

T.C.
ULAŞTIRMA BAKANLIĞI
Strateji Geliştirme Başkanlığı

18-08-2010

7/14978
GK: 180

Sayı :B.11.0.SGB.0.01.00.610.01/1610
Konu :Uşak Milletvekili
Sayın Osman COŞKUNOĞLU'nun
yazılı soru önergesi.

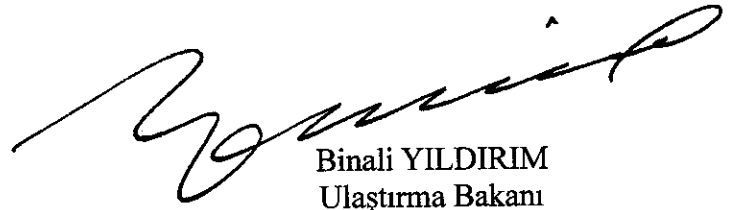
TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

İlgi: a)TBMM Başkanlığının 16.06.2010 tarihli ve KAN.KAR.MD.A.01.0.GNS.0.10.00.02-7/14978-23979/49511 sayılı yazısı.

b) Başbakanlığın 21.06.2010 tarihli ve B.02.0.KKG.0.12/106-222-19/2778 sayılı yazısı.

Uşak Milletvekili Sayın Osman COŞKUNOĞLU tarafından Sayın Başbakanımıza yöneltilen ve Sayın Başbakanımızın da kendileri adına Bakanlığımız koordinatörlüğünde cevaplandırılmasını tensip ettikleri 7/14978 esas sayılı yazılı soru önergesinin cevabı hazırlanarak ekte sunulmuştur.

Bilgilerinize arz ederim.


Binali YILDIRIM
Ulaştırma Bakanı

EK :

1) Cevap formu (6 Sayfa)

DAĞITIM:

TBMM Başkanlığı
Başbakanlık

UŞAK MİLLETVEKİLİ SAYIN OSMAN COŞKUNOĞLU'NUN
7/14978 SAYILI YAZILI SORU ÖNERGESİ VE CEVABI

Check Point, internet güvenlik ürünleri geliştiren İsrail kökenli bir firmadır. Geçen hafta, Mavi Marmara gemisine İsrail askerleri saldırdığı sıralarda, Check Point'in internet filtreleme ürününü kullanan kuruluşların İHH web sitesine (ihh.org) girmeleri engellenmiştir. Bunun nedeni, Check Point veya onun hizmet aldığı firmanın ihh.org sitesini "nefret saçan" ("Hate speech") kategorisine dahil etmiş olmasıdır. Bu bilgi ışığında:

SORULAR:

1.İçinde bankaların ve devlet kurumlarının da olduğu, pek çok kuruluşun Check Point ürünleri kullandığı doğru mudur?

2.Hangi kamu kuruluşlarında Check Point ürünleri kullanılmaktadır?

3.İsrail'in stratejik müttefiki ve en yakın dostu olan ABD'de, Check Point 2006 yılında güvenlik ürünü geliştiren bir Amerikan firmasının (Snorts) satın almak istediğinde buna Bush yönetiminin ulusal güvenlik nedeniyle izin vermediğini biliyor muydunuz? T.C. başbakanı olarak, bir yandan uluslararası platformlarda İsrail ile ilgili keskin sözler sarfederken bir yandan da bu İsrail firmasına Bush'dan bile daha fazla mı güveniyorsunuz da devlet kurumlarında bile kullanılmasına izin veriyorsunuz?

4.Check Point ürünü olmasa da, ülkemizde kullanılan internet güvenlik ürünlerinin tamamına yakınının yabancı firmalar tarafından geliştirildiği doğru mudur? Bu kadar yabancı ürün bağımlılığı, özellikle devlet kurumlarında ciddi bir güvenlik riski oluşturmuyor mu?

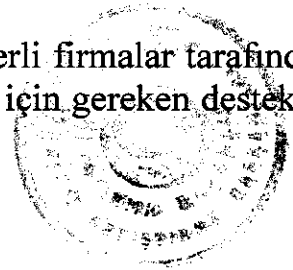
5.Önemli kurumlarda kullanılan güvenlik ürünlerinin alımında ciddi bir inceleme süreci var mıdır? Güvenlik ürünleri tercih edilirken bağımsız uzmanlara denetim yaptırılmakta mıdır?

