



T.C.
ULAŞTIRMA VE ALTYAPI BAKANLIĞI
Strateji Geliştirme Başkanlığı

Sayı : 44697349-610.01/ 76080
Konu : Ankara Milletvekili
Sayın Levent GÖK'ün
yazılı soru önergesi

11 Ekim 2018

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

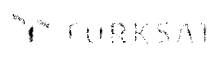
İlgi: 20.09.2018 tarihli ve 43452547-120.07-E.354429 sayılı yazınız.

Ankara Milletvekili Sayın Levent GÖK'ün 7/1753 esas sayılı yazılı soru önergesinin cevabı
ilişikte sunulmaktadır.

Bilgilerinize arz ederim.

M. Cahit TURHAN
Bakan

EK :1) Cevap formu (3 Sayfa)





T.C.
ULAŞTIRMA VE ALTYAPI BAKANLIĞI
Strateji Geliştirme Başkanlığı

**ANKARA MİLLETVEKİLİ SAYIN LEVENT GÖK'ÜN
7/1753 ESAS SAYILI YAZILI SORU ÖNERGESİ VE CEVABI**

Ulusal ve uluslararası kurumlara güvenlik hizmeti veren bir Türk şirketi tarafından e-Devlet uygulamasının da için de bulunduğu 94 adet gov.tr uzantılı resmi internet sitesi güvenlik testinden geçirilmiştir. Güvenlik testinde 94 siteden sadece 18 tanesinin güvenli olduğu saptanmış, sitelerin 1'inde kritik, 43'ünde yüksek, 122'sinde ise orta seviyede 642 farklı güvenlik sorunu gözlemlenmiştir. Sitelerden 31'inde sızma ve saldırılara karşı önemli seviyede güvenlik açığı gözlenirken, 40 sitede ise orta seviye güvenlik problemleri belirlenmiştir. Bir site de yüksek seviyede güvenlik riski içermektedir. Testten geçirilen 94 siteden sadece 26'sı varsayılan bağlantı şekli olarak güvenli bağlantı kullanırken, 68 sitenin bağlantısı ise güvensiz. Test sonuçlarına göre 32'si acil olmak üzere toplam 72 sitenin güvenlik yapısının sızıntılara karşı gözden geçirilmesi gerektiği ortaya çıkmıştır.

Milyonlarca yurttaşımızın ve devlet bilgilerinin risk altında olduğunu gözler önüne seren rapor BTK'ya sunulmuş ve çalışmanın dikkate alınacağı cevabı alınmıştır. Yıllardır hizmet veren kamusal internet sitelerinin bugüne kadar kapsamlı bir güvenlik testinden geçirilmemiş olması Türkiye'nin küresel siber dünyada savunmasız bırakıldığı anlamına gelmektedir.

Bu bilgiler ışığında:

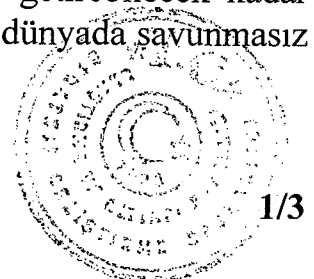
SORULAR:

1) Sözü geçen güvenlik testleri stratejik önem taşıyan kamusal sitelere neden bugüne kadar uygulanmamıştır?

2) 2007 - 2018 yılları arasında kamusal internet siteleri kaç kere saldırıya uğramıştır? Bu saldırılarda devlete ait bilgilerde yaşanan kayıpları ve çalınan vatandaşlık bilgilerini açıklar mısınız?

3) 2007 - 2018 yılları arasında kamusal internet sitelerine yapılan saldırılar sebebiyle sözü geçen siteler toplamda kaç saat kullanım dışı kalmıştır?

4) Günümüzde bilgi depolama, bürokratik işlemler ve vatandaş-devlet ilişkileri ağırlıklı olarak elektronik ağlar üzerinden sağlanmaktadır. Sözü geçen ağlarda yaşanacak güvenlik açıkları bütün bir ülkeyi savunmasız hale getirebilecek kadar büyük tehlikelere sebebiyet verebilmekteyken Türkiye'nin siber dünyada savunmasız bırakılmasını doğru buluyor musunuz?





