, giderek siber güvenlik mimarisinin ayrılmaz bir bileşeni hâline gelmekte olup güvenlik süreçlerinin otomatikleştirilmesinde ve insan uzmanların karar alma süreçlerinin desteklenmesinde farklı kullanım alanlarında yaygın biçimde kullanılmaktadır. (Kaur vd.,2023)

Bankacılıkta siber güvenliğin artırılmasına yönelik kullanılan önemli araçlardan biri de biyometrik yöntemlerdir. Parmak izi taramaları ve yüz

tanıma gibi biyometrik yöntemler, kullanıcıların fiziksel özelliklerine dayalı olarak tanınmasını sağlayarak işlem yetkilendirme süreçlerinde kullanılmaktadır. Bazı bankalar, biyometrik doğrulamayı çok faktörlü kimlik doğrulama sistemleriyle birlikte uygulayarak güvenlik seviyesini yükseltmeyi hedeflemektedir. Bu teknolojiler, internet bankacılığı hizmetlerinde yetkisiz erişim ve siber suç risklerini azaltmaya yönelik bir güvenlik katmanı olarak değerlendirilmektedir (Khan vd, 2023).

Bankacılık sektöründe bilgi güvenliğinin sağlanmasının bir diğer önemli unsuru da siber güvenlik farkındalığıdır. Üst yönetimin açık desteği ve sahiplenmesi, yeterli bütçe tahsisi, belirlenen güvenlik politikalarına tutarlı biçimde uyum ve kurum genelinde benimsenmiş bir siber güvenlik kültürü, farkındalığın etkin biçimde yerleşmesini sağlayan başlıca unsurlardır. Çalışanların günlük operasyonlar sırasında aldıkları kararların bilgi güvenliği üzerindeki etkilerini yeterince gözetmemesi, kurumsal düzeyde net bir yönlendirme ve politika çerçevesi oluşturulmasını gerekli kılmaktadır. Bu çerçevede, kurum içinde geliştirilen güçlü bir siber güvenlik kültürü, bilgi sistemleri yönetiminin etkinliğini artırmakta ve insan kaynaklı güvenlik zafiyetlerinin azaltılmasına katkı sağlamaktadır (Al-Alawi ve Al Bassam, 2019).

Kullanıcılar açısından değerlendirildiğinde mobil bankacılık ortamında kullanılan modern güvenlik mekanizmalarının benimsenmesi, ağırlıklı olarak algılanan fayda, kullanım kolaylığı ve güven unsurları etrafında şekillenmektedir. Bu bağlamda biyometrik kimlik doğrulama yöntemleri, özellikle parmak izi tanıma gibi uygulamalar, pratiklik sağlamaları ve kullanıcı etkileşimini azaltmaları nedeniyle öne çıkmaktadır. Benzer şekilde, yapay zekâ tabanlı kısa mesaj uyarıları ve anlık bildirim sistemleri, gerçek zamanlı izleme ve hızlı müdahale imkânı sunmaları sayesinde mobil bankacılık güvenliğinde yaygın biçimde tercih edilen araçlar arasında yer almaktadır. Buna karşılık, teorik olarak yüksek güvenlik seviyesi sunmasına rağmen çok faktörlü kimlik doğrulama (MFA) uygulamalarının kullanımının sınırlı kaldığı; bu durumun büyük ölçüde farkındalık eksikliği ve uygulamaya ilişkin bilgi yetersizliğinden kaynaklandığı görülmektedir. Güçlü parola politikaları güvenlik açısından gerekli kabul edilmekle birlikte, parolaların hatırlanmasındaki güçlükler ve yazılı olarak saklanma eğilimi, bu yöntemin kendi içinde yeni güvenlik zafiyetleri üretebildiğini göstermektedir. Genel olarak değerlendirildiğinde, güvenlik araçlarının teknik varlığından ziyade bu araçların nasıl çalıştığına ve nasıl uygulanması gerektiğine ilişkin bilginin, benimseme düzeyi üzerinde belirleyici olduğu anlaşılmaktadır (Riasat vd., 2025).

