



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

03 Temmuz 2014

Sayı : 64272063- 610 -1888
Konu :Yazılı Soru Önergesi (7-44685)

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

İlgi: TBMM Başkanlığının 10.06.2014 tarih ve 43452547-120.00-181890 sayılı yazısı.

Ankara Milletvekili Sayın Özcan YENİÇERİ'nin tarafıma tevcih ettiği 7/44685 esas nolu yazılı soru önergesi, T.B.M.M. İç Tüzüğü'nün 99 uncu maddesi gereği aşağıda cevaplandırılmaktadır.

Bilgilerinize arz ederim.

Taner YILDIZ
Bakan

EK :
Önerge Cevabı (1 Sayfa)

ANKARA MİLLETVEKİLİ SAYIN ÖZCAN YENİÇERİ'NİN
YAZILI SORU ÖNERGESİ VE CEVAPLARI
(7/44685)

Sorular 1, 2, 3, 4:

18-19 Mayıs 2014 tarihlerinde kamuoyunda Redhack adı ile bilinen hacker grubu Türk İşbirliği ve Koordinasyon Ajansı Başkanlığı'nın (TİKA) elektronik posta ve kullanıcı giriş bilgilerini sosyal medya ve internet üzerinden paylaşmıştır. Daha önce tüm bakanlıklar ile Türkiye Büyük Millet Meclisi Başkanlığına sunduğum yazılı soru önergelerine bugüne kadar herhangi bir veri ile bilgi kaybı yaşanmadığı ve siber saldırılara karşı her türlü tedbirin alındığı şeklindeki yanıtlar üzerine TİKA'nın elektronik posta ve kullanıcı giriş bilgilerinin bir hacker grubu tarafından ele geçirilmesi son derece kaygı vericidir. Buradan hareketle;

- 1 Ocak 2014 tarihinden bu yana bakanlık ile bakanlığa bağlı kurum ve kuruluşlara yönelik siber saldırıların sayısı kaçtır? Bu saldırıların kaynağı hangi ülkelerdir?
- Bahsi geçen saldırılar sonucunda bakanlık ile bakanlığa bağlı kurum ve kuruluşlarca herhangi bir veri ve bilgi kaybı yaşanmış mıdır? Yaşandı ise bu bilgi ile veriler hangileridir?
- 1 Ocak 2014 tarihinden bu yana siber saldırılar sonucunda bakanlık ile bakanlığa bağlı kurum ile kuruluşların internet hizmetlerinde yaşanan aksamaların sayısı kaçtır? Bu aksamaların her birinin süresi ne kadardır?
- Mayıs 2014 itibarı ile bakanlık ile bakanlığa bağlı kurum ile kuruluşların internet güvenliğinin artırılması ve güncellenmesi adına yürütülmekte olan çalışma ile projeler var mıdır? Var ise bunlar hangileridir ve ne aşamadır?

Cevaplar 1, 2, 3, 4:

Bakanlığımız, bağlı ve ilgili kuruluşlarımıza karşı yapılan bir siber saldırı bulunmadığı gibi herhangi bir veri kaybı da yaşanmamıştır.

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.