



T.C.
ULAŞTIRMA VE ALTYAPI BAKANLIĞI
Strateji Geliştirme Başkanlığı

7/7879
GK 85

Sayı : 44697349-610.01/14008
Konu : Ankara Milletvekili
Sayın Levent GÖK'ün
yazılı soru önergesi

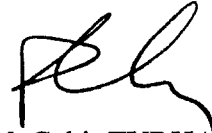
20-02-2019

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

İlgi: 24.01.2019 tarihli ve 43452547-120.07-E.418848 sayılı yazınız.

Ankara Milletvekili Sayın Levent GÖK'ün 7/7879 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 10 16

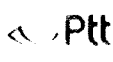
Faks: 213 07 60

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

İnternet Adresi: www.uab.gov.tr

Ayrıntılı bilgi alınacak kişi:
C. Tanfer TEMİZKAN

Şef





T.C.
ULAŞTIRMA VE ALTYAPI BAKANLIĞI
Strateji Geliştirme Başkanlığı

**ANKARA MİLLETVEKİLİ SAYIN LEVENT GÖK'ÜN
7/7879 ESAS SAYILI YAZILI SORU ÖNERGESİNİN CEVABI**

Ülkemizin siber güvenliğine karşı çıkan tehditlerin belirlenmesi, muhtemel saldırı ve olayların etkilerinin azaltılması veya ortadan kaldırılmasına yönelik önlemlerin geliştirilmesi ve belirlenen aktörlerle paylaşılması amacıyla Ulusal Siber Olaylara Müdahale Merkezi (USOM) 2013 yılında Bilgi Teknolojileri ve İletişim Kurumu (BTK) bünyesinde kurulmuştur.

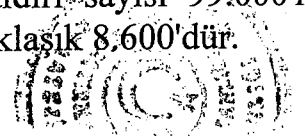
Oluşturulan Ulusal Siber Güvenlik Organizasyonu kapsamında USOM, kamu kurum ve kuruluşları ile kritik altyapı sektörlerinde Kurumsal ve Sektörel Siber Olaylara Müdahale Ekipleri (SOMELER) siber olaylara müdahale konusunda 7/24 esasına göre koordineli biçimde görev yapmaktadır.

Günümüz itibarıyla, Bakanlığımızca hazırlanan Kurumsal ve Sektörel SOME Kurulum ve Yönetim Rehberleri doğrultusunda oluşturularak faaliyet gösteren 1086 adet Kurumsal ve 14 adet Sektörel SOME bulunmaktadır. USOM tarafından siber olaylara ve tehditlere ilişkin alarm, duyuru, farkındalık faaliyetleri yürütülmekte, web sitesi ve diğer kanallar üzerinden güvenlik bildirimleri yayınlamak kurumlara bildirilmektedir.

Bu kapsamda, güvenlik açıklıklarının kapatılmasına yönelik aksiyonların ilgili kurum ve kuruluşlara iletilmesi USOM tarafından sürekli ve rutin bir faaliyet olarak sürdürülmektedir. Bu çerçevede, kurum ve kuruluşlara kritik ve acil olarak ele alınması gereken tedbirlerle birlikte 2018 yılı içerisinde yaklaşık 3.000 adet, 2017 yılında ise yaklaşık 1.550 adet siber güvenlik bildirimi gönderilmiştir.

Öte yandan 2018 yılı içerisinde zararlı yazılımlarda ve oltalama amacıyla kullanılan 25.000'in üzerinde zararlı bağlantı (URL, IP, domain) tespit edilerek kontrolleri yapılmış ve altyapı seviyesinde erişimi engellenmiştir. Bu sayı 2017 yılında yaklaşık 7.800 iken 2016 ve öncesinde ise yaklaşık 500 olarak gerçekleşmiştir.

Dünya genelinde olduğu gibi ülkemize yönelik siber saldırılar da çoğunlukla elektronik haberleşme, enerji, bankacılık, sağlık gibi kritik sektörleri hedef almaktadır. 2018 yılı içerisinde elektronik haberleşme sektöründe faaliyet gösteren işletmeciler tarafından USOM'a raporlanan toplam siber saldırı sayısı yaklaşık 73.000'dir. Ayrıca, 2017 yılında raporlanan toplam siber saldırı sayısı 99.000'in üzerindeyken, 2016 yılında raporlanan siber saldırı sayısı ise yaklaşık 8.600'dür.





T.C.
ULAŞTIRMA VE ALTYAPI BAKANLIĞI
Strateji Geliştirme Başkanlığı

Diğer taraftan, Bakanlığımız koordinasyonunda hazırlanarak yürürlüğe giren 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planının gerçekleştirilmesi çalışmaları sorumlu kurumlar tarafından sürdürülmektedir. Eylem Planı ile siber güvenlik ekosisteminin geliştirilmesi amaçlanmaktadır. Bu kapsamda gerçekleştirilecek çalışmalarla ilgili bazı eylem maddeleri ve hedeflenen kazanımlar aşağıda belirtilmiştir.

- Siber güvenlikle ilgili yerli teknoloji ve ürünlerin desteklenmesi eylem maddesi ile siber güvenlik kapsamında yerli Ar-Ge kapasitesinin geliştirilmesi ile kullanıcıların BT ürünlerine duyduğu güvenin artırılması, yabancı ürünlerden kaynaklanan risklerin işlenmesi, bakım sürecinde avantaj sağlanması,
- Pardus'un yaygınlaştırılması eylem maddesi ile bilgi sistemlerinin yabancı işletim sistemlerinde bulunabilecek arka kapı vb. açıklıklardan arındırılması;
- Kritik siber güvenlik teknolojilerinin kazanımı eylem maddesi ile kazanılması gereken siber güvenlik teknoloji alanlarında geliştirme çalışmaları yapılması ve siber güvenlik risklerinin yerli/güvenilir teknoloji kullanılarak bertaraf edilmesi.

Eylem planı kapsamında ülkemizde güçlü İnternet Değişim Noktası (İDN) kurma çalışmaları da sürdürülmektedir. İDN ile kaynağı ve hedefi yurtiçi olan internet trafiğinin yurtdışından dolaşması önlenecek, siber güvenlik zafiyetlerinin önüne geçilip ülkemizin siber güvenlik seviyesi bir üst seviyeye çıkarılacaktır.

Öte yandan, kamu kurum ve kuruluşları arasında veri iletişiminin internete kapalı ve daha güvenli bir ağ üzerinden yapılması amacıyla 2015 yılında Kamu Sanal Ağı (KamuNet) hayata geçirilmiştir. 21 Haziran 2017 tarihinde yayımlanan KamuNet Tebliği ile kurumların KamuNet'e dâhil olması için asgari gereksinimler belirlenmiştir.

Bu asgari gereksinimler ile kamu kurumları siber saldırılara karşı daha dayanıklı hale getirilmiştir. Şu an 134 kurumumuz KamuNet'e dâhil edilmiş olup kalan kurumlarımızın da KamuNet'e dâhil olma çalışmaları devam etmektedir.

