

7/42525
SK 142

T.C.
BİLİM, SANAYİ VE TEKNOLOJİ BAKANLIĞI
Basın ve Halkla İlişkiler Müşavirliği

13.08.2014

Sayı : 86782684 - 610 / 142
Konu : Soru Önergeleri

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA
TBMM Ana Bina Bakanlıklar-ANKARA

İlgi: 02/05/2014 tarihli ve 43452547-120.00-176074 sayılı yazı.

Ankara Milletvekili Sayın Aylin NAZLIAKA'nın, "Bakanlığımız ile bağlı, ilgili ve ilişkili kuruluşlarına yapılan siber saldırılarına" ilişkin olarak tarafımdan cevaplandırılmasını istediği (7/42525) esas nolu yazılı soru önergesi ile ilgili cevap ekte tekdin edilmiştir.

Bilgilerinizi ve gereğini arz ederim.


Fikri IŞIK
Bakan

Ek: Soru Önergesi Cevabı (3 Sayfa)

ANKARA MİLLETVEKİLİ SAYIN AYLİN NAZLIAKA’NIN
7/42525 ESAS NOLU YAZILI SORU ÖNERGESİNE İLİŞKİN CEVAPLAR

Günümüzde internet, bilgi ve iletişim sistemlerinin kullanımı yaygınlaşmış, internet bilgi ve erişim sistemleri hemen hemen hayatın her alanına girmiştir. Kamu kurumları başta olmak üzere finansal hizmetlerde, ulaşım, haberleşme, enerji, sağlık gibi sektörlerde bilgi ve iletişim sistemlerini yoğun olarak kullanmaktadır. Kurumsal ya da bireysel verileri ele geçirmek ya da kullanılan bilgi ve iletişim sistemini bozmak için yapılan siber saldırılar, ekonomi ve bilgi güvenliği açısından risk oluşturmaktadır.

Dışişleri, İçişleri, Adalet ve Maliye Bakanlıkları, Emniyet Genel Müdürlüğü, Bilgi Teknolojileri ve İletişim Kurumu başta olmak üzere bütün kamu kurumlarına siber saldırılar yapılmaktadır.

Uzmanlar, internet kullanımıyla ilgili özel sektör değerlendirmelerinde Türk şirketlerinin bilgi ve iletişim teknolojileri kullanım oranının yüzde 40’a ulaştığını belirtmektedir. International Data Corporation’ın (IDC) Mayıs 2012’deki Küresel Korsan Yazılım Kullanımı raporunda; Türkiye’de lisanssız yazılım kullanım oranının yüzde 62 olarak gözükmesi nedeniyle siber korsanların hedefi haline gelme riskini arttırdığını söylemektedir.

Bilişim teknolojilerinin gelişmesiyle birlikte siber güvenlik, siber terörizm, siber suç kavramları politika ve hukuk literatürlerinde yer almaya başlamıştır. Pek çok uluslararası kuruluş ve devlet siber güvenlik stratejileri geliştirmektedir. Bu konuda ülkemizde de gerekli önlemlerin alınması hem ulusal güvenlik hem de ekonomi açısından büyük önem taşımaktadır.

Bu bağlamda;

Soru 1- 2002-2012 döneminde Bakanlığınıza bağlı ilgili ve ilişkili kurum ve kuruluşlara kaç siber saldırı gerçekleştirilmiştir? 2013 yılında bu sayı ne olmuştur? Artış oranı nedir?

Soru 2- Bakanlığınıza bağlı ilgili ve ilişkili kurum ve kuruluşlara siber saldırıların önlenmesi için alınan önlemler nelerdir? Bu önlemler için 2013 yılında ayrılan kaynak miktarı nedir? Bu miktar 2014 yılında ne olmuştur?

Soru 3- Bakanlığınıza bağlı ilgili ve ilişkili kurum ve kuruluşlarda bu konularla ilgili çalışan personel sayısı kaçtır? Bu alanda kurum dışından hizmet alınmakta mıdır? Alınıyorsa ihale tarihi ve bedeli nedir?

Cevap 1-2-3- 2002 – 2012 döneminde Bakanlığınıza yönelik siber saldırı gerçekleşmemiştir. 2013 yılında da herhangi bir siber saldırı olmamıştır. Bakanlığımızda siber saldırıların önlenmesi için rutin kontroller ve testler yapılmaktadır. Bu önlemler için 2013 yılında ayrılan kaynak 43.000 TL + KDV’dir. Bu çerçevede 2013 yılında kurum dışından hizmet alınmış olup ihale tarihi Nisan 2013’tür. Bakanlığımızda konu ile ilgili bir personel çalışmaktadır.

