İKV BİLGİ NOTU

AVRUPA KOMİSYONUNDAN SİBER DAYANIKLILIK YASASI

Sema Nur Yeniyıldız, İKV Uzman Yardımcısı

Avrupa Komisyonu, 15 Eylül 2022 tarihinde, dijital unsurları barındıran ürünlerin yatay siber güvenlik gereksinimlerine ilişkin "Siber Dayanıklılık Yasası" başlıklı tüzük taslağını yayımladı. Taslağa göre, dijital unsurlara sahip olan bir ürün (herhangi bir dijital donanım, yazılım ürünü veya uzaktan da olsa veri işleme çözümleri) üreticisi, ürünlerini AB pazarında satmak istiyorsa, AB'nin siber güvenlik yükümlülüklerini karşılaması gerekiyor.

16 Aralık 2020 tarihli AB'nin Dijital On Yılı için siber Güvenlik Stratejisi doğrultusunda dijital ürünler ve yardımcı hizmetler için yeni siber güvenlik kurallarını oluşturmayı amaçlayan Siber Dayanıklılık Yasası, konuyla ilgili mevcut AB mevzuatını, güncellenme aşamasında olan Ağ ve Bilgi Güvenliği Yönergesi'ni (*Network and Information Security*-NIS) ve 2019 AB Siber Güvenlik Yasası'nı tamamlamayı amaçlıyor.

Kamuoyu incelemesi ve istişaresi ile oluşturulan Siber Dayanıklılık Yasası, iç pazarın düzgün bir şekilde işlemesini amaçlayan iki temel hedef ortaya koyuyor:

- Yazılım ve dijital donanım ürünlerinin daha az güvenlik açığı ile piyasaya sürülmesini ve dijital unsurlara sahip bir ürünün yaşam döngüsü boyunca siber güvenliği garanti etmesini sağlayarak güvenli ürünlerin geliştirilmesi için koşullar yaratmak;
- Kullanıcıların dijital unsurlara sahip ürünleri seçerken ve kullanırken, siber güvenliği dikkate almalarını ve güvenlik ile ihtiyaçlarını eşleştirerek kullanmalarını sağlamak.

Yasanın belirlediği dört özel hedef ise şu şekilde sıralanıyor:

- Yazılım ve dijital donanım üreticileri için siber güvenlik kurallarına uyumu kolaylaştıran, tutarlı bir siber güvenlik çerçevesi oluşturmak;
- Üreticilerin, tasarım ve geliştirme aşamasından itibaren dijital unsurlar barındıran ürünlerin yaşam döngüsü boyunca güvenliğini geliştirmelerini sağlamak;
- Dijital unsurları barındıran ürünlerin güvenlik özelliklerinin şeffaflığını artırmak;
- İşletmelerin ve vatandaşların, dijital unsurları barındıran ürünleri güvenli bir şekilde kullanmalarını sağlamak.

Yasaya Göre Güvenlik İlkesi

Komisyon, Siber Dayanıklılık Yasası'nda, Tasarıma Göre Güvenlik (*Security-by-Design*) ilkesi ile iki kategori arasında ayrım yapıyor: (i)dijital unsurları barındıran ürünler ve (ii) dijital unsurları barındıran kritik ürünler.

İlk ürün kategorisi, önerilen yasanın Ek II'sinde yer alıyor. Az sayıda düzenlemeden oluşan Ek II, bu ürün kategorisine bazı yükümlülükler getiriyor. Ayrıca bu ürünler üreticilerinin, varsayılan ayarları güvenli hâle getirme, güvenli veri aktarım yöntemleri ve güvenlik durumunu güncelleme gibi seçenekleri sunmalarını zorunlu kılıyor. Böylece, kullanıcıların

satın aldığı yazılımların ve ağ bağlantılı ürünlerin kullanımı süresince güçlü siber güvenlik önlemleriyle uyumlu hâle getirilmesi hedefleniyor.

Yasanın Ek III'ü ise kritik ürün kategorisine giren şifre yöneticileri, virüs tarayıcıları, belirli işletim sistemleri, mikro-işlemciler, uygulamaya özel devreler (*application-specific circuits*-ASICs) ve ağ cihazları gibi yazılımlar için dağıtım şirketlerine siber güvenliğin sağlanması konusunda çok daha kapsamlı yükümlülükler getiriliyor.

Siber Dayanıklılık Yasası'nın Muhtemel Etkisi 2026'da

AB, ağ bağlantılı cihazların siber güvenliğini iyileştirmenin aciliyetini kabul etse de uzmanlar, yasanın bu yasama döneminde istişare ve onay sürecini geçemeyeceğini belirtiyor. Ayrıca Komisyonun yasa ile dijital unsurları barındıran ürünler ve bu ürünlerin üreticileri için öngördüğü geçiş süreleri oldukça uzun; yasanın kabul edildiği tarih ile yürürlüğe girmesi ve uygulamaya başlanması arasında iki yıl süre verilmesi planlanıyor. Bununla birlikte, piyasadaki ürünlerle ilgili değişiklik yapılmadığı sürece bu ürünler yeni düzenlemeye tabi olmayacak. Belirlenen uzun geçiş sürecinin dışında özellikle küçük işletmelerin, Siber Dayanıklılık Yasası yükümlülüklerine uyum sağlama ve bu yükümlülükleri uygulamaya geçirme konusunda ne kadar istekli olacağı da büyük bir soru işareti olarak karşımıza çıkıyor. Tüm bu koşullar, Siber Dayanıklılık Yasası'nın muhtemelen 2026 yılına kadar yürürlüğe giremeyeceğini gösteriyor.