T.C.
ULAŞTIRMA VE ALTYAPI BAKANLIĞI
Strateji Geliştirme Başkanlığı
Strateji Daire Başkanlığı

Sayı : E-44697349-610-2494132
Konu : Konya Milletvekili Sayın Barış BEKTAŞ'ın yazılı soru önergesi

7/20471 GK 66

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

İlgi : 18.12.2024 tarihli ve E-43452547-120.07.04-1550133 sayılı yazınız.

Konya Milletvekili Sayın Barış BEKTAŞ'ın 7/20471 esas sayılı yazılı soru önergesinin cevabı ilişikte sunulmaktadır.

Bilgilerinize arz ederim.

Abdulkadir URALOĞLU
Bakan

Ek: Cevap Formu (1 Sayfa)

Hakkı Turayliç Caddesi No:5 06338 Emek / Çankaya / ANKARA
KEP Adresi : uab@hs01.kep.tr

Bilgi için:Cahit Tanfer TEMİZKAN
Şube Müdür V.
Telefon No:(312) 203 10 16
E-Posta:
soruonerge.sgb@uab.gov.tr

T.C.
ULAŞTIRMA VE ALTYAPI BAKANLIĞI
Strateji Geliştirme Başkanlığı

KONYA MİLLETVEKİLİ SAYIN BARIŞ BEKTAŞ'IN 7/20471 ESAS SAYILI YAZILI SORU ÖNERGESİNİN CEVABI

Ülkemizde ulusal siber güvenliğin sağlanmasına ilişkin faaliyetler, 5809 sayılı Kanun çerçevesinde Bakanlığımız ile Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından sürdürülmektedir.

Bu kapsamda; BTK bünyesinde 2013 yılında kurulan Ulusal Siber Olaylara Müdahale Merkezi (USOM) koordinasyonunda, kamu kurumları ve kritik altyapı sektörlerinde oluşturulan ve sayıları 2.317'ye ulaşan Kurumsal ve Sektörel SOME'ler (Siber Olaylara Müdahale Ekipleri), siber olaylara müdahale konusunda 7/24 görev yapmaktadır. Anılan çalışmalarda, yerli ve milli imkanlarla, tamamen iç kaynaklarla gerçekleştirilen, yapay zekâ ve makine öğrenmesi imkânlarını kullanan AVCI, AZAD, KASIRGA, ATMACA ve KULE gibi hızlı tespit ve erken müdahale sistemleri kullanılmaktadır.

Tespit edilen zafiyetler ve zararlı yazılımlara ilişkin bulgular, alınması gerekli önlemleri de içerecek detaylı açıklamalar ile vakit geçirmeksizin ilgili kurum/kuruluş ile paylaşılmakta ve bu kurum/kuruluşlarca gerekli önlemlerin alınması sağlanmaktadır.

10.12.2024 akşamı 21:35 itibari ile PTT HGS mobil uygulaması anlık bildirim servisi üzerinden anlamsız mesajlar gönderilmesi üzerine sisteme anında müdahale edilmiş ve ilk dakika içerisinde ilgili uygulama servislerinde önlem alınmıştır.

Saldırganların özellikle mobil uygulamalar içerisinde yerleşik API anahtarlarını kullanarak müşterilere bildirimler gönderebildikleri ve bu bildirimler aracılığı ile vatandaşları dolandırmaya ve paniğe sevketmeye yönelik aksiyonlar aldıkları bilinmektedir.

Gerçekleşen olayın dış kaynak 3. parti yazılım olarak kullanılan Onesignal servisi üzerinden kullanıcılara anlık bildirim gönderimi yapılarak gerçekleştirildiği tespit edilmiş ve son günlerde farklı mobil uygulamalarda benzer şekilde yaşanan bu durum süresince kişisel veriler dahil HGS verilerine hiçbir şekilde erişim, sızma, müdahale olmamış veya verilerin güvenliğine yönelik herhangi bir olumsuz durum yaşanmamıştır.

Onesignal uygulamasına erişim için kullanılan Apikey şifrelenmiş ve erişim algoritmaları değiştirilerek uygulama mimarisinin erişimi tamamı ile değiştirilmiştir. Ayrıca; siber saldırganların tespit edilmesine yönelik olarak 16.12.2024 tarihinde Ankara Cumhuriyet Başsavcılığına suç duyurusunda bulunulmuş ve kolluk kuvvetlerine de gerekli teknik destek sağlanmıştır.