5. Siber Güvenlikle İlgili Düzenleyici Çerçeve

Siber güvenlik stratejilerinin tanımlanması konusunda son yıllarda belirli ilerlemeler kaydedilmiş olmakla birlikte, bu alanda önemli yapısal boşluklar varlığını sürdürmektedir. Ulusal düzeyde ve finans sektörüne odaklanan siber güvenlik stratejileri giderek daha fazla önem kazanmış ve birçok yargı alanı bu tür stratejiler geliştirmiştir. Artan siber güvenlik riskleriyle etkin biçimde başa çıkabilmek için düzenleyici ve denetleyici kapasitenin güçlendirilmesi acil bir önceliktir. Bu kapsamda, belirlenen boşluklara dayalı hedefli ve risk temelli bir yaklaşımın benimsenmesi, daha etkili sonuçlar sağlayacaktır. Bununla birlikte, insan kaynağı, teknik altyapı ve finansal imkânlara ilişkin kaynak kısıtlarının, siber risklere yönelik kapsamlı bir denetim çerçevesinin oluşturulmasında optimal olmayan ilerlemeye yol açtığı değerlendirilmektedir. Ayrıca, kötü niyetli aktörlerin siber saldırılar gerçekleştirmek üzere giderek daha etkin biçimde iş birliği yaptığı bir ortamda, denetleyici otoritelerin yalnızca kendi iç kapasitelerini artırmaları yeterli değildir. Finansal istikrarın korunabilmesi için denetleyici kurumların diğer düzenleyici otoriteler ve ilgili kamu kuruluşlarıyla koordinasyonlarını güçlendirmeleri kritik önem taşımaktadır. Siber risk denetiminin etkinliğinin artırılabilmesi amacıyla, yerinde inceleme yapma kapasitesinin geliştirilmesi, uzaktan denetimin mevcut seviyelerin ötesine taşınarak yoğunlaştırılması ve denetim kapsamının kritik üçüncü tarafları da içerecek biçimde genişletilmesi gerekmektedir (Ravikumar, 2025).

Tablo 1. Finansal Sistemde Siber Düzenlemelerin Uluslararası Uyumunu Kolaylaştıran Çalışmalar

Kaynak: Crisanto, J. C., Umebara Pelegrini, J. ve Prenio, J. (2023). Banks' cyber security: A second generation of regulatory approaches (FSI Insights on policy implementation No. 50). Financial Stability Institute.

Finansal sistemde siber güvenliğe ilişkin uluslararası standartlar, ilke setleri ve düzenleyici çalışmaların sayısı ve kapsamı belirgin biçimde artmıştır. Tablo 1, Finansal İstikrar Kurulu'nun (FSB) bankacılık sektöründe siber güvenliğe yönelik ikinci nesil düzenleyici yaklaşım çerçevesinde geliştirdiği ve finansal sistemde siber düzenlemelerin uluslararası uyumunu kolaylaştırmayı amaçlayan temel çalışma alanlarını göstermektedir. Çerçeve; sistemik siber dayanıklılık yaklaşımları, operasyonel dayanıklılık ilkeleri, üçüncü taraf ve dış kaynak kullanımına bağlı siber risk yönetimi, siber olay yönetimi ve raporlama mekanizmaları, ortak siber terminolojinin oluşturulması ve siber önlemlerin etkinliğinin test edilmesi gibi birbirini tamamlayan bileşenlerden oluşmaktadır. Bu bileşenler, CPMI-IOSCO, G7, BCBS ve FSB tarafından yayımlanan rehberler ve ilkeler doğrultusunda şekillendirilmiş olup, finansal kuruluşların siber riskleri tutarlı, karşılaştırılabilir bir şekilde değerlendirmesine olanak sağlamaktadır (Crisanto vd., 2023).

