



T.C.
ULAŞTIRMA VE ALTYAPI BAKANLIĞI
Strateji Geliştirme Başkanlığı

7/9425
61-101

Sayı : 44697349-610.01/29721
Konu : Ankara Milletvekili
Sayın Levent GÖK'ün
yazılı soru önergesi

15-04-2019

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

İlgi: 14.03.2019 tarihli ve 43452547-120.07-E.441413 sayılı yazınız.

Ankara Milletvekili Sayın Levent GÖK'ün 7/9425 esas sayılı yazılı soru önergesinin cevabı ilişikte sunulmaktadır.

Bilgilerinize arz ederim.


M. Cahit TURHAN
Bakan

EK :1) Cevap formu (2 Sayfa)

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

Telefon: 203 13 66

E-posta: soruonerge.sgb@uab.gov.tr

Faks: 213 07 60

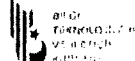
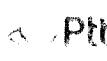
İnternet Adresi: www.uab.gov.tr

Ayrıntılı bilgi alınacak kişi:

N.GÜMÜŞ

V.H.K.İ

Başarıyla Gönderildi





T.C.
ULAŞTIRMA VE ALTYAPI BAKANLIĞI
Strateji Geliştirme Başkanlığı

ANKARA MİLLETVEKİLİ SAYIN LEVENT GÖK'ÜN
7/9425 ESAS SAYILI YAZILI SORU ÖNERGESİNİN CEVABI

Ülkemizde siber tehditlerle mücadele kapsamında yürütülen çalışmalar, her geçen gün artarak devam etmektedir. Bu çerçevede hazırlanan “2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı”, ülkemizin siber güvenliğe yönelik dört yıllık vizyon belgesini oluşturmaktadır.

Bahse konu eylem planı kapsamında başta elektronik haberleşme, finans, sağlık, enerji gibi kritik sektörler ve altyapılar olmak üzere ülkemizin siber alandaki güvenliğinin artırılmasına yönelik çalışmalar yürütülmektedir. Ayrıca, ülkemizde siber güvenlik konusunda nitelikli insan kaynağını artırmaya yönelik faaliyetler ile farkındalık oluşturmaya yönelik faaliyetlerimiz ise aralıksız devam etmektedir. Diğer yandan, ülkemizdeki siber güvenlik ekosisteminin geliştirilerek yerli ve milli ürünlerin artırılması ve yaygınlaşması da eylem planı kapsamında yürütülen önemli faaliyetlerden biridir.

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 Başkanlığı (BTK) bünyesinde faaliyet göstermektedir. Ayrıca, kamu kurum ve kuruluşları ile kritik altyapı sektörlerinde oluşturulan Kurumsal ve Sektörel Siber Olaylara Müdahale Ekipleri (SOME), USOM koordinasyonunda siber olaylara müdahale konusunda görev yapmaktadır. Halihazırda Bakanlığımızca hazırlanan Kurumsal ve Sektörel SOME Kurulum ve Yönetim Rehberleri doğrultusunda oluşturularak faaliyet gösteren 1135 adet SOME bulunmaktadır.

Siber saldırganların ülkemizde kamu kurumlarını, özel sektör ve vatandaşlarımızı hedef alarak bu amaçlarını gerçekleştirmelerinin önlenmesi için USOM tarafından, kritik kamu kurumları ve kritik kamu hizmetlerinin 7/24 esasına göre izlenmesi başta olmak üzere zafiyet tarama ve tespit çalışmaları sürdürülmektedir. Ayrıca, bünyesindeki siber güvenlik uzmanları tarafından siber tehdit analiz, tespit ve önleme faaliyetleri de yürütülmektedir. Bu çalışmalar neticesinde tespit edilen zafiyetler ve zararlı yazılımlara ilişkin bulgular, alınması gerekli önlemleri de içerecek detaylı açıklamalar ile vakit geçirmeksizin ilgili kurum/kuruluş ile paylaşmakta ve bu kurum/kuruluşlarca gerekli önlemlerin alınması sağlanmaktadır.

Öte yandan, siber saldırılar nedeniyle oluşan zararın ekonomik boyutunun belirlenmesine yönelik dünya genelinde gerçekleştirilen çalışmalarda ortak kullanılan ve kabul görmüş bir model bulunmamakta, genellikle varsayım, tahmin ve öngörülere dayalı olarak yapılmaktadır. Yapılan tahminlerde siber saldırılar sonucu doğrudan oluşan zararlar, karşılaşılan siber saldırılara müdahalenin maliyetleri, siber saldırılar sonucu itibar kayıpları ile kayıt dışı ekonominin büyümesi gibi dolaylı zararlar şeklinde bir kısmı veya tamamı kesin olarak öngörülemeyecek veya mutlak bilgiye ulaşmanın mümkün olamayacağı bileşenler yer almaktadır.



T.C.
ULAŖTIRMA VE ALTYAPI BAKANLIĐI
Strateji GeliŖtirme BaŖkanlıĐı

Bu konuda gerekleŖtirilen farklı alıŖmalarda yayınlanan ekonomik maliyete iliŖkin rakamlar birbirinden ok farklı sonular ortaya koyabilmektedir. Dolayısı ile belirli varsayımlar zerinden ulaŖılan bu tr alıŖmaların sonularında bir kesinlik bulunmamaktadır.

Ayrıca, elektronik haberleŖme sektrnde faaliyet gsteren iŖletmeciler tarafından USOM'a raporlanan siber saldırı sayısı 2015 yılında 1.489, 2016 yılında 8.625, 2017 yılında 99.600 ve 2018 yılında 72.975 olarak gerekleŖmiŖ olup, bu saldırıların %95'inden fazlasını daĐıtık servis dıŖı bırakma (DDoS) ve oltalama (Phishing) saldırıları oluŖturmaktadır. Saldırıların byk oĐunluĐunda elektronik haberleŖme, enerji, bankacılık, saĐlık, ulaŖtırma gibi kritik sektrlerde faaliyet gsteren kurum ve kuruluŖlar hedef alınmaktadır.

Oltalama amacıyla kullanılan zararlı baĐlantılar gerek USOM'un kendi analizleri gerekse eŖitli paydaŖlardan gelen ihbar ve bildirimler zerinden tespit edilmekte ve sz konusu zararlı baĐlantılara eriŖim, 5809 sayılı Elektronik HaberleŖme Kanunu ile verilen yetkiler erevesinde elektronik haberleŖme sektrnde faaliyet gstermekte olan iŖletmeciler vasıtasıyla altyapı seviyesinde engellenmektedir. Hali hazırda USOM tarafından, siber saldırılarda kullanıldıĐı tespit edilen 38.000'e yakın zararlı baĐlantı (alan adı, IP veya URL) bu kapsamda engellenmiŖ olup, bunlardan yaklaşık 19.000 tanesi oltalama amacıyla kullanılan zararlı baĐlantılardan oluŖmaktadır.

Son bir ay ierisinde ise oltalama faaliyetinde kullanıldıĐı tespit edilen zararlı baĐlantılara ynelik olarak lkemizden toplam 6.642.207 adet baĐlantı isteĐi tespit edilmiŖtir. USOM koordinasyonunda iŖletmeciler tarafından altyapı seviyesinde alınan nlemler sonucunda bu baĐlantı istekleri engellenmiŖ ve vatandaŖlarımızın zarar grmeleri nlenmiŖtir.

