T.B.M.M.
CUMHURİYET HALK PARTİSİ
Grup Başkanlığı
Tarih: 14 Ağustos 2025
Sayı: 13407

34512

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

Aşağıdaki sorularımın **Sanayi ve Teknoloji Bakanı Sayın Mehmet Fatih KACIR** *tarafından yazılı olarak yanıtlanmasını arz ederim*

Av. Dr. M. Sezgin TANRIKULU
Diyarbakır Milletvekili

Türkiye'nin ulusal güvenliği, ekonomik istikrarı ve vatandaşların mahremiyeti açısından büyük önem taşıyan siber güvenlik, günümüzün en kritik konularından biridir. Kamu kurum ve kuruluşları, barındırdıkları hassas veriler ve yürüttükleri stratejik faaliyetler nedeniyle siber saldırıların başlıca hedefleridir. Bu bağlamda, 1 Ocak 2021 ile 30 Haziran 2025 tarihleri arasındaki döneme ilişkin kamu kurum ve kuruluşlarına yönelik siber saldırılar hakkında aşağıdaki soruların yanıtlanması elzem hale gelmiştir. Bu bağlamda;

1- 1 Ocak 2021 - 31 Aralık 2021, 1 Ocak 2022 - 31 Aralık 2022, 1 Ocak 2023 - 31 Aralık 2023, 1 Ocak 2024 - 31 Aralık 2024 ve 1 Ocak 2025 - 30 Haziran 2025 tarihleri arasında, kamu kurum ve kuruluşlarına yönelik gerçekleştirilen siber saldırıların yıl bazında sayısı ve hedef alınan kurum/kuruluş isimleri nelerdir?

2- Bu dönemde en çok hedef alınan kamu kurum ve kuruluşları hangileridir ve bu kurumların hangi alanlarda faaliyet gösterdikleri göz önünde bulundurulduğunda, saldırganların motivasyonları hakkında ne gibi çıkarımlar yapılmaktadır?

3- Yukarıda belirtilen dönemler itibarıyla, kamu kurum ve kuruluşlarına yönelik siber saldırıların kaç adedi başarılı bir şekilde engellenmiştir?

4- Engellenemeyen ve sisteme nüfuz edebilen siber saldırı sayısı kaçtır? Bu saldırıların başarılı olmasının temel nedenleri nelerdir (örn. insan hatası, yazılım açığı, donanım yetersizliği vb.)?

5- Gerçekleşen siber saldırıların türlerine göre dağılımı nasıldır (örn. fidye yazılımı, oltalama, DDoS, veri sızdırma, casus yazılım vb.)? Hangi saldırı türleri daha yaygın olarak gözlemlenmiştir?

6- Bu saldırıların kaynak ülkeleri veya bölgeleri hakkında elde edilen istihbari bilgiler nelerdir? Yabancı istihbarat servisleri, terör örgütleri veya organize suç çetelerinin bu saldırılardaki rolüne ilişkin herhangi bir bulguya rastlanmış mıdır?

7- Engellenemeyen siber saldırılar sonucunda kamu kurum ve kuruluşlarında meydana gelen maddi zararın toplam boyutu ne kadardır? Bu zararlar hangi kalemlerde (örn. sistem onarımı, veri kurtarma, adli bilişim incelemeleri vb.) oluşmuştur?

8- Çalınan veya erişilen verilerin ülke menfaatleri açısından oluşturduğu veya oluşturacağı potansiyel zararlar nelerdir? Bu verilerin ulusal güvenlik, savunma sanayii, ekonomik bilgiler, kritik altyapı sistemleri veya vatandaşlık bilgileri gibi hassas alanlara ilişkin olup olmadığı hususunda bir değerlendirme yapılmış mıdır? Yapıldıysa sonuçları nelerdir?

9- Kamu kurum ve kuruluşlarının siber güvenlik altyapısı ve kapasitesi, bu dönemdeki siber tehditlere karşı yeterli midir?

10- Siber güvenlik alanında personel yeterliliği, teknolojik altyapı eksiklikleri veya mevzuatsal boşluklar gibi tespit edilen eksiklikler nelerdir ve bunların giderilmesi için hangi adımlar atılmıştır veya atılması planlanmaktadır?

11- Siber saldırılara karşı ulusal düzeyde bir koordinasyon mekanizması bulunmakta mıdır? Bu mekanizma ne kadar etkin çalışmaktadır?

12- Siber güvenlik konusunda uluslararası işbirlikleri ve anlaşmalar yapılmış mıdır? Yapıldıysa, bu işbirlikleri siber saldırıların önlenmesi ve faillerin tespiti konusunda ne kadar etkili olmuştur?

13- Gelecekte siber saldırıların önlenmesi ve siber güvenliğin güçlendirilmesi amacıyla orta ve uzun vadeli ulusal siber güvenlik stratejileri belirlenmiş midir? Belirlendiyse, bu stratejilerin temel hedefleri ve uygulama takvimi hakkında tarafıma özet bilgi verilmesini talep ediyorum.

14- Kamu personeline yönelik siber güvenlik farkındalığını artırmak ve saldırılara karşı dirençlerini güçlendirmek amacıyla düzenlenen eğitim ve bilgilendirme faaliyetleri nelerdir? Bu faaliyetlerin etkinliği hangi kriterlere göre ölçülmektedir?