Geleneksel siber güvenlik yaklaşımları, büyük ölçüde saldırıların önlenmesine odaklanmış ve bilgi sistemlerinin dış tehditlere karşı korunmasını temel amaç olarak benimsemiştir. Ancak günümüz tehdit ortamında, gelişmiş ve kalıcı siber saldırıların tamamen önlenmesinin mümkün olmadığı giderek daha fazla kabul görmektedir. Bu bağlamda, literatürde ve düzenleyici çerçevelerde "siber dayanıklılık" kavramı ön plana çıkmıştır. Siber dayanıklılık, bankaların siber olayları yalnızca önleme kapasitesini değil, aynı zamanda bu olayları erken tespit etme, etkilerini sınırlama ve kritik bankacılık faaliyetlerini mümkün olan en kısa sürede yeniden sürdürebilme yetkinliğini ifade etmektedir (Kopp vd., 2017).

Bank for International Settlements (BIS) ve International Organization of Securities Commissions (IOSCO) tarafından hazırlanan rehber finansal piyasa altyapılarının siber dayanıklılıklarını güçlendirmelerine yönelik olarak yönetişim, tanımlama, koruma, tespit ile müdahale ve toparlanma gibi beş temel risk yönetimi kategorisi ve siber dayanıklılık çerçevesinin tamamına yayılması gereken üç üst düzey bileşen (test etme, durumsal farkındalık ve öğrenme-evrilme) sunmaktadır (Tablo 2). Rehberde ayrıca dayanıklılık hedeflerine ulaşabilmek için bu yatırım alanlarının birlikte ele alınması, etkili olabilmesi ve beklenen sonuçları üretebilmesi için ise bu faaliyetleri destekleyen kullanıcı farkındalığı eğitimleri gibi tamamlayıcı varlıklara yatırım yapılması da özellikle tavsiye edilmektedir (Committee on Payments and Market Infrastructures (CPMI) & International Organization of Securities Commissions (IOSCO), 2016).

Tablo 2. Finansal Piyasa Altyapıları için Siber Dayanıklılık Çerçevesi

Bileşen	Açıklama
Yönetişim	Siber risk yönetimine ilişkin stratejik yaklaşımın ve rol–sorumlulukların yönetim kurulu ve üst yönetim düzeyinde tanımlanması
Tanımlama	Kritik işlevlerin, bilgi varlıklarının, sistemlerin ve dış bağımlılıkların belirlenmesi ve önceliklendirilmesi
Koruma	Bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğini sağlamak üzere uygun güvenlik kontrollerinin uygulanması
Tespit	Olası siber olaylara işaret eden anormal faaliyetlerin zamanında izlenmesi ve belirlenmesi
Müdahale ve Toparlanma	Siber olayların etkisinin sınırlandırılması ve kritik operasyonların güvenli biçimde yeniden başlatılması
Test Etme	Siber dayanıklılık çerçevesinin etkinliğinin düzenli testler yoluyla değerlendirilmesi
Durumsal Farkındalık	Tehdit ortamının izlenmesi, tehdit istihbaratının kullanılması ve paydaşlarla bilgi paylaşımı
Öğrenme ve Evrilme	Değişen siber risklere uyum sağlayacak şekilde sürekli iyileştirme ve kurumsal öğrenmenin teşvik edilmesi

Kaynak: CPMI & IOSCO, 2016, Guidance on cyber resilience for financial market infrastructures. BIS & IOSCO.

