Bankacılığın Yeni Sınavı: SİBER GÜVENLİK

Milyonlarca kişinin kullandığı dijital bankacılık hizmetleri, siber suç örgütlerinin en cazip hedeflerinden biri haline geldi. Kimlik avından fidye yazılımlarına uzanan tehditler, finans dünyasında yeni bir güvenlik anlayışını zorunlu kılıyor.

Esra ERİK AKYOL
Dr. Öğr. Üyesi, İstanbul Kültür Üniversitesi, Meslek Yüksekokulu, Bankacılık ve Sigortacılık Programı, e.akyol@iku.edu.tr, ORCID: 0009-0001-5529-518X

Bankalar, finansal sistemin merkezinde yer alan önemli kuruluşların başında yer almaktadır. Küçük ölçekli ve dağınık halde bulunan tasarrufları toplayarak bunları kredi mekanizması yoluyla reel sektöre aktarmaktadır. Böylece fon fazlası olan birimler (tasarruf sahipleri) ile fon açığı bulunan birimler (yatırımcılar) arasında bir köprü görevi üstlenmektedirler. Bankacılık sisteminde ortaya çıkabilecek herhangi bir olumsuz durum (kriz gibi) tüm finansal sistemi dolayısıyla da reel ekonomiyi büyük ölçüde etkilemektedir. Bu nedenle bankaların yüksek sermaye yeterliliği oranları, likidite gereklilikleri ve risk yönetimi standartlarının ayrı bir önemi bulunmaktadır.

Bankalar; havale, EFT, FAST, kredi kartı ve dijital ödeme altyapıları gibi sistemleri kullanmaktadır. Bu sistemler, ekonomik faaliyetlerin sürekliliğini sağlamakta ve ticaretin kesintisiz yürütülmesine katkı sağlamaktadır. Eğer ödeme sistemlerinde bir aksama meydana gelirse ekonomik faaliyetler yavaşlayabilir ve hatta faaliyetler durma noktasına da gelebilir. Dolayısıyla modern ekonomilerde bankalar, güvenli ve hızlı ödeme sistemlerinin işletilmesinde kilit bir rol üstlenmektedir. Bankacılık ekosistemi gerek barındırdığı hassas finansal veriler gerekse sistem içinde gerçekleştirilen yüksek hacimli para transferleri nedeniyle siber suç örgütlerinin birincil hedefi konumunda yer almaktadır. Siber risk kavramı ise dijital sistemlerde, ağlarda ve verilerde ortaya çıkabilecek olan tehditleri veya bu tehditlerin yaratabileceği zarar unsurlarını tanımlamaktadır. Bankacılık sistemlerine yönelik gerçekleştirilen bu siber tehditlerde yalnızca maddi kayıplarla sınırlı kalmayıp ülkelerin finansal istikrarını tehdit edebilen ve müşteri güvenini sarsarak ekonomik istikrarı zedeleyebilen çok boyutlu etkiler ortaya çıkarabilmektedir.

Siber saldırılar dönemi

Bankacılık ekosistemini tehdit eden başlıca siber saldırılar arasında; oltalama saldırıları (phishing attacks-kimlik avı, mızraklı oltalama saldırıları, sesli oltalama saldırıları, ortadaki adam saldırısı, iş e-postası ele geçirme gibi), kötü amaçlı yazılımlar (malwere-virüsler, ağ solucanları, Truva atları, rootkit, bots, keylogger, fidye yazılımları, casus yazılımları ve botnets gibi) ve işlem dolandırıcılığı (transaction fraud) gibi çeşitli yöntemler yer almaktadır. Bu saldırıların önlenmesi için yalnızca teknik güvenlik önlemleri almak yeterli değildir, aynı zamanda güçlü yasal bir düzenleme ve denetim mekanizmasının bulunmasını da zorunlu kılmaktadır.

Türk Ceza Kanunu'nda (TCK) siber suçlara yönelik olarak önemli yaptırımlar öngörülmüştür.

