

11/30 6-16

T.C.
DIŐIŐLERİ BAKANLIĐI
BİLGİ İŐLEM DAİRESİ BAŐKANLIĐI
(BİLD)

Sayı : 80981219-610-2018/14440719
Konu : Yazılı Soru Önergesi/Dr. M. Sezgin
Tanrikulu/7/1930

08 Ocak 2019

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŐKANLIĐINA

İlgi: TBMM Başkanlığının 08.10.2018 tarih ve 43452547-120.07-E.00000357734 sayılı yazısı.

İstanbul Milletvekili Sayın Dr. M. Sezgin Tanrikulu'nun ilgede kayıtlı 7/1930 sayılı yazılı soru önergesinin yanıtı ilişikte sunulmaktadır.

Saygılarımla arzederim.



Mevlüt ÇAVUŐOĐLU
Dışışleri Bakanı

Ek: Soru Önergesi Yanıt

İSTANBUL MİLLETVEKİLİ MUSTAFA SEZGİN TANRIKULU'NUN YÖNELTTİĞİ 7/1930 NO'LU YAZILI SORU ÖNERGESİNİN YANITI

SORU :

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 sonucunda internet siteleri çökertilip, kamu kurumuna ait verilere erişilmektedir.

Bu bağlamda;

1. Bakanlığınıza bağlı kurum ve kuruluşlar bilgisayar korsanlarınca (hacker) saldırıya uğramış mıdır? Bu saldırılar ne zaman ve hangi bağlı kuruma yapılmıştır?
2. Siber saldırıya uğrayan Bakanlığınıza bağlı 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 bağlı 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 bağlı kurum ve kuruluşlarda, bilgisayar korsanlarına karşı önleyici tedbirler alınmış mıdır? Bu tedbirler ve saldırıların kuruma maliyeti nedir?

YANIT :

Bakanlığımız sürekli olarak siber tehditlere maruz kalmakta, bu tehditler çoğunlukla bilişim sistemlerimizi yavaşlatma amacı gütmekte ve kullanıcı hesaplarına ait parolaları ele geçirmeye yönelik olmakla birlikte, sözkonusu tehditler alınan fiziki, donanımsal ve yazılımsal güvenlik tedbirleri ile zamanında önlenmekte ve bertaraf edilmektedir.

Bakanlığımızda güvenli bilişim ve haberleşme sistemlerine ilişkin kurallar "T.C. Dışişleri Bakanlığı Bilişim Güvenliği Yönergesi" ve "T.C. Dışişleri Bakanlığı Kontrollü Evrak Yönergesi" hükümleri doğrultusunda titizlikle uygulanmakta olup, gizli ve üzeri gizlilik derecesindeki bilgilerin işlenmesinde sözkonusu yönergede belirtilen, özel olarak üretilmiş ve dışarıdan yetkisiz herhangi bir müdahaleye karşı korunan cihaz ve sistemler kullanılmaktadır.

Keza, Bakanlığımızda uygulanmakta olan siber güvenlik tedbirleri Bakanlığımızın bilgi ve belge sistemlerini de kapsamakta olup, herhangi bir resmi belgenin açığa çıktığına dair bilgi bulunmamaktadır.

Bakanlığımızda, siber güvenlik uygulamaları çerçevesinde, "Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev Ve Çalışmalarına Dair Usul Ve Esaslar Hakkında Tebliğ" ve "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" doğrultusunda kurumsal Siber Olaylara Müdahale Ekibi (SOME) oluşturulmuştur. Bakanlığımız kurumsal SOME'si, Bilgi ve İletişim Kurumu Başkanlığı uhdesindeki Ulusal Siber Olaylara Müdahale Merkezi (USOM) ile eşgüdüm halinde görev yapmaktadır. Güvenlik mimarisinin farklı katmanlarına hitap eden

ürünler ve çözümler temin edilmekte, gerekli eğitimler alınmakta, bilgi güvenliğine yönelik kurumsal farkındalık ve standardizasyon çalışmaları yürütülmektedir.