Uluslararası kuruluşlar tarafından geliştirilen bu ilke ve çerçeveler, siber güvenliğe ilişkin küresel bir referans noktası oluşturmakla birlikte, her ülkenin kendi finansal yapısı ve düzenleyici öncelikleri doğrultusunda ulusal mevzuata yansıtılmaktadır. Türkiye'de bankacılık sektörüne yönelik siber güvenlik ve bilgi sistemleri düzenlemeleri, Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) tarafından belirlenen mevzuat çerçevesinde şekillenmektedir. BDDK düzenlemeleri uyarınca bankalar, bilgi sistemlerinin güvenliğini sağlamak, bilgi varlıklarını yetkisiz erişim, bozulma, kayıp ve kesintilere karşı korumakla yükümlüdür. Bu kapsamda bankaların; bilgi sistemleri risklerini tanımlayan, ölçen, izleyen ve kontrol altına alan yazılı politika ve prosedürler oluşturması, bu süreçleri iç kontrol ve risk yönetimi sistemlerine entegre etmesi zorunlu tutulmaktadır. Düzenlemelerde, bankacılık faaliyetlerinde kullanılan bilgi sistemlerinin gizlilik, bütünlük ve erişilebilirlik ilkeleri doğrultusunda işletilmesi gerektiği açıkça belirtilmekte; müşteri bilgilerinin ve bankacılık sırlarının korunması temel yükümlülükler arasında sayılmaktadır. Ayrıca bilgi sistemlerine ilişkin risklerin düzenli olarak değerlendirilmesi ve bu değerlendirmelerin yönetim kurulu düzeyinde izlenmesi mevzuat kapsamında öngörülmektedir.

BDDK mevzuatı, bankaların bilgi sistemleri kaynaklı kesintilere ve siber olaylara karşı iş sürekliliği ve felaket kurtarma planları hazırlamasını ve bu planları düzenli olarak test etmesini zorunlu kılmaktadır. Bankaların, bilgi sistemlerinde meydana gelen önemli olayları kayıt altına alması, olaylara müdahale süreçlerini tanımlaması ve gerekli hâllerde düzenleyici otoriteyi bilgilendirmesi gerekmektedir. Ayrıca dış hizmet alımı yoluyla kullanılan bilgi sistemleri ve hizmet sağlayıcılar da bankanın risk alanı içinde değerlendirilmekte; bu hizmetlerin güvenliği, sürekliliği ve denetlenebilirliği bankanın sorumluluğunda kabul edilmektedir. Düzenlemeler, bilgi sistemleri ve siber risk alanında iç denetim faaliyetlerinin yürütülmesini, kontrol eksikliklerinin raporlanmasını ve giderilmesini zorunlu kılarak bankacılık sektöründe operasyonel ve dijital dayanıklılığın tesis edilmesini hedeflemektedir (BDDK,2020).

Bankacılık sektöründe siber dayanıklılığın yalnızca teknik kontrollerle sağlanamayacağı, düzenleyici çerçevelerde de açık biçimde ortaya konmaktadır. BDDK tarafından yayımlanan Bilgi Sistemlerine İlişkin Sızma Testleri dokümanı, bankaların bilgi sistemlerine yönelik zafiyetleri periyodik ve senaryoya dayalı testlerle tespit etmesini zorunlu kılmakta; sızma testlerini teknik bir faaliyet olmanın ötesinde, risk yönetimi ve üst yönetim gözetimi altında yürütülmesi gereken kurumsal bir süreç olarak tanımlamaktadır. Bu yaklaşım, siber risklerin önlenebilir olduğu kadar kaçınılmaz da olabileceği varsayımına dayanmakta ve bankaların siber olaylar karşısında yalnızca korunma değil, hazırlık ve toparlanma kapasitelerini de test etmelerini amaçlamaktadır (BDDK,2012).

01.04.2021 tarihli Resmî Gazete'de yayımlanan Uzaktan Kimlik Tespiti Yönetmeliği, bankacılık işlemlerinde siber risklerin daha işlem öncesi aşamada sınırlandırılmasını hedeflemektedir. Yönetmelik, uzaktan müşteri edinimi süreçlerinde kimlik tespitinin gerçek zamanlı görüntülü görüşme yoluyla yapılmasını, müşterinin fiziksel varlığının ve kimlik belgesinin orijinalliğinin doğrulanmasını zorunlu kılmaktadır. Ayrıca, kimlik tespiti sürecinin sesli ve görüntülü olarak kayıt altına alınması ve bu kayıtların denetlenebilir şekilde saklanması öngörülerek, olası uyuşmazlıklar ve siber dolandırıcılık vakaları karşısında izlenebilirlik ve inkâr edilemezlik güçlendirilmiştir. Kimlik doğrulama ile elektronik ortamda kurulan sözleşme arasında teknik bağın korunmasına ilişkin hükümler ise, kimlik hırsızlığı ve yetkisiz işlem başlatma risklerine karşı düzenleyici bir güvenlik katmanı oluşturmaktadır (BDDK, 2021).

