

T.C.
ULAŞTIRMA BAKANLIĞI
Strateji Geliştirme Başkanlığı

01 Aralık 2010

Sayı :B.11.0.SGB.0.10.01.610.01/2216
Konu :Samsun Milletvekili
Sayın Osman ÇAKIR'ın
yazılı soru önergesi.

7/15610
GK 23

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

- İlgi: a) TBMM Başkanlığının 21.07.2010 tarihli ve KAN.KAR.MD. A.01.0.GNS.0.10.00.02-7/15610-24961/51505 sayılı yazısı.
b) Başbakanlığın 23.07.2010 tarihli ve B.02.0.KKG.0.12/106-230-7/3392 sayılı yazısı

Samsun Milletvekili Sayın Osman ÇAKIR tarafından Sayın Başbakanımıza yöneltilen ve Sayın Başbakanımızın da kendileri adına Bakanlığımız koordinatörlüğünde cevaplandırılmasını tensip ettikleri 7/15610 sayılı yazılı soru önergesinin cevabı hazırlanarak ekte sunulmuştur.

Bilgilerinize arz ederim.



Binali YILDIRIM
Ulaştırma Bakanı

EK :

1) Cevap formu (2 Sayfa)

DAĞITIM:
TBMM Başkanlığı
Başbakanlık

**SAMSUN MİLLETVEKİLİ SAYIN OSMAN ÇAKIR'IN
7/15610 SAYILI YAZILI SORU ÖNERGESİ VE CEVABI**

Basından elde edilen bilgilere göre;

Mavi Marmara saldırısının yaşandığı günlerde İHH'nın internet sitesini bloke eden Check Point isimli internet güvenlik şirketinin bilgilerinin Tel Aviv'den güncellendiği, bunun İsrail bağlantılı olduğu, aralarında Merkez Bankası, Ziraat Bankası, Vakıfbank, Halkbank, Eximbank, Kara Kuvvetleri Komutanlığı ve bağlı tüm birimleri, Cumhurbaşkanlığı, Başbakanlık, Milli Eğitim, Sağlık ve Adalet Bakanlıkları, ÖSYM; Dışişleri Bakanlığı gibi birçok kamu kurumunun da internet güvenliğinin İsrail bağlantılı bir şirket tarafından sağlandığı belirtilmektedir. Buna göre;

SORULAR:

- 1- İsraili şirketlerin ülkemizin iletişim hatlarını kontrol altına aldığı doğru mudur?
- 2- Bu kurumların bu şirket veya taşeronları vasıtasıyla internet güvenliklerini sağladığı gerçek midir?
- 3- Bunlar doğruysa, şirketlerin hangileri doğrudan İsraili hangileri taşeron kullanmaktadır?
- 4- Taşeron değilse bu şirketlerin verdiği hizmetleri İsraili firmalar neden referans gösterilmektedir?
- 5- Türkiye'de İsrail'e bu bağımlılığı kimler güvence altında tutmaktadır?

CEVAPLAR:

Bilgi ve iletişim sektöründeki güvenlik kavramı esasen iki ortamda gerçekleşmektedir. Bunlardan birisi bilgisayar sistemine sahip olan kurumların kendi inisiyatifleri doğrultusunda gerçekleşen güvenlik sistemi, diğeri ise bu bilgisayar sistemlerinin internet ortamındaki şebeke güvenliğidir. İnternet ortamında güvenli şebeke erişimini sağlamak ve bu konuda gerekli tedbirleri almak Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı'nın (BTK) düzenlemeleri çerçevesinde İşletmecilerin yükümlüğündedir. Kullanıcı konumunda olan Kurum/Kuruluşların bilgisayar ve veri güvenliği ise bu kurum ve kuruluşların kendi inisiyatifinde gerçekleşmektedir.

Ülkemizdeki bilgi ve iletişim altyapı ve şebekelerinde güvenli ve güvenilir hizmet sunulmasının sağlanması Bakanlığımız politikaları arasındadır ve bu konuya ilişkin Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı tarafından gerekli düzenleme çalışmaları yapılmıştır.

Bu kapsamda, 10.11.2008 tarih ve 5809 sayılı Elektronik Haberleşme Kanunu ile; Bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi, izinsiz erişime karşı şebeke güvenliğinin sağlanması, elektronik haberleşme sektörüne yönelik olarak, milli güvenlik, kamu düzeni veya kamu hizmetinin gereği gibi yürütülmesi amacıyla mevzuatın öngördüğü tedbirlerin alınması gibi görevler Bakanlığımızın ilişkili kurumu olan Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı'na verilmiştir.

Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı ise 5809 sayılı kanunun yürürlüğe girdiği tarihten önce 20.07.2010 tarih ve 26942 sayılı Resmi Gazete'de yayımlanan Elektronik Haberleşme Güvenliği Yönetmeliği ile gerekli çalışmaları başlatmış ve 5809 sayılı Elektronik Haberleşme Kanunu'nun yürürlük tarihinden sonra da güncellemiştir. Ayrıca, Bakanlık olarak bu konuda Kurum, Kuruluşlar ve kullanıcılar ile son kullanıcılar nezdinde bir farkındalık yaratmak amacıyla "Güvenli İnternet Günü" gibi etkinlikler düzenlenmiştir.

Ülkemizin iletişim altyapısında yabancı menşeli yazılım ve donanımlar kullanılabilmektedir. Ülkemizin teknolojik bağımsızlığını sağlamak amacıyla, çeşitli kurumlarıyla araştırma ve geliştirme faaliyetleri gerçekleştirilmektedir. Milli güvenlik duvarı, ulusal Linux dağıtımı (Pardus), milli kript sistemleri, milli haberleşme sistemleri vb. çok kritik alanlarda milli ürünler geliştirilmekte, bu milli ürünler kamuda yaygınlaştırılmakta ve ülkemizin teknolojik bağımsızlığının artırılması amacıyla çalışmalar devam etmektedir.

Güvenlik duvarı, internet ağı ile kurum ağı arasındaki iletişimin kısıtlanması amacıyla kullanılan temel bir güvenlik bileşenidir. Söz konusu Checkpoint güvenlik duvarı yazılımı ya da yabancı menşeli farklı marka ve modellerde ticari güvenlik yazılımları ülkemizde de dünya genelinde de internet güvenliğinin sağlanması amacıyla yaygın olarak kullanılmaktadır. Güvenlik duvarı yazılımı tek başına internet güvenliğinin sağlanması için yeterli değildir. Sistemlerde kullanılan farklı ürünlerin üretici firmaları farklı ülkelerden olabilmekle birlikte, sistem güvenliğinin sağlanması ve ilgili ayarların kontrolü sistem sahibinin yetkisi dahilindedir. Yazılımlarla ilgili bazı güncellemeler ürün tarafından otomatik olarak yapılabilir. Fakat bu özelliklerin kullanımı sistem sahibinin tercihinine bağlıdır. Şüphesiz ki bu ürünlerin milli imkanlar ile geliştirilmesi ve altyapıda kullanılması güvenlik seviyesini ve sistem güvenilirliği artıracaktır. Ülkemizde bu konuda önemli çalışmalar yapılmaktadır. Siber Güvenlik olarak da adlandırılabilir olan bu konuda TÜBİTAK gibi diğer kamu ve kuruluşlarının da önemli çalışmaları mevcuttur. Örneğin, bu çerçevede 1990'ların sonlarından 2006 yılına kadar Milli Savunma Bakanlığı koordinasyonunda ulusal bilgi güvenliği konusundaki hukuki boşluğu gidermek için çalışmalar yapılmış olup, bu bağlamda, Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı Taslağı hazırlanmıştır.

Öte yandan, Kara Kuvvetleri Komutanlığı, iletişim ortamı olarak TAFİCS altyapısını kullanmakta olup, tüm hatların kontrolü tamamen Kara Kuvvetleri Komutanlığına veya Genelkurmay Başkanlığına ait durumdadır. Kara Kuvvetleri Komutanlığının internet güvenliği ile ilgili ihtiyaç duyduğu donanım ve yazılımlar; şartnamelerde marka ve model belirtilmeden tanımlanmakta, bağımsız kurum ve kuruluşlar tarafından denetlenen, çalıştıkları alanlarda dünyada en iyiler arasında yer alan, uzun yıllar denenmiş ve kendini ispat etmiş, ürünleri en uygun fiyata temin eden firmalar arasından, Kamu İhale Kanununda düzenlenmiş bulunan açık ihale usulü hükümlerine göre Milli Savunma Bakanlığı tarafından tedarik edilmektedir.

Ülkemizin bilgi toplumuna dönüşüm sürecinin koordinasyonu amacıyla yürütülen e-Dönüşüm Türkiye Projesi kapsamında hazırlanan ve 2006-2010 dönemini kapsayan Bilgi Toplumu Stratejisi ve ek'i Eylem Planı, 2006/38 sayılı Yüksek Planlama Kararı ile onaylanmış ve 28 Temmuz 2006 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Eylem Planında yer alan "Bilgi Güvenliği ile İlgili Yasal Düzenlemeler" başlıklı 87 numaralı eylem Adalet Bakanlığı'na verilmiştir.

Ayrıca, bilindiği gibi ithal edilecek Telsiz ve Telekomünikasyon Terminal Ekipmanlarından 2010/8 sayılı Dış Ticarete Standardizasyon Tebliği kapsamında frekans ve/veya lisans kısıtlaması olan cihazlara onay verilmekte olup onay verilen cihazlar ise BTK Başkanlığı internet sayfasında güncellenerek yayımlanmaktadır. (<http://www.btk.gov.tr/SpektrumYonetimi/sinif2/sinif2.htm>)