



T.C.
ULAŞTIRMA VE ALTYAPI BAKANLIĞI
Strateji Geliştirme Başkanlığı

7/2087
Ek 16

Sayı : 44697349-610.01/94775
Konu : İstanbul Milletvekili
Sayın Mustafa Sezgin TANRIKULU'nun
yazılı soru önergesi

17 Aralık 2018

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

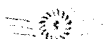
İlgi: 08.10.2018 tarihli ve 43452547-120.07-E.357734 sayılı yazınız.

İstanbul Milletvekili Sayın Mustafa Sezgin TANRIKULU'nun 7/2087 esas sayılı yazılı soru önergesinin cevabı ilişikte sunulmaktadır.

Bilgilerinize arz ederim.

M. Cahit TURHAN
Bakan

EK :1) Cevap formu (7 Sayfa)



T.C. TÜRKİYE BÜYÜK MİLLET MECLİSİ



T.C.
ULAŖTIRMA VE ALTYAPI BAKANLIđI
Strateji GeliŖtirme BaŖkanlıđı

İSTANBUL MİLLETVEKİLİ
SAYIN MUSTAFA SEZGİN TANRIKULU'NUN
7/2087 ESAS SAYILI YAZILI SORU ÖNERGESİ VE CEVABI

Birçok ülkenin ulusal güvenlik tehditleri arasında siber saldırılar yer almaktadır. Bilgisayar korsanları (hacker) tarafından kamu kuruluşlarının resmi internet sayfaları ve veri tabanları saldırıya uğramakta, bu saldırılar sonucu internet siteleri çökertilip, kamu kurumuna ait verilere erişilmektedir. Bu bağlamda;

SORULAR:

1.Bakanlığınıza bađlı kurum ve kuruluşlar bilgisayar korsanlarınca (hacker) saldırıya uğramış mıdır? Bu saldırılar ne zaman ve hangi bađlı kuruma yapılmıştır?

2.Siber saldırıya uğrayan Bakanlığınıza bađlı kurum ve kuruluşlardan çalınan belgeler var mıdır? Var ise sayısı nedir? Bu belgeler arasında çok gizli ve gizli ibareli belge bulunmakta mıdır?

3.Siber saldırıya uğrayan Bakanlığınıza bađlı kurum ve kuruluşlardan çalınan iç yazışma belgeleri, tayin-terfi yazıları, soruşturma rapor ve belgeleri bulunmakta mıdır? Açığa çıkan belgeler nelerdir?

4.Siber saldırıya uğrayan Bakanlığınıza bađlı kurum ve kuruluşlarda, bilgisayar korsanlarına karşı önleyici tedbirler alınmış mıdır? Bu tedbirler ve saldırıların kuruma maliyeti nedir?

CEVAPLAR:

Bakanlığımızın siber güvenliğe ilişkin görev ve yetkileri 2012/3842 sayılı Bakanlar Kurulu Kararı ve 5809 sayılı Elektronik Haberleşme Kanunu ile belirlenmiştir. Bu çerçevede yürütölen çalışmalarla kamu kurum ve kuruluşlarınca bilişim altyapılarının güvenliğinin sağlanmasına yönelik tedbirlerin alınması ve bilgi iletişim teknolojilerine ilişkin kritik altyapıların uymaları gereken usul ve esasların düzenlenmesi gibi iş ve işlemler Bakanlığımızca yapılmaktadır.

Bu kapsamda Bakanlığımızca alınan tedbirler aşağıda verilmiştir:

- Bakanlığımızca iki adet strateji ve eylem planı hazırlanmıştır. Bunlardan ilki olan "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" kapsamındaki çalışmalar önemli ölçüde tamamlanmış olup gelişen teknolojiler ve deđişen şartlar doğrultusunda strateji ve eylem planımız güncellenmiştir. Bu kapsamda 10 Şubat 2016 tarihli Siber Güvenlik Kurulunda onaylanan "2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" yürürlükte olup eylem maddelerinin uygulanması konusundaki çalışmalar, sorumlu kurumlar koordinasyonunda devam etmektedir.