BDDK'nın 2023/1 sayılı genelgesi ise elektronik bankacılık kanallarında kimlik doğrulama ve işlem güvenliğini, Bankaların Bilgi Sistemleri

ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik (BSEBY) hükümleri çerçevesinde ele almakta ve bankaların, internet ve mobil bankacılık işlemlerinde en az iki bileşenden oluşan güçlü kimlik doğrulama mekanizmaları kullanmasını zorunlu kılmaktadır. Düzenlemede, finansal sonuç doğuran işlemler için müşteri onayının gösterilen tutar ve alıcı bilgilerine özgü biçimde alınması, bu onayın teknik olarak doğrulanabilir ve inkâr edilemez şekilde kayıt altına alınması gerektiği vurgulanmakta; böylece işlem güvenliği ile sorumluluk atamasının sağlanması amaçlanmaktadır. Ayrıca, elektronik ortamda sözleşme kurulması ve servis modeli bankacılığı kapsamında arayüz sağlayıcılar üzerinden sunulan hizmetlerde, kimlik tespiti ve işlem güvenliğine ilişkin yükümlülüklerin servis bankası ve arayüz sağlayıcı tarafından birlikte yerine getirilmesi gerektiği düzenlenmektedir. Genelge, bankacılık faaliyetlerinde siber güvenliğin hukuki sorumluluk, müşteri onayı ve kurumsal yönetişim boyutları da olan bir risk alanı olduğunu ortaya koymaktadır (BDDK, 2023).

6. Sonuç

Finansal sistemde dijital kanal kullanımının hızla yaygınlaşması, siber riskleri bankacılık ve finansal kurumlar açısından yalnızca operasyonel bir tehdit olmanın yanı sıra finansal istikrarı etkileyebilecek sistemik bir risk unsuru hâline getirmiştir. Son yıllarda yaşanan büyük ölçekli siber olaylar ve siber saldırılar ödeme sistemleri, veri bütünlüğü, operasyonel süreklilik ve piyasa güveni üzerinde geniş çaplı etkiler yaratmaktadır. Bu sebeple siber güvenliğin finansal sistemin dayanıklılığı açısından stratejik bir öncelik olarak ele alınması bir zorunluluk haline gelmiştir.

Uluslararası kuruluşlar tarafından geliştirilen rehberler ve ilke setleri, siber risklerin yönetiminde ortak bir referans çerçevesi sunmakla birlikte, giderek daha fazla ikinci nesil düzenleyici yaklaşımlara yönelindiği görülmektedir. Bu yaklaşımlar, teknik kontrollere ek olarak sistemik siber dayanıklılık, üçüncü taraf risk yönetimi, siber olaylara hazırlık ve raporlama mekanizmaları ile test ve değerlendirme süreçlerini bir arada ele almaktadır. Siber güvenlik günümüz koşullarında artık kurumsal yönetişim ve risk yönetimi süreçlerinin ayrılmaz bir parçası hâline gelmektedir.

Küresel eğilimler, ulusal düzeyde düzenleyici çerçevelerin şekillendirilmesinde de belirleyici olmaktadır. Türkiye'de bankacılık sektörüne yönelik siber güvenlik düzenlemeleri, BDDK tarafından yayımlanan mevzuat ve rehberler aracılığıyla uluslararası standartlarla uyumlu biçimde yapılandırılmıştır. Bu düzenlemeler, bankaların bilgi sistemleri güvenliğini güçlendirmeyi, siber olaylara karşı hazırlık düzeyini artırmayı ve denetim

süreçleri yoluyla risklerin süreklilik arz eden bir biçimde izlenmesini amaçlamaktadır. Bu yönüyle ulusal mevzuat, küresel siber dayanıklılık yaklaşımının yerel finansal sistemin ihtiyaçlarına uyarlanmış bir yansıması niteliğindedir.

