T.B.M.M.
CUMHURİYET HALK PARTİSİ
Grup Başkanlığı
Tarih : 15 Nisan 2025
Sayı : 10830

27188

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

Aşağıdaki sorularımın ***Cumhurbaşkanı Yardımcısı Sayın Cevdet Yılmaz*** tarafından Anayasa'nın 98'inci ve TBMM İçtüzüğünün 96'ncı ve 99'uncu maddeleri gereğince yazılı olarak cevaplandırılmasını talep ederim.

Saygılarımla.

Doç. Dr. Gökhan GÜNAYDIN
İstanbul Milletvekili
CHP Grup Başkanvekili

Türkiye'de yaşanan kişisel veri hırsızlığı ve yasa dışı satış iddiaları ve kişisel verilerin güvenliğine yönelik zafiyet uzun zamandır tartışılıyor. AKP elinde veri güvenliği yok edilmiştir. 2016'da, 50 milyondan fazla Türk vatandaşının kişisel verileri çevrimiçi olarak sızdırıldı. Bu, Türkiye'nin bilinen en büyük veri ihlali olarak kayıtlara geçti. 2022'de e-Nabız verilerinin eski AKP Gençlik Kolları Başkanı Adem Ali Yılmaz ile bağlantılı Bilbest adlı şirket tarafından Katar'a yaklaşık 100 milyon dolara satıldığı iddia edildi. 2023'te "Sorgu Paneli" adlı bir web sitesinin, Türk vatandaşlarının adres ve banka bilgileri gibi kişisel ve finansal verilerine erişim sağladığı ortaya çıktı. 2024'te Free Web Turkey, aralarında ölen vatandaşlar ve yabancı ziyaretçilerin de bulunduğu 108 milyon kişinin kişisel verilerinin çalındığını ve beş Google Drive dosyasında saklandığını iddia etti.

10 Nisan 2025 tarihinde basına yansıyan ve tartışmaların yeniden başlamasına yol açan Ankara Cumhuriyet Başsavcılığı'nca yürütülen soruşturma, Türkiye'de kişisel bilgilerin gizliliğine yönelik yaşanan zafiyeti de bir kez daha gözler önüne serdi. Şüpheliler hakkında hazırlanan ve Ankara 28'inci Ağır Ceza Mahkemesi'nde kabul edilen iddianamede, çok kritik ayrıntılar yer almaktadır. Toplam 101 milyon kişinin bilgilerinin paylaşıldığı paralı internet sitelerinden, MSB ve MİT personelinin bilgisinin de paylaşıldığı ortaya çıkmıştır.

Geçtiğimiz ay "veri sızıntısı" iddiasıyla haber yapanlara ve paylaşanlara hapis cezası getiren Siber Güvenlik Yasası çıkarılırken, iktidarın aynı aylarda devletin verilerini çaldırdığı bu yeni İddianameyle kanıtlanmaktadır. Öyle ki "veri sızmadı, yalan söyleniyor" diyenler, yeni İddianamede mağdur ve müşteki olmuşlardır. 19-25 yaşları arasında olan toplam 16 şüphelinin yargılandığı iddianamenin mağdurları, Sağlık Bakanlığı, Çevre ve Şehircilik Bakanlığı, MEB, SGK, İŞKUR, Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü, Ankara Büyük Şehir Belediyesi,

Adana Yüreğir Belediyesi, 6 üniversite, Yavuz Sultan Selim ve Kuzey Çevreyolu Otoyol İşletmesi'dir.

Yeni iddianame devletin, MSB ve MİT gibi kritik önemdeki kurumların, kurum personelinin ve vatandaşların temel verilerinin siber korsanların kripto para cüzdanında gezdirildiğini; veri hırsızlarının abonelerden kripto hesaplarındaki soğuk para cüzdanlarına para yatırılmasını istediklerini ortaya çıkarmıştır.

İddianame açıkça vatandaşların E-devlet, MERNİS, tapu ve kadastro, TC kimlik ve plaka, cep telefonu, okul öğrenci bilgilerinin, sağlık verilerinin hukuka aykırı yolla ele geçirildiği ve illegal sorgu platformları açılarak paylaşıldığını, üçüncü kişilere para karşılığı satıldığını, farklı platformlar üzerinden işbirliği ve iştirak iradesiyle bu şüphelilerce para kazanma amacıyla suç işlendiğini göstermektedir. Türkiye'ye sağlık amaçlı gelen yabancıların da birçok verisi bu saldırganların altyapısına alınmıştır. MİT ve MSB personelinin verileri, lojman ve adres bilgileri dahi sistemlere sızdırılmış, para karşılığı abonelere satılmış, bu veriler üzerinden sahte kimlik ve belge üretimi altyapısı kurulmuştur. Devlete ait sitelere sızılarak memurların şifre ve kullanıcı adları dahi çalınmıştır. MTV borcu olanlar dahi süzülerek bilgileri çalınmıştır. Bu yasadışı platformlara abone olan herkese, kripto soğuk para cüzdanlarına yatırdıkları ücret karşılığı "mahrem" veriler satılığa çıkarılmıştır. Çıkan kanun maddesi ile bu iddianamenin zamanlaması kıyaslandığında, nelerin örtbas edilmek istendiği, basının bu iddianamedeki asıl yönleri neden daha ayrıntılı yazamadığı daha iyi anlaşılabilir.