T.C.
ULAŞTIRMA VE ALTYAPI BAKANLIĞI
Strateji Geliştirme Başkanlığı

- Ülkemizin siber güvenliğine karşı siber ortamda ortaya 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.

- USOM; kamu kurum ve kuruluşları ile kritik altyapı işleten özel sektör kuruluşlarında kurularak sayıları 1060'a ulaşan Kurumsal ve Sektörel SOME'lerle (Siber Olaylara Müdahale Ekipleri) koordineli olarak siber olaylara müdahale konusunda 7x24 esasına göre görev yapmaktadır. Siber olaylara ve tehditlere ilişkin alarm, duyuru, farkındalık faaliyetleri yürütmekte, web sitesi ve diğer kanallar üzerinden güvenlik bildirimleri yayınlarak kurumlara bildirmektedir.

-Her geçen gün artan siber tehditlere karşı kamu kurum ve kuruluşları arasındaki veri iletişiminin güvenli bir şekilde sağlanabilmesi amacıyla Siber Güvenlik Kurulu kararları doğrultusunda KamuNet (Kamu Sanal Ağı) projesi hayata geçirilmiştir. İnternete kapalı bu sanal ağ ile veri iletişimde standart ve ortak uygulamalar için güvenli bir altyapı oluşturulmuştur. Projenin en kısa süre içerisinde tamamlanarak kamu kurum ve kuruluşlarının KamuNet ağına dâhil olması amacıyla 2016/28 sayılı KamuNet'e ilişkin Başbakanlık Genelgesi, KamuNet'e bağlantı için kurumların karşılaması gereken asgari gereklilikler ile denetlenmelerine ilişkin usul ve esasları belirten 21 Haziran 2017 tarihli KamuNet Tebliği yayımlanmıştır.

-Kurumsal ve Sektörel SOME Kurulum ve Yönetim Rehberleri olmak üzere Bakanlığımızca siber güvenliğe yönelik rehberler hazırlanmıştır. Bu rehberlerle kurum ve kuruluşlara siber güvenlik açısından yol gösterici olunması amaçlanmaktadır.

-Uluslararası işbirliğinin güçlendirilmesi kapsamında başta Birleşmiş Milletler, Kuzey Atlantik Anlaşması Örgütü (NATO) ve Avrupa Güvenlik ve İşbirliği Teşkilatı (AGİT), olmak üzere uluslararası organizasyonların çalışmalarına katılım ve katkı sağlanmaktadır.

Ulusal siber güvenliğin sağlanmasına yönelik görevler 5809 sayılı Kanuna eklenen hükümler kapsamında 17 Ağustos 2016 tarihinden itibaren Bilgi Teknolojileri ve İletişim Kurumu Başkanlığınca yürütülmekte olup bu tarihten itibaren ülkemizi hedef alan siber tehditlerin USOM koordinasyonunda bertaraf edilmesi sağlanmıştır.





T.C.
ULAŞTIRMA VE ALTYAPI BAKANLIĞI
Strateji Geliştirme Başkanlığı

Bu kapsamda, güvenlik açıklıklarının kapatılmasına yönelik aksiyonların ilgili kurum ve kuruluşlara iletilmesi USOM tarafından sürekli ve rutin bir faaliyet olarak sürdürülmektedir. Bu çerçevede, 2018 yılı içerisinde kurum ve kuruluşlara kritik ve acil olarak ele alınması gereken tedbirlerle birlikte 01 Ekim tarihi itibarıyla 2476 adet siber güvenlik bildirimi gönderilmiştir. Öte yandan 01 Ekim tarihi itibarıyla 2018 yılı içerisinde zararlı yazılımlarda ve oltalama amacıyla kullanılan 18039 zararlı bağlantı (URL, IP, domain) tespit edilerek kontrolleri yapılmış ve altyapı seviyesinde erişimi engellenmiştir.