Artan dijitalleşme ve karmaşıklaşan siber tehdit ortamı, siber güvenliği yalnızca finansal kurumlar açısından değil, aynı zamanda bu kurumların sunduğu dijital hizmetleri kullanan bireysel ve kurumsal kullanıcılar açısından da hassas bir güven unsuru hâline getirmiştir. Siber olaylar; finansal kurumlarda operasyonel aksamalar ve ekonomik kayıplar yaratmanın yanı sıra, kullanıcılar bakımından maddi zararlar, kişisel verilerin ihlali, kimlik hırsızlığı ve dijital hizmetlere duyulan güvenin zedelenmesi gibi çok boyutlu sonuçlar doğurmaktadır.

Sonuç olarak, artan dijitalleşme ve karmaşıklaşan tehdit ortamı karşısında siber güvenliğin, bankalar için dinamik ve sürekli gelişen bir risk yönetimi süreci olarak ele alınması gerekmektedir. Önümüzdeki dönemde siber risklerin etkin biçimde yönetilebilmesi; uluslararası standartlarla uyumlu, ulusal mevzuatla desteklenen ve kurumsal yönetişim yapılarıyla bütünleşmiş bir siber dayanıklılık yaklaşımının benimsenmesine bağlıdır. Bunun yanı sıra kullanıcıların dijital ortamlarda karşılaşabilecekleri riskleri tanıyabilmesi, güvenli finansal davranışlar geliştirebilmesi ve sunulan koruma mekanizmalarını doğru biçimde kullanabilmesi de önemli bir husustur. Dolayısıyla siber güvenlik politikalarına kurumsal siber dayanıklılık uygulamaları ile kullanıcıların dijital finansal okuryazarlığını güçlendirmeye yönelik farkındalık ve eğitim süreçlerinin de dahil edilmesi siber risk kaynaklı zararların azaltılmasında etkili olacaktır.

Kaynakça

Al-Alawi, A. I., & Al-Bassam, S. A. (2021). Assessing the factors of cybersecurity awareness in the banking sector. *Arabian Gulf Journal of Scientific Research, 39*(1), 18–30.

Bankacılık Düzenleme ve Denetleme Kurumu. (2012). *Bilgi sistemlerine ilişkin sızma testleri* (Sayı: B.02.1.BDK.0.77.00.00/010.06.02-1). https://www.bddk.org.tr/Mevzuat/DokumanGetir/915

Bankacılık Düzenleme ve Denetleme Kurumu. (2020). *Bankaların bilgi sistemleri ve elektronik bankacılık hizmetleri hakkında yönetmelik*. Resmî Gazete (Sayı: 31069, 15 Mart 2020).

Bankacılık Düzenleme ve Denetleme Kurumu. (2021). *Bankalarca kullanılacak uzaktan kimlik tespiti yöntemlerine ve elektronik ortamda sözleşme ilişkisinin kurulmasına ilişkin yönetmelik*. Resmî Gazete (Sayı: 31441). https://www.resmigazete.gov.tr/eskiler/2021/04/20210401-7.htm

Bankacılık Düzenleme ve Denetleme Kurumu. (2023). *Elektronik bankacılık hizmetlerinde ve elektronik ortamda sözleşme ilişkisinin kurulmasında kimlik doğrulama ve işlem güvenliği için sağlanması gereken kriterler hakkında genelge* (2023/1).

Chandra Sekhar, S., & Kumar, M. (2023). An overview of cybersecurity in the digital banking sector. *East Asian Journal of Multidisciplinary Research, 2*(1), 43–52.