6.Mavi Marmara gemisine İsrail saldırısı üzerine, İsrail'den ülkemize internet üzerinden başka siber saldırılar olmuş mudur? Kaç gün süren hangi saldırılar veya engellemeler olmuştur? Bu gibi saldırılara karşı ülkemiz hazırlıklı mıdır?

7.Söylemde "bilgi toplumu" veya "bilgi çağı" kavramlarını sık sık kullanan, ama kendi hükümetinizin hazırlattığı ve 2006 Temmuz'unda Resmi Gazete'de yayımlanan "Bilgi Toplumu Stratejisi"nin içindeki eylemleri bile 4 yıldır gerçekleştiremeyen hükümetiniz, internet güvenliğimiz konusunda da ciddiyyetle uzak bir yaklaşım içerisinde olmuyor mu?

8.Ülkemizde internet güvenliği üzerine araştırma yapma ve ürün geliştirme konusunda yetkin mühendisler ve firmalar olduğu halde, hükümetiniz neden yabancı ürün bağımlılığına seyirci kalarak ülkemiz için riskli bir durum yaratıyor? Neden bu konuda yerli ürün geliştirilmesi teşvik edilmiyor?

9.Hiç değilse devlet kurumlarında kullanılması için yerli firmalar tarafından, tercihen açık kaynak kodlu güvenlik yazılımları geliştirilmesi için gereken destekleri sağlayacak mısınız?



10.Üçüncü dünya ülkeleri dışındaki her ülke siber güvenliğe önem verirken, bir siber saldırı karşısında yazılımları ve verileri kaybetmemek için yedekleme sistemleri geliştirirken, hatta bilişim alanında olası bir ulusal krizi önlemek ve yönetmek için gerekli kurumları (örneğin, ABD'de CERT) kurarken, siber güvenlikten sorumlu kişiler atarken, neden hükümetiniz ülkemizi bu konularda üçüncü dünya ülkeleri gibi tamamen hazırlıksız ve korumasız bir durumda bırakıyor?

CEVAPLAR:

Ülkemizdeki telekomünikasyon sektöründe yetkilendirmelere ilişkin düzenleme yapma görevi, İşletmecilere verilen yetkilendirmelerin denetlenmesi ve işletmecilerin hizmet sundukları telekomünikasyon şebekesinin hangi usul-esaslara göre işletileceği ve tarifelerin onaylanması gibi hususlar ile bu konuların yeniden düzenlenmesi görevleri mer'i mevzuat hükümleri çerçevesinde Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı'na aittir.

Bilgi toplumu, internet güvenliği ve yerli ürün konularında Bakanlık politikalarımız, bilgi toplumunun oluşumunu hızlandırmak amacıyla ülkemiz kaynakları, bilgi birikimi ve potansiyelini en üst seviyede kullanarak güvenli internet erişimini sağlamak şeklinde özetlenebilir.

Check point isimli firmaya, bugüne kadar ithal ettiği ürünlere ilişkin olarak Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı tarafından, Bildirim Formu (sınıf 2) başvurusu ile onay alma işlemi gerçekleştirilmemiştir.

AR-GE ve yerli katkı payı konularına, Bakanlığımız özel bir önem vermektedir. 2008 yılı Kasım ayında yayınlanan Elektronik Haberleşme Kanunu'yla ülkemizde ilk kez AR-GE'yi desteklemek amacıyla sektöre özel bir fon oluşturulmuştur. Ayrıca, 3G olarak adlandırılan projede, sağlanması gereken yerli katkı payının oranını ve proje gereksinimlerinin ülkemiz insan kaynağı ile tedariki konusunda özel hükümler getirerek ülkemiz telekomünikasyon sektöründe ilk kez İmtiyaz Sözleşmelerine yerli katkı payıyla ilgili somut bir yükümlülük getirilmiştir.

Yerli katkı oranı ve AR-GE faaliyetleri, bugünden yarına hemen sonuç veren konular değildir. Bu nedenle Bakanlığımız AR-GE ve yerli katkı oranlarını yükseltmeye yönelik bu faaliyetlerin temelini atmaya çalışmaktadır. Bu kapsamda; 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 "Ulusal Bilgi Sistemleri Güvenlik Programı" başlıklı 88 numaralı eylem ile TÜBİTAK-UEKAE'ye Bilgisayar Olaylarına Acil Müdahale Merkezi (TR - BOME) kurma görevi verilmiştir.

