7/24824

T.C.
BİLİM, SANAYİ VE TEKNOLOJİ BAKANLIĞI
Strateji Geliştirme Başkanlığı

Sayı : 75833232 - 610E.253
Konu : Soru Önergeleri

10/04/2018

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA
(Kanunlar Ve Kararlar Başkanlığı)

İlgi : 20/03/2018 tarihli ve 43452547-120.07-250529 sayılı yazınız.

Bakanlığıma intikal eden ilgi yazı eki, Niğde Milletvekili Sayın Ömer Fethi GÜRER tarafından tevcih edilen 7/24824 esas numaralı yazılı soru önergesinin cevabı ekte gönderilmektedir.

Bilgilerinizi ve gereğini arz ederim.

Faruk ÖZLÜ
Bakan

Ek:
Cevabi Yazı (1 sayfa)

Güvenli Elektronik İmzalı
Aslı ile Aynıdır.
..11../.04./20K.

Macide ÇİÇEK
Strateji Geliştirme Başkanlığı
Memur

"Bu belge, güvenli elektronik imza ile imzalanmıştır."

Mustafa Kemal Mahallesi Dumlupınar Bulvarı
Eskişehir Yolu 2151.Cadde No:154 06510
Çankaya /ANKARA
☎ 03122016138
✉ rabia.canakcioglu@sanayi.gov.tr
Bilgi İçin İrtibat: Rabia ÇANAKÇIOĞLU Mali Hizmetler Uzmanı
🖷 03122016103
🖳 www.sanayi.gov.tr
Evrak bilgisine www.sanayi.gov.tr adresindeki e-hizmetler bölümünden, "luuql1D85E5B" DYS No ve evrak tarihi ile erişebilirsiniz.luuql1D85E5B

NİĞDE MİLLETVEKİLİ SAYIN ÖMER FETHİ GÜRER'İN

7/24824 ESAS SAYILI YAZILI SORU ÖNERGESİNE İLİŞKİN CEVAPLAR

Soru 1- Bilgi ve İletişim Teknolojileri kullanılarak bir kişi veya gruba yönelik teknik ya da ilişkisel tarzda zarar verme davranışı gösteren, şifrelerin çalınması ya da zararlı yazılım içeren mesajlar gönderilmesi hatta WEB sitelerine saldırılarak işlevsiz bırakan, siber zorbalık yapan kişilere yönelik ne gibi işlemler yapılmaktadır?

Soru 2- 2017 yılında belirlenen kişi sayısı kaçtır, herhangi bir işlem uygulanmış mıdır?

CEVAPLAR:

Cevap 1-2- Bu önergenin muhatabının Ulaştırma, Denizcilik ve Haberleşme Bakanlığımız olduğu mütalaa edilmekle birlikte Bakanlığımız teşkilatı bünyesinde de, tarafımıza gerçekleşebilecek muhtemel siber saldırılara karşı her daim önlem alınmaktadır.

Nitekim bir siber saldırı karşısında, yüksek düzey ve isabet oranıyla tespit yapılabilmesi için gerekli kanıt miktarı ve niteliğinin toplanması gerekmektedir. Bu bağlamda siber saldırının yapıldığı tespit edilir edilmez, ilgili kaynak adresinin erişimi engellenir ve karantinaya alınır. İlgili kaynak adresin siber güvenlik repütasyonu sorgulanıp bilgi toplanır. Sonraki süreçte ise, yapılan istekler güvenlik cihazları üzerinden alınan kayıtlarda incelenmekte ve saldırının amacı tespit edilmeye çalışılır. Ayrıca, gerektiğinde USOM ve bağlı kuruluşlara ilgili durum hakkında bilgi verilir.

Bu çerçevede 2017 yılında, bilgi toplama ve keşif çalışması gerçekleştirilen toplam 204 ip adresi engellenmiştir.