

T.C.
EKONOMİ BAKANLIĞI

Sayı : 84832410-610-[2013/173] _804

Konu : Yazılı Soru Önergesi

8 Temmuz 2013

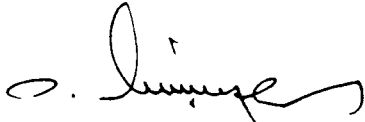
47308

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

İlgi : 26/06/2013 tarihli ve 43452547-120.00-130455 sayılı yazıları.

İlgi'de kayıtlı yazıları ekinde yer alan İstanbul Milletvekili Sn. Dr. M. Sezgin TANRIKULU tarafından verilen 7/25839 sayılı yazılı soru önergesine ilişkin cevap ilişikte sunulmaktadır.

Bilgilerine arz ederim.



Zafer ÇAĞLAYAN
Bakan

EKLER:

1- Cevap yazısı (1 sayfa)

T.C.
EKONOMİ BAKANLIĞI

İstanbul Milletvekili Sn. Dr. M. Sezgin TANRIKULU tarafından verilen 7/25839 sayılı yazılı soru önergesine ilişkin sorular ve cevaplar:

Sorular :

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

Bu bağlamda;

1- Bakanlığınıza bağlı kurum ve kuruluşlar bilgisayar korsanlarınca (hacker) saldırıya uğramış mıdır? Bu saldırılar ne zaman ve hangi bağlı kuruma yapılmıştır?

2- 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?

3- 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?

4- Siber saldırıya uğrayan Bakanlığınıza bağlı kurum ve kuruluşlarda, bilgisayar korsanlarına karşı önleyici tedbirler alınmış mıdır? Bu tedbirler ve saldırıların kuruma maliyeti nedir?

Cevaplar:

Bakanlığım sitelerine, sunucularına ve ağlarına yapılan siber saldırılar, 2012 yılında DDOS servis durdurma atağı ve 2013 yılında da bir sitenin bilgisine erişmek için SQL injection atağı şeklinde gerçekleşmiştir. Ancak bu saldırı girişimleri alınan başarılı tedbirler sayesinde püskürtülmüştür.

Herhangi bir siber saldırı sonucu Bakanlık bilgi sistemleri üzerinden çok gizli ve gizli ibareli belgeler dâhil açığa çıkan herhangi bir belge yoktur.

Bakanlığıma ait internet siteleri, ağları, sunucularına karşı yapılacak siber ataklar için mümkün olan tedbirler alınmaktadır. Bakanlığım güvenlik duvarları, atak tespit sistemleri, filtre içerik kontrolü, virüslere karşı koruma yazılımları kullanırken, servis durdurmayı ve içerik yoluyla atakları tespit ve önlemeye yönelik İnternet Servis Sağlayıcıdan sağlanan hizmetler kullanılmaktadır. Ayrıca, gerek işletim sistemleri gerekse yazılımların güvenlik açıklarını giderecek güncellemeler yapılmakta ve geliştirilen uygulamaların güvenlik testleri yaptırılmaktadır. Bununla birlikte, tüm sistemler üzerinde de güvenlik testleri yaptırılmaktadır. Bu testlerin 2013 yılından itibaren yılda 2 defa (Haziran ve Aralık aylarında) olmak üzere düzenli olarak yapılması planlanmıştır.

Yapılan web siteleri ve hazırlanan yazılımlarda SQL Injection gibi yazılım açıkları kontrol edilmekte ve düzeltilmektedir. Siber saldırıları önlemek için gerekli tedbirler alınmakla olup güvenlik önlemleri için harcanan maliyetler bütçe kaynakları çerçevesinde karşılanmaktadır.