

7/21838

T.C.
BAŞBAKAN YARDIMCILIĞI

Sayı : 71366025-031- 546

29/05/2013

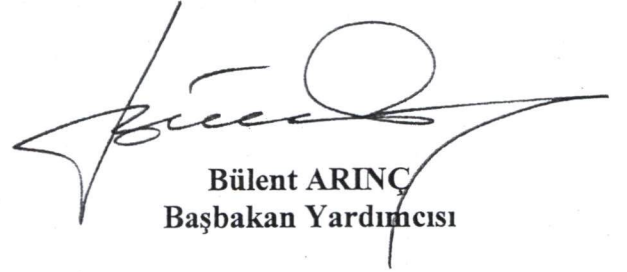
Konu : Soru Önergesi

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

İlgi :06/05/2013 tarihli ve 4345247-120.07-121693 sayılı yazınız.

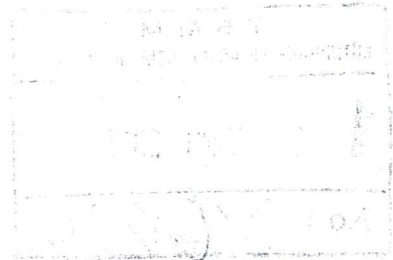
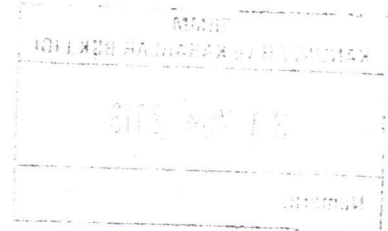
Ankara Milletvekili Sayın Özcan YENİÇERİ tarafından tevcih edilen 7/21838 esas numaralı yazılı soru önergesine ilişkin cevap ekte gönderilmektedir.

Bilgi ve gereğini arz ederim.


Bülent ARINC
Başbakan Yardımcısı

EK:

Cevabi yazı (2 sayfa)



T.C.
BAŞBAKAN YARDIMCILIĞI
(Sn. Bülent ARINÇ)

**ANKARA MİLLETVEKİLİ SAYIN ÖZCAN YENİÇERİ TARAFINDAN
TEVCİH EDİLEN 7/21838 SAYILI YAZILI SORU ÖNERGESİ CEVAPLARI**

Bakanlığım sorumluluğundaki kurum ve kuruluşlardan alınan bilgilere göre 2008-2013 yılları arasında;

Atatürk Kültür, Dil ve Tarih Yüksek Kurumu ile bünyesinde yer alan kurumlardan aynı binada yer alan Atatürk Kültür Merkezi ve Atatürk Araştırma Merkezi internet siteleri, ağları ve sunucularına, çok sık münferit siber saldırı gerçekleşmektedir.

Çoğunlukla internet sitesine yönelik olan bu saldırılar, siteye ait sistemlerde zafiyet arama ve port tarama şeklinde olup organize nitelik taşımamaktadır. Bu tür saldırıların sayısı, ayda ortalama 200-300 arasında değişmektedir. 2008-2013 yılları arasında sadece bir defa organize siber saldırı gerçekleştirilmiş, yapılan incelemede, Atatürk Kültür, Dil ve Tarih Yüksek Kurumu sunucu sistemleri üzerinden Amerikan bankalarının hedef alındığı tespit edilmiştir.

Anılan yıllar arasında, Türk Dil Kurumuna, Türk Tarih Kurumuna ait Genel Ağ (İnternet) sitesine, yerel ağına, sunucularına, sosyal medya hesaplarına karşı siber saldırı olmamıştır.

Atatürk Kültür, Dil ve Tarih Yüksek Kurumuna ait internet siteleri, sunucu ve ağ sistemleri güncel güvenlik duvarları ile korunmaktadır. Özellikle internetten erişime açık sistemler sürekli takip edilerek, yazılım zafiyetlerine karşı otomatik yama yönetimi etkin hâle getirilmiştir. E-posta sistemleri ve istemci bilgisayarlar üzerinde anti-virüs ve anti-spam yazılımları yüklenerek olası botnet ve DDOS saldırılarına karşı tedbirler alınmıştır. Kullanıcı ve yönetici şifreleri "brüte force" saldırılarına karşı karmaşık olarak belirlenmiş, belirli aralıklarla şifrelerin değiştirilmesi zorunlu tutulmuştur.

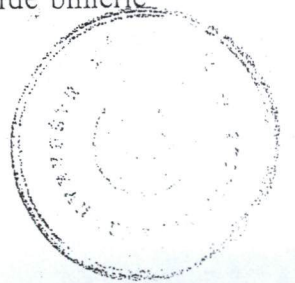
Atatürk Araştırma Merkezinize ait internet sitesi, yerel ağları, sunucuları, sosyal medya hesapları vesaireye karşı yapılabilecek olası siber saldırılarına karşı firewall güvenlik cihazı ve anti-virüs yazılımları kullanılmaktadır.

Türk Dil Kurumu Genel Ağ sitesine, yerel ağlarına ve sunucularına yapılabilecek saldırılara karşı güvenlik duvarları oluşturulmuş ve güncel anti-virüs yazılımları kurulmuştur. Sosyal medya hesaplarında ise güçlü şifreler kullanılmaktadır.

