



T.C.
KALKINMA BAKANLIĞI
Özel Kalem Müdürlüğü

22060
Gk-167

Sayı : 43728771-610.00- / 3733
Konu : 7/22060 Esas Sayılı Yazılı Soru Önergesi

23 TEMMUZ 2013
ÇOK İVEDİ

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

İlgi: TBMM Kanunlar ve Kararlar Başkanlığının 06.05.2013 tarihli ve 43452547-120.07-121693 sayılı yazısı.

İlgi yazıyla, Ankara Milletvekili Sayın Özcan YENİÇERİ'nin tarafıma tevcih ettiği 7/22060 esas sayılı yazılı soru önergesinin cevaplandırılması talep edilmektedir.

Söz konusu yazılı soru önergesiyle ilgili cevabımız ekte sunulmuştur.

Gereğini arz ederim.

Cevdet YILMAZ
Bakan

EK :
1- Yazılı Soru Önergesiyle İlgili
Cevaplar (3 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>

5070 sayılı Elektronik İmza Kanunu'na uygun olarak Güvenli Elektronik İmza ile üretilmiştir.
Evrak teyidi <https://dpteb.dpt.gov.tr/Sorgu> adresinden 98MP-01B8-8H5G kodu ile yapılabilir.

okaynar@kalkinma.gov.tr



**T.C.
KALKINMA BAKANLIĞI
Özel Kalem Müdürlüğü**

**ANKARA MİLLETVEKİLİ SAYIN ÖZCAN YENİÇERİ'NİN YÖNELTTİĞİ 7/22060
ESAS SAYILI YAZILI SORU ÖNERGESİYLE İLGİLİ CEVAPLAR:**

KALKINMA BAKANLIĞI

Soru 1:2008-2013 yılları arasında, yıllara göre Kalkınma Bakanlığı ve Bağlı Kurumlara ait internet siteleri, ağları, sunucuları, sosyal medya hesapları vs. ye karşı yapılan başarılı ve başarısız siber saldırıların sayısı kaçtır?

Cevap 1:Bakanlığımıza ait internet sitesi ve sunucularına yönelik 10.06.2011 tarihinde bir adet siber saldırı tespit edilmiştir.

Soru 2:Kalkınma Bakanlığı ve Bağlı Kurumlara ait internet siteleri, ağları, sunucuları, sosyal medya hesapları vs.' ye karşı yapılabilecek olası siber saldırılara karşı alınan önlemler nelerdir?

Cevap 2:Siber saldırılara karşı alınan tedbirler:

- 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.

Soru 3:2008-2013 yılları arasında, yıllara göre Kalkınma Bakanlığı ve Bağlı Kurumlara ait siber saldırılar sonucunda devre dışı kalan internet sitesi, ağ, sunucu, sosyal medya hesapları vs. in devre dışı kaldıkları süreler nelerdir?

Cevap 3:Siber saldırı nedeniyle Telekomünikasyon İletişim Başkanlığı'nın talimatı üzerine İnternet sağlayıcımız Türk Telekom tarafından erişimimiz 12 saat süre ile devre dışı kalmıştır.

BAĞLI KURUMLAR

TÜRKİYE İSTATİSTİK KURUMU

Soru 1:2008-2013 yılları arasında, yıllara göre Kalkınma Bakanlığı ve Bağlı Kurumlara ait internet siteleri, ağları, sunucuları, sosyal medya hesapları vs. ye karşı yapılan başarılı ve başarısız siber saldırıların sayısı kaçtır?



Cevap 1: 2008-2013 yılları arasında, Kurumun dışarıya hizmet veren ve dış dünyadaki kullanıcıların erişebildiği internet sayfalarına, sunucularına, sosyal medya hesapları vs.'ye yönelik, hizmeti durdurmak veya zarar vermek amaçlı saldırı olarak nitelendirilebilecek bir olay yaşanmamıştır.

Soru 2: Kalkınma Bakanlığı ve Bağlı Kurumlara ait internet siteleri, ağları, sunucuları, sosyal medya hesapları vs.' ye karşı yapılabilecek olası siber saldırılara karşı alınan önlemler nelerdir?