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 gün, 24 saat izlenmesi olmak üzere zafiyet tarama ve tespit çalışmaları sürdürülmektedir. Ayrıca, bünyesindeki siber güvenlik uzmanları tarafından siber tehdit analiz, tespit ve önleme faaliyetleri 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, Bakanlığımız ile bağlı, ilgili, ilişkili kurum ve kuruluşları tarafından kurumsal sitelerine yapılabilecek siber saldırıları önleme kapsamında yapılan çalışmalar kuruluşlarımız itibarıyla aşağıda verilmiştir.

BAKANLIĞIMIZ MERKEZ TEŞKİLATI:

2010 yılı 1 adet DDOS saldırısı (aşırı talep yapılarak sunucunun yoğunluğa cevap verememesi) (Bakanlık web sayfası), 2013 yılı Ocak ayında bilgilendirme yayını yapan 1 adet web sunucu (yazılım kodundaki bir açıklık sebebiyle) saldırıya uğramıştır. Diğer yıllarda tespit edilebilen önemli bir hacker saldırısı gözlemlenmemiştir. Bakanlığımız sistemlerinden herhangi bir belgenin çalındığına dair bir bulgu gözlemlenmemiş olup gizli ve çok gizli belgeler evrak sistemlerine kayıt edilmemektedir.

Siber Saldırılara Karşı Alınan Önlemler:

- Bakanlığımız kullanıcı bilgisayarlarında antivirüs yazılımları kullanılmaktadır.
- Bakanlığımız güvenlik duvarlarında çeşitli güvenlik önlemleri arttırılmıştır.
- Sunucu sistemlerindeki güvenlik kontrolleri sürekli yapılmaktadır.
- Herhangi bir saldırı anında saldırıların sunuculara gelmeden önlenmesi amacıyla İnternet Servis Sağlayıcısından DDOS ve IPS Güvenlik Hizmeti alınmaktadır.
- 2015 yılından bu yana bilişim sistemleri güvenliği için toplam 4.329.041,00 TL harcama yapılmıştır.





T.C.
ULAŞTIRMA VE ALTYAPI BAKANLIĞI
Strateji Geliştirme Başkanlığı

TCDD İşletmesi Genel Müdürlüğünde verinin tutulduğu veri tabanı sistemlerinin önünde veri tabanı firewall hizmeti veren ürünü bulunmakta ve erişim bilgileri loglanmaktadır. Veriler lokal sistemlerde tutulmakta ve sadece yetkili kişilerin erişimine izin verilmektedir.

Saldırı sistemlerine karşı, Kurumsal SOME (Siber Olaylara Müdahale Ekibi) personelimizin eğitim ve tecrübenmesine azami özen gösterilmektedir. Bu hizmeti veren diğer kuruluşlarla bağlantılı çalışmakta ve yeni saldırı türlerinden anında haberdar olunmaktadır.

Siber saldırıların önlenmesine yönelik tedbirler kapsamında; Lisanslarının güncellenmesi, bakımlarının yapılması ve sistemlerin 7/24 izlenmesi için 1 yılına toplam 4.970.000,00 TL bedelle hizmet alımı yapılmıştır.

TCDD TAŞIMACILIK A.Ş. GENEL MÜDÜRLÜĞÜ:

TCDD Taşımacılık A.Ş. Genel Müdürlüğünün fiilen faaliyetlerine başladığı 01.01.2017 tarihinden itibaren web sitesine ve bilişim sistemlerine herhangi bir siber saldırı gerçekleşmemiştir. TCDD Taşımacılık A.Ş. Genel Müdürlüğüne ait network ve siber güvenlik hizmetleri, TCDD Genel Müdürlüğü tarafından sağlanmaktadır. Bu kapsamda prezentasyon ve zaafiyet testleri düzenli olarak yapılmaktadır. Diğer yazılım uygulamaları için kaynak kod analizi alınmış ve karşılığında 64.000 TL+KDV ücret ödenmiştir.