Türk Standardları Enstitüsü (TSE):

Türk Standardları Enstitüsü'nde 2002-2013 yılları arasında Kurum uygulamalarına toplam 2 adet saldırı olmuştur. 2013 yılında ise 1 adet saldırı olduğu ve bu saldırının da başarıyla engellendiği tespit edilmiştir. Siber saldırıların önlenmesi adına TSE uygulamalarına periyodik olarak sızma testleri yapılmakta, saldırı tespit ve önleme sistemleri ve çeşitli gateway, antivirüs, anti spam ve firewall cihazları kullanılmaktadır. Bu iş için 2013 yılında ayrılan kaynak 200.000 TL iken 2014 yılında 500.000 TL civarında bir kaynak öngörülmektedir. Kurumun Bilgi İşlem Dairesi Başkanlığında Sistem ve Veritabanı Şefliği bünyesinden 4 Bilgisayar mühendisi tarafından bu işlemler yürütülmektedir. Dış kaynak ise sızma testlerinde kullanılmaktadır.

Küçük ve Orta Ölçekli İşletmeleri Geliştirme ve Destekleme İdaresi (KOSGEB):

KOSGEB web sitesi bahse konu dönemde 2 kez saldırıya uğramıştır. Muhtemel siber saldırıları önlemek amacıyla KOSGEB bünyesinde kurulu sistemler aşağıda sıralanmıştır:

- 1) Yedekli bir yapıda çalışan Güvenlik Duvarı, IPS, Dos/DDoS saldırı önleme, Malware zararlıları koruma sistemi,
- 2) Bilgisayar virus saldırılarına karşı merkezi olarak yönetilen son kullanıcı antivirüs programı,
- 3) İstenmeyen e-postaları engellemeye yönelik Antispam sistemi,
- 4) Zararlı web içeriklerinin, web sayfalarından bulaşabilecek virüslerin ve kötü amaçlı yazılımların engellenmesi için içerik filtreleme ve proxy sistemi,
- 5) Kablosuz ağ güvenliği için gerekli sistemler.

Bunların yanı sıra Bilgi İşlem network sorumlu personeline belirli aralıklarla ağ ve güvenlik eğitimleri aldırılmaktadır.

Bu önlemler için 2013 yılında ayrılan kaynak miktarı 200.000 TL olup bu miktar 2014 yılında 250.000 TL'ye yükseltilmiştir.

KOSGEB'de bu konularla ilgili olarak 3 kişi görevlidir. Bu alanda kurum dışından bir hizmet alınmamaktadır.

Türk Patent Enstitüsü (TPE):

2002-2012 döneminde Türk Patent Enstitüsüne her hangi bir siber saldırı gerçekleştirilmemiştir. Enstitüde dış ve iç kullanıcılardan kaynaklanabilecek tehditler için güvenlik duvarı (firewall) ve antivirüs uygulamaları mevcuttur. Dış tehditlere karşı ve uygulama sunucuları için güvenlik duvarı (firewall) kuralları ve internet erişim kuralları yazılmaktadır. Enstitüde kullanıcılara ilişkin yetkiler ve kısıtlar personelin görev alanları ile ilişkili olarak belirlenmektedir. Öte yandan TPE 2013 yılında penetrasyon testi hizmeti satın almıştır. Söz konusu hizmet alımının ihale bedeli 39.438 TL'dir. 2014 yılı için bugüne kadar kaynak kullanımı olmamıştır. Enstitüde konuyla ilgili 2 personel görev yapmaktadır.

Kullanılan güvenlik ürünlerine ilişkin olarak destek paket hizmeti alınmaktadır. Güvenlik duvarı (firewall) hizmetinin ihale tarihi Mart 2014, ihale bedeli ise 37.690 TL'dir.

Şeker Kurumu:

Şeker Kurumuna 2002-2013 seneleri içinde herhangi bir siber saldırı gerçekleşmemiştir. Kurumun bilgi işlem sistemlerine yapılacak saldırıları önlemek için firewall cihazı kullanılmakta olup bu cihaz 2012 yılında 501 TL bedel ile temin edilmiştir. Kurumda siber saldırılar ile mücadele için ayrıca personel istihdam edilmemekte olup, bilgi işlem konuları ile ilgili bir personel görevlendirilmiş bulunmakta ve hizmet alımı yolu ile de bir adet bilgi işlem personeli istihdam edilmektedir. Ayrıca bilgisayar sistemleri bakım ve onarım kapsamında bir firma ile sözleşme imzalanmış, bu işin alımı Şubat 2014 tarihinde yıllık 6.900 TL bedel ile gerçekleşmiştir.

Türkiye Bilimler Akademisi (TÜBA):

TÜBA'ya 2002-2012 dönemleri arasında herhangi bir siber saldırı olmamıştır. 2013 yılı içerisinde ise bir kez saldırıya maruz kalınmıştır. Saldırı anında da anlık müdahale yapılmıştır. Kullanılan yazılımların hepsi lisanslıdır. TÜBA'da siber saldırılarına karşı donanımsal firewall (güvenlik duvarı) kullanılmakla birlikte yazılımsal olarak ek programlarla sistemler devamlı kontrol edilerek açık portlar ve zararlı e-postalar tespit edilerek anında kapatılmaktadır. 2013 yılında bu iş için ayrılan kaynak 44.000 TL'dir. 2014 yılında herhangi bir ödenek tahsis edilmemiştir. Bu alanda çalışan personel sayısı bir kişidir. Hizmet alımı için (Penetration Testing uygulaması gibi) ise herhangi bir firmadan satın alım yapılmamıştır.