25847

ENERJİ VE TABİİ KAYNAKLAR BAKANLIĞI

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

29 Temmuz 2013

Sayı : 64272063-610 - 2197
Konu : Yazılı Soru Önergesi (7-25847)

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

İlgi: TBMM Başkanlığının 26.06.2013 tarih ve A.01.0.KKB.0.10.00.00-130455 sayılı yazısı.

İstanbul Milletvekili Sayın Sezgin TANRIKULU'nun tarafıma tevcih ettiği 7/25847 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

ENERJİ VE TABİİ KAYNAKLAR BAKANLIĞI

İSTANBUL MİLLETVEKİLİ SAYIN SEZGİN TANRIKULU'NUN YAZILI SORU ÖNERGESİ VE CEVAPLARI (7/25847)

Sorular 1, 2, 3, 4:

Çağımızda birçok ülkenin ulusal güvenlik tehditleri arasında siber saldırılar yer almaktadır. Bilgisayar korsanları (hacker) tarafından kamu kuruluşlarının resmi internet sayfaları ve veri tabanları saldırıya uğrakta, bu saldırılar sonucu internet siteleri çökertilip, kamu kurumuna ait verilere erişilmektedir. Bu bağlamda;

- Bakanlığınıza bağlı Kurum ve Kuruluşlar bilgisayar korsanlarınca (hacker) saldırıya uğramış mıdır? Bu saldırılar ne zaman ve hangi bağlı Kuruma yapılmıştır?
- 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?
- 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?
- Siber saldırıya uğrayan Bakanlığınıza bağlı Kurum ve Kuruluşlarda, bilgisayar korsanlarına karşı Önleyici tedbirler alınmış mıdır? Bu tedbir ve saldırıların kuruma maliyeti nedir?

Cevaplar 1, 2, 3, 4:

Bakanlığımız, bağlı ve ilgili kurumlarımıza ait internet siteleri, ağları, sunucuları ve sosyal medya hesaplarına karşı yapılan herhangi bir siber saldırı bulunmamaktadır.

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.