Chen, W., Li, X., Wu, H., & Zhang, L. (2024). The impact of managerial myopia on cybersecurity: Evidence from data breaches. *Journal of Banking & Finance, 166*, 107254. https://doi.org/10.1016/j.jbankfin.2024.107254

Chen, Z., Li, H., Wang, T., & Wu, J. (2023). How digital transformation affects bank risk: Evidence from listed Chinese banks. *Finance Research Letters, 58*, 104319. https://doi.org/10.1016/j.frl.2023.104319

Crisanto, J. C., Umebara Pelegrini, J., & Prenio, J. (2023). *Banks' cybersecurity: A second generation of regulatory approaches* (FSI Insights on Policy Implementation No. 50). Financial Stability Institute. https://www.bis.org

Darem, A. A., Alhashmi, A. A., Alkhaldi, T. M., Alashjaee, A. M., Alanazi, S. M., & Ebad, S. A. (2023). Cyber threats classifications and countermeasures in banking and financial sector. *IEEE Access, 11*, 125138–125158. https://doi.org/10.1109/ACCESS.2023.3327016

European Union Agency for Cybersecurity. (2024). *ENISA threat landscape: Finance sector 2024*. ENISA. https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf

European Union Agency for Cybersecurity. (2025). *ENISA threat landscape 2025*. Publications Office of the European Union.

Forscey, D., Bateman, J., Beecroft, N., & Woods, B. (2022). *Systemic cyber risk: A primer*. Carnegie Endowment for International Peace & The Aspen Institute.

Identity Theft Resource Center. (2025, May 11). *What can a scammer do with your banking information?* https://www.idtheftcenter.org

Identity Theft Resource Center. (2025, November 28). *How to protect your bank account from attacks*. https://www.idtheftcenter.org/post/how-to-protect-your-bank-account-from-attacks/

International Monetary Fund. (2024). *Global financial stability report: The last mile—Financial vulnerabilities and risks* (Chapter 3: Cyber risk: A growing concern for macrofinancial stability). IMF.

Islam, M. S., Wang, T., Farah, N., & Stafford, T. (2022). The spillover effect of focal firms' cybersecurity breaches on rivals and the role of the CIO. *Journal of Accounting and Public Policy, 41*, 106916. https://doi.org/10.1016/j.jaccpubpol.2022.106916

Katuri, S. (2025). Cybersecurity threats in digital banking: A comprehensive analysis. *International Journal on Science and Technology, 16*(1), 1–16.

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion, 97*, 101804. https://doi.org/10.1016/j.inffus.2023.101804

Kelton, A. S., & Yang, Y.-W. (2024). Understanding cybersecurity breach contagion effects. *International Journal of Accounting Information Systems, 55*, 100714. https://doi.org/10.1016/j.accinf.2024.100714

Khan, H. U., Malik, M. Z., Nazir, S., & Khan, F. (2023). Utilizing biometric systems for enhancing cybersecurity in the banking sector. *IEEE Access, 11*, 80181–80202. https://doi.org/10.1109/ACCESS.2023.3298824

Mahato, S., Sah, R., & Sapkota, S. (2024). Cybersecurity challenges and threats. *International Journal of Advanced Research in Science, Communication and Technology, 4*(5), 651–660. https://doi.org/10.48175/IJARSCT-22497

Nisha, T. N., & Kulkarni, M. S. (2022). Zero-click attacks: A new cyber threat for the e-banking sector. *Journal of Financial Crime, 30*(4). https://doi.org/10.1108/JFC-06-2022-0140

Office of Financial Research. (2025). *2025 annual report to Congress*. U.S. Department of the Treasury. https://www.financialresearch.gov/annual-reports/files/OFR-AR-2025.pdf

Ravikumar, R. (2025). *Strengthening cybersecurity: Lessons from the cybersecurity survey* (IMF Technical Notes and Manuals No. 2025/06). International Monetary Fund.

Riasat, I., Shah, M., & Gonul, M. S. (2025). Strengthening cybersecurity resilience. *Computers, 14*(4), 129. https://doi.org/10.3390/computers14040129

Wang, Q., & Ngai, E. W. T. (2022). Firm diversity and data breach risk. *Journal of Strategic Information Systems, 31*(4), 101743. https://doi.org/10.1016/j.jsis.2022.101743