TÜDEMSAŞ GENEL MÜDÜRLÜĞÜ:

30.03.2015 ve 08.06.2018 tarihlerinde kurum personelinin kullandığı masaüstü bilgisayarlara kriptovirüs bulaşmış olup, virüs ağda yayılmadan temizlenmiş, herhangi bir sistem ve veritabanı dosyası zarar görmemiştir. Herhangi bir belge ve yazışma çalınmamıştır.

Kurum bünyesinde bulunan sunucu ve istemcilerin güvenlik güncellemeleri yapılmakta, güncel virüs programı kullanılmakta, ağ trafiği güvenlik duvarı tarafından kontrol edilmektedir.

Belirli zaman aralıklarında sızma testleri yaptırılarak sistemde tespit edilen güvenlik açıklarına karşı tedbirler alınmaktadır. Ayrıca USOM tarafından gönderilen uyarı ve farkındalık oluşturma amaçlı mailler personele iletilmektedir. Bu tedbirlerin maliyeti (Güvenlik duvarı ve virüs programı) toplam 132.393,89-TL'dir.

TÜLOMSAŞ GENEL MÜDÜRLÜĞÜ:

TÜLOMSAŞ Genel Müdürlüğünün sistemleri bilgisayar korsanları tarafından herhangi bir saldırıya uğramamıştır. Dijital evraklar TÜLOMSAŞ Genel Müdürlüğünün iç ağında bulunmakta olup, dışarıdan bilgisayar korsanları tarafından erişilmesi mümkün değildir. Bu kapsamda tüm önlemler alınmakta ve faaliyetleri Bakanlığımız ile koordineli olarak yürütülmekte olup alınmış olan tedbirlerin maliyeti toplam 216.000 TL'dir.



T.C.
ULAŞTIRMA VE ALTYAPI BAKANLIĞI
Strateji Geliştirme Başkanlığı

TÜVASAŞ GENEL MÜDÜRLÜĞÜ:

TÜVASAŞ Genel Müdürlüğünün sistemleri bilgisayar korsanları tarafından herhangi bir saldırıya uğramamıştır. Siber saldırılara karşı önleyici tedbirlerin maliyeti toplam yaklaşık 571.000 TL'dir.

PTT A.Ş. GENEL MÜDÜRLÜĞÜ:

PTT A.Ş. Genel Müdürlüğüne ait sistemlerde servis dışı bırakmaya yönelik DDOS saldırıları hariç siber saldırı tespit edilmemiştir.

Siber saldırılardan korumak amacıyla; Servis sağlayıcıdan DOS, DDOS (Servis Dışı Bırakma Saldırısı) hizmeti, Local'de DOS, DDOS cihazı konumlandırılması, APT : Tehdit önleme platformu, IPS: Saldırı tespit ve engelleme sistemi, Antivirüs: Zararlı yazılım engelleme sistemi ve Altı aylık dönemler halinde sızma testleri yapılmaktadır. Ayrıca, otomotize toollar ile oluşabilecek güvenlik açıklıkları tespit edilmektedir. Bahsi geçen önlemlerin yıllık maliyeti KDV dahil yaklaşık 1.045.000 TL'dir.

TÜRKSAT A.Ş. GENEL MÜDÜRLÜĞÜ:

TÜRKSAT, 2008 yılından itibaren geliştirme ve işletmesini gerçekleştirdiği e-Devlet Kapısı portalı (www.turkiye.gov.tr) ve TÜRKSAT bilişim altyapı ve sistemleri ile ilgili tüm faaliyetleri uluslararası kabul görmüş güvenlik kriterlerine uygun şekilde yapmaktadır.