TCK'da bilişim alanındaki suçlara ilişkin 243. ve 244. Maddelerinde düzenlemeler yapılmış olup; banka veya kredi kurumlarının bilişim sistemlerini hedef alan saldırılarda cezalar yarı oranında artırılmakta, haksız yarar sağlanması durumunda ise iki yıldan altı yıla kadar hapis cezası ve beşbin güne kadar adli para cezası uygulanacağı belirtilmektedir. Bu yasal düzenlemeden de anlaşılacağı üzere konunun ne denli stratejik bir önem arz ettiği anlaşılmaktadır. Türkiye'de bankacılık sektörünün düzenleyici ve denetleyici otoritesi olan Bankacılık Düzenleme ve Denetleme Kurumu (BDDK), bilgi sistemleri ve elektronik bankacılık hizmetlerine ilişkin çeşitli düzenlemeler yayımlamıştır. "Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik" ile bankaların bilgi güvenliği yönetim sistemi kurmaları, siber risk analizleri yapmaları ve iş sürekliliği planları oluşturmaları zorunlu tutulmuştur. Türkiye Cumhuriyet Merkez Bankası (TCMB) ise ödeme ve elektronik para kuruluşlarına yönelik siber güvenlik standartlarını belirleyerek finansal altyapının güvenliğini güçlendirmeyi hedeflemektedir. Öte yandan, siber tehditler konusunda Türkiye Bankalar Birliği (TBB) bünyesinde yürütülen koordinasyon çalışmaları da konuya ilişkin sektörel farkındalığın artırılmasına katkı sağlamaktadır. Diğer yandan, küresel düzeyde siber tehditlere yönelik olarak Basel Bankacılık Denetleme Komitesi (Basel Committee on Banking Supervision) tarafından yayımlanan "Siber Risk Yönetim İlkeleri" de bankalar için bir rehber niteliği taşımaktadır. Bu ilkeler ile siber risklerin ve tehditlerin kurumsal risk yönetimi çerçevesine entegre edilmesi ve üst yönetim sorumluluğunun güçlendirilmesi amaçlanmaktadır.

Son yıllarda Türk bankacılık sistemini hedef alan siber tehditlerin hem nicelik hem de nitelik bakımından arttığı da görülmektedir. Bunda Türkiye'nin gelişmiş dijital bankacılık altyapısı ve yüksek mobil bankacılık penetrasyon oranlarının etkili olduğu söylenilebilir. Türkiye Bankalar Birliği'nin Dijital, İnternet ve Mobil Bankacılık istatistikleri Haziran 2025 dönemi itibariyle toplam (bireysel ve kurumsal) aktif dijital bankacılık müşteri sayısı 120 milyon 999 bin kişiye ulaşmıştır. Bu sayının 1 milyon 230 bin kişisi sadece internet bankacılığı işlemi yaparken, 113 milyon 355 bin kişisi ise sadece mobil bankacılık işlemi yapmıştır. Hem internet hem mobil bankacılık işlemi yapan kullanıcı sayısı 6 milyon 413 bin kişidir. Bu yüksek kullanım düzeyi siber tehditlerin daha da genişleyebileceğini göstermektedir. Öte yandan, İçişleri Bakanlığı'nın resmî açıklamalarına göre de 2020-2026 yılları arasında şüpheli banka hesaplarından gerçekleştirilen işlem hacminin toplam 2 Milyar 183 Milyon TL'lik (yaklaşık 50,35 milyon dolar) olduğu tespit edilmiştir. 1 Şubat 2026 tarihinde yürürlüğe giren yeni düzenlemelerin ardından da Mali Suçları Araştırma Kurulu'na (MASAK) geniş yetkiler verilmiştir. Bu yetkilendirme ile birlikte MASAK, hesap aktivasyonu ve işlem gerçekleştirilmesi öncesinde kimlik doğrulama süreçlerini doğrudan denetleme yetkisine sahip olmuştur. Böylece bankacılık sistemindeki kimlik doğrulama prosedürü bir adım olmaktan çıkıp işlem açısından bir zorunluluk kapsamına dahil edilmiştir.

Sonuç olarak, dijitalleşme ve gelişen teknolojik sistemler nedeniyle bankacılık ekosistemi sürekli siber risklerle karşı karşıya kalmaktadır. Bu siber risk ve tehditlere karşı yalnızca teknik önlemler almak yeterli olmamakta; hukuki, idari, beşerî ve uluslararası boyutları da kapsayıcı bütüncül bir ulusal güvenlik stratejisinin uygulanması gerektirmektedir. Bu bağlamda, siber güvenlik için teknolojik yatırımların artırılması, kamu-özel sektör iş birliğinin sağlanması, mevzuatın güçlendirilmesi ve uygulanması ile konuya ilişkin farkındalığın artırılması amacıyla eğitimlerin düzenli olarak yapılması önerilmektedir. Bu şekilde finansal yapı içinde yer alan tüm paydaşlar arasında bir koordinasyon sağlanabilir ve karşılaşılan siber tehdit unsurlarıyla mücadele edilebilir.