İddianamenin konu edindiği birkaç örnek sorgu sistemi (illegal panel) vardır. TAVŞANCIK, İLLEGALCITY, XLOG, PRIVEX, FEARCHECK, GUSİCHE, PERLAAPİ, HYDRA FORUMS, DARK DEEP adlı yasadışı panel ve internet siteleri üzerinden milyarlarca kişisel ve kamusal veri para karşılığı erişime açılmıştır.

Bu suç panellerinin geneline bakıldığında; 101 milyon kişisel veriye ek olarak, E-SINAV verileri, SGK ve ilaç bilgileri, tapu kayıtları, plaka bilgileri, aşı takibi, yatay geçişler, cep telefonları, tüm nüfus bilgileri güncel ve anlık paylaşıma açıktır. Bu panel yöneticileri organize biçimde TC aleyhine organize faaliyete iştirak etmiş, kritik verilerin çalınması ve satılmasında birlikte hareket etmiştir. MİT, asker, polis jandarma kimlik kartı, TC kimlik kartları, ehliyet ve diplomaların sahtelerinin üretilmesi için hazır veritabanı sağlamıştır. Suç tarihi 2024 yılında olmasına karşın, ilgili site ve sorgulama sistemlerinin daha öncesinde de faaliyette olduğu düşünüldüğünde, şu an 19-25 aralığındaki bu gençlerin reşit yaştan önce de bu veri sızıntısı faaliyetine katıldıkları, dolayısıyla 18 yaş altındaki çocukların suça teşvik edilmesi, siber zorbalık, devlet kurumlarının alenen aşağılanması suçlarının oluştuğu savunulmaktadır. Üstelik, iddianameye göre bu gençlerin çoğunun bilgisayar sistemleri ve veri yönetimi konusunda aşırı donanımlı olmadığı, orta ya da alt düzeydeki tecrübeleriyle ve kısıtlı yabancı dille de bu işi yapabildiği ya da onlara yaptırıldığı görülmüştür. Sistemde abonelik bedelleri bazı platformlarda soğuk cüzdan kripto para adresine transferle mümkündür.

Bu bağlamda;

1. Söz konusu veriler; görevde olan personel ve yakınları için hayati tehlike oluşturmakta mıdır? Eğer oluşturuyorsa bunun için önlem alındı mı? Alınan önlem varsa ne tür önlemler alındı?

2. Veri sızıntısına kasten, ihmal yüzünden veya yetersiz eğitim ve uzmanlık yüzünden sebep olan kurum çalışanları, taşeron şirket çalışanları tespit edildi mi? Bu çalışanların mali hareketleri inceleniyor mu?

3. Bu verilerin yayınlandığı platformlar sadece iddianamede geçenlerden mi ibaret?

4. Verilere erişim sağlayan tüm kullanıcılar tespit edilebildi mi?

5. Verilere erişim sağlayanlar içerisinde T.C. ile menfaat çatışmasına sahip olan ülkelerin istihbarat kurumları var mı?

6. Dark Web üzerinde sızıntılar için tarama yapıldı mı, kurumlarda bu taramayı yapacak ürünler var mı (SpyCloud, Recorded Future, IntSights, Kela, Digital Shadows, Constella Intelligence, vb.) ve rutin olarak kullanılıyor mu?

7. Bu sızıntı özelinde TOR (Onion Ağları) ve OSINT (Açık İstihbarat) taraması yapıldı mı? Bu taramalar için standartlar ve görevlendirilmiş birimler var mı?

8. Kurumlarımızın sızıntı tespiti anında ilk yapılacaklar için rutin prosedürü belirlendi mi ve kurumlarda ilgili personele eğitimi verildi mi?

9. Bu veri sızıntısında KamuNet ağında yer alan sistemlerde yer alan zafiyetlerin rolü var mı? Bu ağa erişen personel ve entegrasyon yapan paydaşların hareketleri takip altında mıdır?

10. Sızıntılarda bireysel erişim dışında kurumlar arasındaki Web Servis entegrasyonlarının rolü nedir? Bu entegrasyonlarda hizmet verilen kurumdaki erişim sağlayan kullanıcı bilgisi izleniyor ve loglanıyor mu?

11. Yine entegrasyon ve sistem geliştirme süreçlerinde yer alan taşeron şirketlerin/kurumların bu sızıntılardaki rolü nedir? Bu şirketlerin ve kurumların çalışanları için uygulanan prosedürler mevcut mudur?

12. Tüm kamu kurumları için bu tip veri sızıntılarını süreçler halinde tanımlayan, rutin sızıntı taramalarını tanımlayan, ilk sızıntı tespiti anında yapılacakları belirleyen, tüm geliştirme ve entegrasyon süreçlerini bu tür saldırılara karşı koruyacak bir veri güvenliği politikası ne zaman oluşturulacaktır?