



T.C.
ULAŞTIRMA VE ALTYAPI BAKANLIĞI
Strateji Geliştirme Başkanlığı

Türkiye Büyük Millet Meclisi -
Türkiye Büyük Millet Meclisi
Başkanlığı
Tarih: 07/12/2021 10:29
Sayı: E-120.07-
0924155



7/53752 GK 34

Sayı : E-44697349-610-77178

Konu : İzmir Milletvekili Sayın Mahir
POLAT'ın yazılı soru önergesi

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

İlgi : 27.10.2021 tarihli ve 43452547-120.07-E.902505 sayılı yazınız.

İzmir Milletvekili Sayın Mahir POLAT'ın 7/53752 esas sayılı yazılı soru önergesinin cevabı
ilişikte sunulmaktadır.

Bilgilerinize arz ederim.

Adil KARAİSMAİLOĞLU
Bakan

Ek: Cevap Formu (1 Sayfa)

Bu belge, güvenli elektronik imza ile imzalanmıştır.

Doğrulama Kodu: 8746E444-3C85-474A-ABFA-1B4EDB41B283

Doğrulama Adresi: <https://www.turkiye.gov.tr/uab-ebys>

Hakkı Turaylıç Caddesi No:5 06338 Emek / Çankaya / ANKARA

KEP Adresi : uab@hs01.kep.tr

Bilgi için: Nurhayat
ORUCUOĞLU
Teknisyen





T.C.
ULAŞTIRMA VE ALTYAPI BAKANLIĞI
Strateji Geliştirme Başkanlığı

**İZMİR MİLLETVEKİLİ SAYIN MAHİR POLAT'IN
7/53752 ESAS SAYILI YAZILI SORU ÖNERGESİNİN CEVABI**

Ülkemizin siber güvenliğine yönelik tehditlerin belirlenmesi, muhtemel saldırı ve olayların etkilerinin azaltılması veya ortadan kaldırılmasına ilişkin önlemlerin geliştirilmesi ve belirlenen aktörlerle paylaşılması amacıyla kurulan Ulusal Siber Olaylara Müdahale Merkezi (USOM), Bilgi Teknolojileri ve İletişim Kurumu (BTK) bünyesinde faaliyet göstermektedir. Ayrıca, kamu kurumları, üniversiteler ve kritik altyapı sektörlerinde oluşturulan Kurumsal ve Sektörel SOME'ler (Siber Olaylara Müdahale Ekipleri), USOM koordinasyonunda siber olaylara müdahale konusunda görev yapmaktadır. Halihazırda Bakanlığımızca hazırlanan Kurumsal ve Sektörel SOME Kurulum ve Yönetim Rehberleri doğrultusunda oluşturularak faaliyet gösteren 1.927 adet SOME bulunmaktadır.

Siber saldırganların ülkemizde kamu kurumlarını, özel sektör ve vatandaşlarımızı hedef alarak bu amaçlarını gerçekleştirmelerinin önlenmesi için USOM tarafından, başta kritik kamu kurumları ve kritik kamu hizmetlerinin 7/24 izlenmesi olmak üzere zafiyet tarama ve tespit çalışmaları sürdürülmektedir. Siber olay durumunda USOM bünyesindeki siber olay müdahale ekipleri tarafından ilgili kurum, kuruluş, üniversite, özel sektör firmaları vb. ile yerinde müdahale çalışmaları yürütülmekte ve olayın tekrar yaşanmaması için alınması gereken tedbirler belirlenmektedir.

USOM bünyesinde siber tehditlerle mücadele kapsamında yürütülen projelerde öz kaynaklarla geliştirilen AVCI, AZAD, KASIRGA, ATMACA ve KULE uygulamaları ile siber saldırılara karşı 7 gün 24 saat mücadele edilmekte ve ulusal siber güvenliğimize önemli katkılar sağlanmaktadır. Ülkemizde en fazla saldırı alan sektörler elektronik haberleşme altyapısı ve kamu kurumları başta olmak üzere enerji, sağlık, bankacılık, finans, ulaşım, havacılık gibi sektörlerdir. Söz konusu saldırıların %99'undan fazlasını dağıtık servis dışı bırakma (DDoS) ve oltalama (phishing) saldırıları oluşturmaktadır.