7/21957

T.C.
ENERJİ VE TABİİ KAYNAKLAR BAKANLIĞI
Strateji Geliştirme Başkanlığı

30 Mayıs 2013

Sayı : 64272063-610-1648
Konu : Yazılı Soru Önergesi (7-21957)

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

İlgi: TBMM Başkanlığının 06.05.2013 tarih ve 43452547-120.07-121693 sayılı yazısı.

Ankara Milletvekili Sayın Özcan YENİÇERİ'nin tarafıma tevcih ettiği 7/21957 esas nolu yazılı soru önergesi, T.B.M.M. İç Tüzüğünün 99 uncu maddesi gereği aşağıda cevaplandırılmaktadır.

Bilgilerinize arz ederim.

Taner YILDIZ
Bakan

EK :
Önerge Cevabı (1 Sayfa)

İnönü Bulvarı No: 27 A Blok Kat 2 Bahçelievler-Ankara
Tel : (0312) 223 64 69 Faks: (0312) 215 36 62
E-mail: asar@enerji.gov.tr

Bilgi için : Arzu ŞAR

T.C.
ENERJİ VE TABİİ KAYNAKLAR BAKANLIĞI

ANKARA MİLLETVEKİLİ SAYIN ÖZCAN YENİÇERİ'NİN
YAZILI SORU ÖNERGESİ VE CEVAPLARI
(7/21957)

Sorular 1, 3:
Kamu kurumlarına karşı yapılan siber saldırılar sıklıkla basında yer almaktadır.
Buradan hareketle;
- 2008-2013 yılları arasında, yıllara göre Enerji ve Tabii Kaynaklar Bakanlığı (ETKB) ve bağlı kurumlara ait internet siteleri, ağları, sunucuları, sosyal medya hesapları vs.'ye karşı yapılan başarılı ve başarısız siber saldırıların sayısı kaçtır?
- 2008-2013 yılları arasında, yıllara ETKB ve bağlı kurumlara ait siber saldırılar sonucunda devre dışı kalan internet sitesi, ağ, sunucu, sosyal medya hesapları vs'nin devre dışı kaldıkları süreler nelerdir?

Cevaplar 1, 3:
2008 ile 2013 yılları arasında Bakanlığımız, bağlı ve ilgili kurumlarımıza ait internet siteleri, ağları, sunucuları ve sosyal medya hesaplarına karşı yapılan herhangi bir siber saldırı bulunmamaktadır.

Soru 2:
ETKB ve bağlı kurumlara ait internet siteleri, ağları, sunucuları, sosyal medya hesapları vs.'ye karşı yapılabilecek olası siber saldırılara karşı alınan önlemler nelerdir?

Cevap 2:
Bakanlığımız bünyesinde internet sitesi geliştirilirken sql enjection açıklarına ve güvenlik duvarı ile içeri sızmalara karşı gerekli önlemler alınmıştır. Sunucu ve network yapısı, yedekli ve geniş bant genişliğine sahip bir yapıda tasarlanmış olmakla birlikte ddos ataklara karşı da önlemler alınmıştır. Antivirüs yazılımları, güvenlik duvarları, içerik filtreleme yazılımları ile güvenlik önlemleri artırılmıştır. Ayrıca, internet sitesi, ağlar ve sunuculara karşı yapılabilecek olası siber saldırılara karşı güvenlik duvarı (Firewall), proxy destekli, içerik filtreleme yapabilen, ve gerçek zamanlı olarak ağ ve sistem tabanlı virüs koruma yapan yazılım ve donanımlar ile IPS (Intrusion Prevention Systems), anti virus, anti spam ve NAC (Network Access Control) sistemleri kullanılarak olası siber saldırılara karşı önlemler alınmıştır.