T.C.
ULAŞTIRMA VE ALTYAPI BAKANLIĞI
Strateji Geliştirme Başkanlığı

CEVAPLAR:

Ulusal Siber Olaylara Müdahale Merkezi (USOM), 2013 yılında kurulmuş olup siber tehditleri önlemek amacıyla alarm, uyarı ve duyuru faaliyetleri yürütmek, kritik durumlarda yerinde müdahale ekipleriyle olayın kontrolünü ele almak ve siber olaylara müdahalede ulusal koordinasyonu sağlamak amacıyla faaliyetlerini sürdürmektedir. Ayrıca, haftanın yedi günü ve kesintisiz olarak, ülkemizdeki kurum ve kuruluşların internete açık kaynaklarında açıklık ya da zafiyet incelemesi gerçekleştirilmektedir. İnternetin canlı doğası gereği, internete açık kaynaklarda meydana gelen değişiklikler veya üretici ve geliştiricilerin ürünlerinde sonradan çıkan güvenlik açıklıkları söz konusu olabilmektedir.

USOM faaliyetleri kapsamında, siber tehdit istihbaratı üretimi çerçevesinde kendi testleri sonucunda zafiyetlere ilişkin bilgiler tespit ettiği gibi ulusal ve uluslararası birçok farklı kaynaktan işbirlikleri kapsamında buna yönelik bilgiler de toplamaktadır.

USOM'a gelen zafiyet bilgileri, gerekli incelemelerden geçirilmek ve işlemlere tabi tutulmak suretiyle teyit edilmektedir. İlgili haberde adı geçen firma çalışanı tarafından yapılan testler de söz konusu haberden önce USOM girişiyle ilgili kişi ile koordine edilerek elde edilmiştir. Bu bilgi ve belgeler USOM bünyesinde gerekli teyit mekanizmalarından geçirilerek aynı gün içerisinde alınması gerekli detaylı aksiyonlarla birlikte ilgili kurum ve kuruluşlarla paylaşılmış ve olabilecek güvenlik açıklarının kapatılması takip edilmiştir.

Ayrıca soru önergesinde belirtilen söz konusu bulgularda sürekli bir bilgi ifşasına neden olabilecek türden bir açıklık bulunmamakta ve yine bahis konusu raporda, e-Devlet Kapısı uygulamasına ait bir güvenlik açığı bulunduğu dair herhangi bir bulgu da yer almamaktadır.

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

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 2.380 adet siber güvenlik bildirimi gönderilmiştir. Ayrıca, 2018 yılı Eylül ayı itibariyle içerisinde zararlı yazılımlar ve ortalama amacıyla kullanılan 17.590 zararlı bağlantı (URL, IP, domain) tespit edilerek kontrolleri yapılmış ve altyapı seviyesinde erişimi engellenmiştir.



T.C.
ULAŖTIRMA VE ALTYAPI BAKANLIĐI
Strateji GeliŖtirme BaŖkanlıĐı

Siber saldırganların lkemizdeki kamu kurumlarını, zel sektr ve vatandaşlarımızı hedef alarak bu amalarını gerekleŖtirmelerinin nlenmesi iin USOM tarafından, baŖta kritik kamu kurumları ve kritik kamu hizmetlerinin haftanın yedi gn, kesintisiz izlenmesi olmak zere, zafiyet tarama ve tespit alıŖmaları srdrlmektedir.

Ayrıca, bnyesindeki siber gvenlik uzmanları tarafından siber tehdit analiz, tespit ve nleme faaliyetleri de yrtlmektedir. Bu alıŖmalar neticesinde tespit edilen zafiyetler ve zararlı yazılımlara iliŖkin bulgular, alınması gerekli nlemleri de ierecek detaylı aıklamalar ile vakit geirmeksizin ilgili kurum/kuruluŖ ile paylaŖılmakta ve bu kurum/kuruluŖlarca gerekli nlemlerin alınması saĐlanmaktadır.

