7/25971

T.C.
KALKINMA BAKANLIĞI
Özel Kalem Müdürlüğü

18 EYLÜL 2013

Sayı : 43728771-610.00- 4502
Konu : 7/25971 Esas Sayılı Yazılı Soru Önergesi

ÇOK İVEDİ

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

İlgi: TBMM Kanunlar ve Kararlar Başkanlığının 26.06.2013 tarihli ve 43452547-120.00-130455 sayılı yazısı.

İlgi yazıyla, İstanbul Milletvekili Sayın M. Sezgin TANRIKULU'nun tarafıma tevcih ettiği 7/25971 esas sayılı yazılı soru önergesinin cevaplandırılması talep edilmektedir.

Söz konusu yazılı soru önergesiyle ilgili cevabımız ekte sunulmuştur.

Gereğini arz ederim.

Cevdet YILMAZ
Bakan

EKLER :
1- Soru önergesine ilişkin cevaplar
(2 sayfa)

Adres: Necatibey Cad. No:110/A-06100 Yücetepe-ANKARA
Telefon: +90 (312) 294 50 00 - 294 50 95 - 294 50 97
Faks: +90 (312) 294 69 77
Elektronik Ağ: http://www.kalkinma.gov.tr sozdemir@kalkinma.gov.tr

İSTANBUL MİLLETVEKİLİ SAYIN M. SEZGİN TANRIKULU'NUN YÖNELTTİĞİ 7/25971 ESAS SAYILI YAZILI SORU ÖNERGESİNE YÖNELİK CEVAPLAR

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

Soru 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?

Soru 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?

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

KALKINMA BAKANLIĞI

Cevap 1-4: Bakanlığımıza ait internet sitesi ve sunucularına yönelik 10.06.2011 tarihinde bir adet siber saldırı tespit edilmiştir.Saldırıda herhangi bir belge çalınmamıştır.

Bakanlığımızda siber saldırılara karşı alınan tedbirler aşağıda verilmiştir:

- Güvenlik cihazları konumlandırılmıştır.
- Sızma testleri yaptırılmıştır.
- Zararlı yazılımlara karşı Kurumsal güvenlik yazılımları kullanılmaktadır.
- Bilgi Güvenliği Yönetim Sistemi Kurulum Projesi başlatılmıştır.
- TÜBİTAK'ın düzenlemekte olduğu Bilgi Güvenliği Eğitimlerine ve Siber Güvenlik Tatbikatlarına katılım sağlanmaktadır.

BAĞLI KURUMLAR

TÜRKİYE İSTATİSTİK KURUMU BAŞKANLIĞI

Cevap 1-4: Türkiye İstatistik Kurumu (TÜİK)'nun dışarıya hizmet veren ve dış dünyadaki kullanıcıların erişebildiği internet sayfalarına, sunucularına, gerek ilgili sistemlerin kayıtlarının incelenmesi sonucunda gerekse günlük yapılan kontrollerde doğrudan sistemleri hedef alan bilgisayar korsanı (hacker) kişi yada sistemler tarafından yapılmış; hizmetleri devre dışı bırakmaya yönelik ve ağ güvenlik sistemlerini aşabilmiş saldırı olarak nitelendirilebilecek bir olay tespit edilmemiştir.

Kurumda koruma amaçlı tedbirler alınmış olup, iyileştirme çalışması sürekli devam ettirilmektedir.

Mevcut yapıda:

- Güvenlik Duvarları (firewall) ile dış dünyadan kuruma ait dışa açık sistemlere erişimlerin kontrollü olarak yapılması sağlanmakta, bu erişimlerin tamamı kayıt altında tutulmaktadır.
- Kurumun tüm internet erişimleri vekil sunucular üzerinden, kimlik doğrulama sistemine tabi olacak şekilde ve bir içerik filtreleme sistemi dahilinde gerçekleşmekte olup, bu erişimlerin tamamı kullanıcı bazlı kayıt altında tutulmaktadır.
- Kullanıcılar ve kullanıcı makinalarının zaafiyetlerinden kaynaklı sorunları en aza indirgemek amacıyla tüm makinalarda antivirüs kurulu olup, bunların güncelliği sağlanmaktadır.
- Kurum bilgisayarlarının ilgili işletim sistemi güncellemeleri merkezi bir "update sunucusu" üzerinden yapılmaktadır.
- 5661 no'lu Yasa kapsamında, Yasanın öngördüğü sistemlerin kayıtları geriye dönük şifreli olarak merkezi bir kayıt sunucusunda tutulmaktadır.
- Sistemlerin güncel tehditler karşısında zaafiyetlerinin tespit edilip bunlara yönelik tedbirlerin alınması amacıyla "Sızma Testi" yaptırılmıştır.

Devam eden Projeler aşağıda verilmiştir:

- Saldırı Tespit ve Engelleme Sistemi (IPS) ile entegre olarak çalışacak Güvenlik Duvarlarının Güncellenmesi Projesiyle değişen kurumsal ihtiyaçlar doğrultusunda ve güncel tehditlere karşı konfigürasyonlarının yapılması
- Web Uygulama Güvenlik Duvarları (Web Application Firewall) ile dış dünyaya açık kurumsal web sayfalarının ve uygulama sunucularının güvenliğinin sağlanması
- Dışarıya açık sistemlere karşı yapılabilecek olası servis dışı bırakma saldırılarına karşı Türk Telekom ile devam eden DDOS, IPS ve firewall hizmet alımı projesinin halen devam eden demo çalışması
- Avrupa Birliği Projesi kapsamında, kurumsal verilerin sızmasının engellenmesine yönelik "veri kaybı önleme" sistemi çalışması
- Avrupa Birliği Projesi kapsamında, internetten gelebilecek zararlı kodların engellenmesi amacıyla içerik filtreleme sistemlerinin güncellenmesi ve iyileştirilmesi çalışması

GÜNEYDOĞU ANADOLU PROJESİ (GAP), DOĞU ANADOLU PROJESİ (DAP), DOĞU KARADENİZ PROJESİ (DOKAP) VE KONYA OVASI PROJESİ (KOP) BÖLGE KALKINMA İDARESİ BAŞKANLIKLARI

Cevap 1-4: GAP, DAP, DOKAP VE KOP Bölge Kalkınma İdaresi Başkanlıkları web sitelerine, datalarına ve bilgisayar sistemlerine yönelik korsanlarca yapılan herhangi bir siber saldırı sözkonusu olmamıştır. Bu konuda gerekli tedbirler alınmaktadır.