İKV BİLGİ NOTU

AB'NİN SİBER GÜVENLİK DURUMU RAPORU

Bared Çil, İKV Uzmanı

Avrupa Sayıştayı tarafından 21 Eylül 2026 tarihinde yayımlanan yeni bir rapor, AB'nin önemli ve geniş ölçekli siber güvenlik olaylarını tespit etme ve bunlara müdahale etme kapasitesinde çeşitli eksiklikler bulunduğunu ortaya koydu.[1] Raporda özellikle bilgi paylaşımının yetersizliği, AB kurumları ve ağları arasındaki görevlerin örtüşmesi, Avrupa Siber Güvenlik Uyarı Sistemi'nin henüz faaliyete geçmemiş olması ve AB fonlarından yararlanan kuruluşlara yönelik güvenlik kontrollerindeki eksiklikler öne çıkıyor.

Siber güvenlik olayları kamu hizmetlerini, işletmeleri, kritik altyapıları ve AB Tek Pazarı'nı aksatabilecek sonuçlar doğurabiliyor. Bu olaylara müdahale esas olarak üye ülkelerin sorumluluğunda olsa da ciddi mali kayıplara veya kişi ve kuruluşlar üzerinde önemli etkilere yol açan olaylarda AB düzeyinde iş birliği önem taşıyor. Birden fazla üye ülkeyi etkileyen ve tek bir ülkenin müdahale kapasitesini aşan geniş ölçekli olaylarda ise AB'nin koordinasyon mekanizmaları daha da önem kazanıyor.

AB, siber güvenlik kapasitesini güçlendirmek amacıyla son yıllarda çeşitli ağ ve mekanizmalar oluştururken bu alana önemli miktarda kaynak da ayırıyor. 2021-2027 dönemindeki Dijital Avrupa Programı kapsamında siber güvenlik için 1,4 milyar avro tahsis edilmiş durumda. Bununla birlikte Avrupa Sayıştayı, oluşturulan iş birliği çerçevesinin henüz tam anlamıyla etkin şekilde işlemediğine dikkat çekiyor.

Rapora göre sistemin temel sorunlarından biri, üye ülkeler ve AB düzeyindeki siber güvenlik ağları arasında yeterli bilgi paylaşımının gerçekleşmemesi. 2025 yılında kabul edilen Siber Güvenlik Kriz Yönetimi Çerçevesi, büyük ölçekli siber krizlerde AB düzeyindeki rol ve sorumlulukları büyük ölçüde netleştirmiş olsa da ulusal siber olaylara müdahale ekiplerini bir araya getiren CSIRTs Ağı ile siber kriz iş birliğine yönelik EU-CyCLONe arasındaki iş birliğinin nasıl yürütüleceğine ilişkin usuller henüz resmî olarak belirlenmiş değil. Ayrıca bazı üye ülkelerde güncellenmiş AB siber güvenlik kurallarının, özellikle NIS 2 Yönergesi'nin uygulanma süreci devam ederken ulusal güvenlik mevzuatı da paylaşılabilecek bilgileri sınırlandırıyor. Bu durum, sınır ötesi tehditlerin erken tespit edilmesini ve etkili bir müdahalenin koordine edilmesini zorlaştırıyor.

Avrupa Sayıştayı, AB kurumları arasında siber tehditlerin izlenmesi konusunda bazı görev örtüşmelerinin bulunduğunu da tespit etti. Komisyon bünyesinde 2022 yılında oluşturulan Siber Durum Merkezi'nin faaliyetlerinin bir bölümünün, Avrupa Birliği Siber Güvenlik Ajansı'nın (ENISA) tehdit izleme ve durumsal farkındalık oluşturma kapasitesiyle benzerlik gösterdiği belirtildi. Sayıştay, mevcut kaynak ve bilgilerin daha

[1] European Court of Auditors, "Information gaps hamper EU response to cybersecurity incidents", 21.09.2026, https://www.eca.europa.eu/en/news/NEWS-SR-2026-19

etkin biçimde bir araya getirilmesiyle mükerrer çalışmaların azaltılabileceği değerlendirmesinde bulundu. Ayrıca merkezin dış hizmet sağlayıcılarına dayanan mevcut sözleşmesinin 2026 sonunda sona erecek olması nedeniyle merkezin geleceğine ilişkin kapsamlı bir planlama yapılması gerektiğine dikkat çekildi.

Raporda ayrıca Avrupa Siber Güvenlik Uyarı Sistemi'nin henüz faaliyete geçmemiş olması eleştirildi. Sistemin parçası olması planlanan ATHENA ve ENSOC sınır ötesi siber güvenlik merkezlerinin kamu alımı süreçlerindeki gecikmeler nedeniyle çalışmalarına başlayamadığı belirtildi. Sayıştay'a göre gerekli iş birliği anlaşmalarının, ortak sınıflandırma sisteminin ve teknik standartların henüz tamamlanmamış olması da sistemin devreye alınmasını geciktiriyor. Bu durum, siber tehditlerin tespit edilmesi ve üye ülkeler arasında ilgili bilgilerin paylaşılması için geliştirilmesi hedeflenen kapasitenin oluşturulmasını yavaşlatıyor.

Avrupa Sayıştayı, AB siber güvenlik fonlarından yararlanan kuruluşlara yönelik güvenlik kontrollerinde de eksiklikler bulunduğunu belirledi. Bu kontrollerin, AB dışındaki ülkelerin müdahale veya nüfuz riskini azaltması ve hassas güvenlik bilgilerinin AB dışındaki makamlarla paylaşılmasını önlemesi amaçlanıyor. Ancak Avrupa Siber Güvenlik Yetkinlik Merkezi (ECCC), mali destek alan üçüncü tarafların mülkiyet ve kontrol yapılarına ilişkin yararlanıcılar tarafından yapılan değerlendirmeleri doğrulamıyor. Sayıştay, bu durumun hassas altyapıların, operasyonel verilerin ve güvenlik açısından kritik teknolojilerin risklere maruz kalmasına yol açabileceği uyarısında bulundu.

Avrupa Sayıştayı, eksikliklerin giderilmesi amacıyla üye ülkeler arasındaki bilgi paylaşımının güçlendirilmesini, siber güvenlik durumsal farkındalığına yönelik kapasitenin daha etkin biçimde koordine edilmesini, Avrupa Siber Güvenlik Uyarı Sistemi'nin faaliyete geçirilmesini ve Dijital Avrupa Programı kapsamındaki projelerin izlenmesine yönelik mekanizmaların geliştirilmesini tavsiye etti. Sayıştay ayrıca siber güvenlik projelerinin performansına ilişkin verilerin daha güvenilir ve sistematik biçimde toplanması gerektiğine dikkat çekti.