Türk Tarih Kurumu Genel Ağ sitesine, yerel ağlarına, sunucuları ve sosyal medya hesaplarına yapılabilecek saldırılara karşı güvenlik duvarları oluşturulmakta ve güncel işletim sistemi, lisanslı virüs koruma programı, kullanıcıları bilinçlendirme çalışmaları yapılmaktadır.

Bahsedilen tarihlerde Atatürk Kültür, Dil ve Tarih Yüksek Kurumu ve bünyesindeki Kurumlara karşı siber saldırılar sonucunda devre dışı kalan internet sitesi, sunucu, sosyal medya hesapları, yerel ağ vs. bulunmamaktadır.

Vakıflar Genel Müdürlüğü internet siteleri, ağları, sunucuları, sosyal medya hesapları vs.'ye yapılmış ve güvenlik önlemlerini aşan başarılı bir saldırı bulunmamaktadır. Bunun dışında, ifade edilen dönem zarfında güvenlik cihazlarına takılan farklı kategorilerde binlerle ifade edilebilecek mutad ve tehdit seviyesi düşük saldırılar gerçekleşmiştir.



Saldırıları önlemek adına alınan önlemler kapsamında; donanım ve yazılım (Güvenlik duvarı, Ids/Ips cihazı, Wcb filtreleme cihazı, spam filtreleme cihazı, dmz kullanımı), kurum dışına açık site ve uygulamalar için penelrasyon testleri yaptırılarak açıkların belirlenmesi ve kapatılması işlemleri ve ISO 27001 kapsamında kurumsal bilgi güvenliği politikasına dayalı yürütülen çalışmalar vardır.

Kurumun internet siteleri, ağları, sunucuları, sosyal medya hesapları vs.'ye yapılmış ve sistemleri devre dışı bırakmış başarılı bir saldırı bulunmadığından devre dışı kalma süresi de bulunmamaktadır.

Basın Yayın ve Enformasyon Genel Müdürlüğünün web sitesinde ve diğer hizmetlerde herhangi bir siber saldırı ile karşılaşılmaamıştır. Siber saldırılara karşı, Genel Müdürlüğün Arşiv ve Bilgi İşlem Şube Müdürlüğünde gelen-giden tüm internet trafiğini denetleyen Checkpoint güvenlik sistemi mevcut olup, 7/24 esasına göre çalışır haldedir. Siber saldırı ile karşılaşmadığından, devre dışı kalma durumu da söz konusu olmamıştır.

Türkiye Radyo-Televizyon Kurumu Genel Müdürlüğüne yönelik herhangi bir siber saldırı bulunmamakla birlikte, Kurumda kişisel bilgisayarların güvenliği uzman bir ekip tarafından sağlanmakta ve bu hizmet güvenlik duvarı cihazları, saldırı önleme sistemleri ve antivirüs yazılımları ile desteklenmektedir. Kurum, TÜBİTAK'ın düzenlemiş olduğu II. Ulusal Siber Güvenlik Tatbikatına katılarak birçok testte tabi tutulmuş ve bu tatbikatı başarı ile tamamlamıştır.

Anadolu Ajansı Genel Müdürlüğü sistemlerine küçük ve büyük saldırılar olmak üzere muhtelif sayılarda siber saldırı yada ataklar olmuştur. Ajansın internet siteleri, ağları, sunucu ve sosyal medya hesaplarına 2008-2013 yılları arasında iki büyük siber saldırı olmuştur. 19.05.2012 tarihinde meydana gelen saldırıda abonelere hizmet verilen paketlerden bir tanesi yaklaşık 8 saat süresince hizmet verememiştir. 10.03.2013 tarihinde meydana gelen saldırı sırasında hizmetlerde kesinti yaşanmamış, bazı web sitelerine kısa süreli olarak erişim problemi yaşanmıştır.

Anadolu Ajansı internet siteleri, ağları, sunucu ve sosyal medya hesaplarına yapılan iki büyük saldırıda da herhangi bir veri kaybı yaşanmamıştır.

Anadolu Ajansı'nın kurumsal sistem alt yapısı hem kurum, hem de ISP sistemlerinde olmak üzere iki katmanlı güvenlik seviyesi uygulanmaktadır. Kurum sistemlerinde güvenlik duvarı, atak önleme - yük dengeleme sistemleri antivirüs yazılımları kullanılmaktadır. Ayrıca ISP sisteminde atak önleme (DDOS) sistemi konumlandırılmıştır.

Radyo ve Televizyon Üst Kurulu Başkanlığına ait internet siteleri, ağları, sunucuları ve sosyal medya hesaplarına herhangi bir başarılı ve başarısız siber saldırı tespit edilmemiştir.

Üst Kurul'a ait internet siteleri, ağları, sunucuları ve sosyal medya hesaplarına karşı yapılacak siber saldırılara karşı, hem yazılım hem de donanım olarak saldırı önleme ve tespit sistemleri temin edilmiş ve gerekli güvenlik tedbirleri alınmıştır. Bunlar; güvenlik duvarları donanım ve yazılımları, e-posta yoluyla olabilecek saldırı engelleme donanım ve yazılımları ve ayrıca kullanıcı bilgisayarlarında da antivirüs vb. yazılımlarıdır.

2008-2013 yılları arasında Üst Kurul'a ait internet siteleri, ağları, sunucuları ve sosyal medya hesapları herhangi bir siber saldırı sonucu devre dışı bırakılmamıştır.