e-Devlet Kapısı, kamu hizmetlerine tek bir noktadan erişim imkânı sağlayan internet sitesidir. E-Devlet Kapısının amacı, tek bir adres üzerinden ve şifre, elektronik imza, mobil imza gibi kimlik doğrulama sistemleri ile güvenli bir şekilde kamu hizmetlerinin vatandaşlarımıza sunulmasıdır. TÜRKSAT A.Ş. Genel Müdürlüğü olarak hem TÜRKSAT'ın bilişim altyapısının hem de E-Devlet Kapısı'nın, oluşabilecek siber güvenlik risklerine karşı gerekli tedbirleri almak için ISO 27001 Bilgi Güvenliği Yönetim Sistemi standardına uygun işletilmesi sağlanmaktadır. Standardın gereği olarak tehditleri önceden tespit etmek için belli aralıklarla gözden geçirme toplantıları düzenlenmekte, güvenlik denetimlerinde tespit edilen bulgular ve alınan aksiyonlar görüşülerek gerekli iyileştirmelerin sürekliliği sağlanmaktadır.

Sürekli izleme çerçevesinde hem e-Devlet Kapısı sistemleri hem de TÜRKSAT bilişim altyapı ve sistemleri 7/24 takip edilmektedir. e-Devlet Kapısı ve TÜRKSAT'ın kendi bilişim altyapısı, Kurumsal Bilgi ve Siber Güvenlik Yönetimi Direktörlüğü bünyesindeki sızma testi uzmanları tarafından sürekli test edilmekte, güvenlik operasyon uzmanları siber saldırı ihtimaline karşı her türlü aykırı durum (anomali) incelenmektedir. Ayrıca bağımsız bilgi güvenliği firmalarınca yapılan güvenlik ve sızma testleriyle düzenli olarak sınanmakta ve doğrulama testlerinden de başarıyla geçmektedir.



T.C.
ULAŖTIRMA VE ALTYAPI BAKANLIĐI
Strateji GeliŖtirme BaŖkanlıĐı

Yapılan gvenlik testleri ve incelemeleri neticesinde edinilen bilgiler doĐrultusunda gvenlik sistemlerinin srekli gncel kalması saĐlanmakta ve bu gncelleme neticesinde, takip edilen sistemlerde oluŖan risk durumuna gre Ŗpheli grlen eriŖimler geici olarak otomatik bir Ŗekilde engellenmektedir. Ayrıca siber saldırganlar tarafından sahte siteler yapılarak kimlik avlama riskine karŖı alınan siber istihbarat servisleri sayesinde ok hızlı mdahale edilerek USOM'dan eriŖimin engellenmesi ve servis saĐlayıcılarda da gerekli yayından kaldırma (abuse) sreci baŖlatılmaktadır.

Bu erevede;

TRK SAT ve e-Devlet Kapısı (turkiye.gov.tr) sitesine ynelik pek ok siber saldırıya ynelik (internette bulunan eŖitli aralarla tarama, sızma testi vb.) denemeler yapıldıĐı Siber gvenlik Ekiplerince tespit edilmektedir. Bu kapsamda sistemimize ynelik siber saldırganlar tarafından yapılan denemeler baŖarıya ulaŖamamıŖtır. Sahip olduĐumuz saldırı tespit/nleme sistemleri ve uzman ekibimizin srekli takibi sayesinde gerekli engellemeler ve tedbir amalı aksiyonlar alınmaktadır.

Srekli izleme, gncelleme, sıklılaŖtırma ve personellerin farkındalıĐını artırmaya ynelik eĐitimler neticesinde TRK SAT ve e-devlet kapısı (turkiye.gov.tr) sitesinden alınan herhangi bir bilgi/belge/veri sızıntısı tespit edilmemiŖtir.

TRK SAT A.Ŗ. Genel MdrlĐnde siber gvenlik ile ilgili alan uzmanlarından oluŖan baĐımsız bir birim bulunmaktadır. Bu birim siber gvenlik tehditlerine karŖı altyapı ve sistemleri srekli izlemekte, gerekli olan yatırımları tespit ederek hayata gemesini saĐlamaktadır. Bu kapsamda, yapılan yatırım maliyeti yıllık 4.000.000 TL civarındadır.