Cevap 2: Kuruma ait internet siteleri, ağları, sunucuları, sosyal medya hesaplarının korunmasına yönelik olarak, ağ güvenliğini sağlayan sistemlerin iyileştirilmesine ve geliştirilmesine çalışılmaktadır. Mevcut durumda aşağıda belirtilmiş olan, alınan tedbirlerle bu tip saldırıların önüne geçilmeye çalışılmakta olup, devam eden projelerle de güncel tehditlerin ve açıkların giderilmesi sağlanarak iyileştirme çalışmaları devam etmektedir. Bunlar dışında kurumsal anlamda kurum içinde devam eden güvenlik tedbirleri de süreç içerisinde uygulanmaktadır.

Mevcut yapıda:

- Güvenlik Duvarları ile dış dünyadan kuruma ait dışa açık sistemlere erişimlerin kontrollü olarak yapılması sağlanmakta, bu erişimlerin tamamı kayıt altında tutulmaktadır.
- Kurumun tüm internet erişimleri büyük oranda 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 bilgisayarlarının zaafiyetlerinden kaynaklı sorunları en aza indirmek amacıyla tüm bilgisayarlarda antivirus kurulu olup, güncel olması sağlanmaktadır.
- Kurum bilgisayarlarının ilgili işletim sistemi güncellemeleri merkezi bir "update sunucusu" üzerinden yapılmaktadır.
- 5661 nolu 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 ve belirli periyotlarla yaptırılması planlanmıştır.

Devam eden Projeler:

- Saldırı Tespit ve Engelleme Sistemi (IPS) ile entegre olarak çalışacak Güvenlik duvarlarının güncellenmesi projesi, 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,
- Kurumsal verilerin bilinçli veya bilinçsiz sızmasının engellenmesine yönelik "veri kaybı önleme" sistemi projesi,





- İnternette gelebilecek zararlı kodların engellenmesi amacıyla içerik filtreleme sistemlerinin güncellenmesi ve iyileştirilmesi çalışması devam etmektedir.

Soru 3: 2008-2013 yılları arasında, Kalkınma Bakanlığı ve bağlı kurumlara ait siber saldırılar sonucunda devre dışı kalan internet sitesi, ağ, sunucu, sosyal medya hesapları vs.'nin devre dışı kaldıkları süreler nelerdir?

Cevap 3: 2008-2013 yılları arasında, kurumun dışarıya hizmet veren ve dış dünyadaki kullanıcıların erişebildiği internet sayfalarının, sunucuların, sosyal medya hesapları vs.'nin siber saldırı olarak nitelendirilebilecek bir durum karşısında devre dışı kalmaları söz konusu olmamıştır.

GÜNEYDOĞU ANADOLU PROJESİ BÖLGE KALKINMA İDARESİ BAŞKANLIĞI

Cevap 1-3: 2008-2013 yılları arasında, Başkanlığın internet sitesine ve web sunucusuna siber saldırı olmamıştır. Başkanlığın web sunucusunda güvenlik duvarı ve virüs koruma programları bulunmaktadır.

DOĞU ANADOLU PROJESİ BÖLGE KALKINMA İDARESİ BAŞKANLIĞI

Cevap 1-3: Başkanlığa ait internet sitesi ve sunucularına herhangi bir siber saldırı gerçekleşmemiş olup, site ve sunucular güncel antivirüs programlarıyla korunmaktadır. Bilgilerin periyodik aralıklarla yedekleri alınmaktadır. Bu güne kadar herhangi bir siber saldırı sonucu devre dışı kalan bir sistem söz konusu değildir.

DOĞU KARADENİZ PROJESİ BÖLGE KALKINMA İDARESİ BAŞKANLIĞI

Cevap 1-3: Başkanlığa ait internet sitesi ve sunucularına yönelik 2012-2013 yıllarında herhangi bir siber saldırı olmamıştır.

KONYA OVASI PROJESİ BÖLGE KALKINMA İDARESİ BAŞKANLIĞI

Cevap 1-3: Sistemlerin faaliyete geçtiği tarihten bu yana herhangi bir siber saldırı ve konuyla bağlantılı bir kesinti gerçekleşmediğinden devre dışı kalma söz konusu olmamıştır.

Başkanlığın web ve eposta sunucuları güvenlik duvarı, virüs koruma programları ve düzenli yedek alma ile siber saldırılara karşı korunmaktadır. Ayrıca, dışarıdan saldırıya maruz kalabilecek bazı protokoller kapatılmıştır ve sistemde bu protokol ve portların takibi yapılmaktadır.