TÜBİTAK-UEKAE tarafından kurulan TR-BOME, ülkemizin olası siber saldırılara karşı savunma gücünü tespit etmek, bilgi sistem güvenliği olaylarına müdahaledeki eksiklikleri ortaya çıkarmak ve kurumlarımızdaki bilgi güvenliği bilincini artırmak amacıyla Ulusal Bilgi Güvenliği Tatbikatları gerçekleştirmeyi kararlaştırmış ve ilk tatbikatı 20-21 Kasım 2008 tarihlerinde Cumhurbaşkanlığı, Başbakanlık, Adalet Bakanlığı, Sayıştay Başkanlığı, Hazine Müsteşarlığı, Merkez Bankası, Sermaye Piyasası Kurulu, Tapu ve Kadastro Genel Müdürlüğü katılımı ile gerçekleştirmiştir.

10.11.2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu ile de Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı'na (BTK);

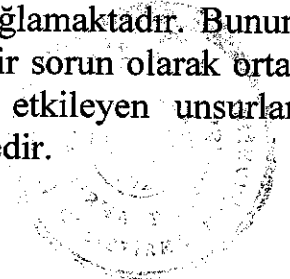
- Bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi,
- İzinsiz erişime karşı şebeke güvenliğinin sağlanması,
- Kişisel veri ve gizliliğin korunması,
- Elektronik haberleşme sektörüne yönelik olarak, milli güvenlik, kamu düzeni veya kamu hizmetinin gereği gibi yürütülmesi amacıyla mevzuatın öngördüğü tedbirlerin alınması görevleri verilmiştir.

TÜBİTAK - UEKAE, 5809 sayılı Kanun sonrasında ortaya çıkan durumu da göz önüne alarak, elektronik haberleşme işletmecilerinin katılımını da temin etmek amacıyla, 2010 yılı içinde yapılacak Siber Güvenlik 2010 Tatbikatını BTK ile birlikte düzenlemek için teklifte bulunmuştur. 5809 sayılı Elektronik Haberleşme Kanunu ile bilgi, şebeke ve haberleşme güvenliği konularında görevlendirilen BTK, Bilgi Toplumu Eylem Planı doğrultusunda siber güvenlik konusunda çalışmalar yapmakta olan TÜBİTAK-UEKAE ile işbirliği içinde, elektronik haberleşme sektöründe faaliyet gösteren istekli işletmecilerin katılımını da sağlayarak Ulusal Siber Güvenlik Tatbikatı'nı düzenlemenin, Ülkemizde siber güvenlik konusunda idari, teknik ve hukuki kapasitenin geliştirilmesine ve farkındalık oluşumuna önemli katkılar sağlayacağını değerlendirerek bu teklif kabul etmiştir.

Bu çerçevede, Siber Güvenlik 2010 Tatbikatı Bilgilendirme Toplantısı 29 Nisan 2010 tarihinde Bilgi Teknolojileri ve İletişim Kurumu'nda yapılmıştır. Toplantıya 23 farklı kamu ve özel sektör kuruluşundan 60'a yakın kişi katılmıştır. Toplantıda, katılımcılara 2008 yılında yapılan ve bu yıl içinde yapılacak olan tatbikat hakkında bilgi verilmiş ve konu ile ilgili görüş alış verişinde bulunulmuştur. Toplantı sonunda katılımcılardan tatbikata katılıp katılmayacakları hususundaki son kararlarını Bilgi Teknolojileri ve İletişim Kurumu'na iletmeleri istenmiştir. Bu talep doğrultusunda şu ana kadar 9 kurum ve kuruluş Siber Güvenlik 2010 Tatbikatına katılımını teyit etmiştir.

Ulusal Bilgi Sistemleri Güvenliği Tatbikatı 2010 Hazırlık Değerlendirme Toplantısı, BTK, TÜBİTAK- UEKAE, kamu kurum ve kuruluşları, özel sektör ve sivil toplum temsilcilerinin katılımıyla BTK'da yapılmış olup, Siber Güvenlik Tatbikatının 2010'un Ekim ayında gerçekleştirilmesi planlanmaktadır.

Ayrıca, bilgi ve iletişim teknolojileri son on yıllarda baş döndürücü bir hızla gelişmekte ve yayılmaktadır. Bu hızlı gelişim hayatın her alanını etkilemekte ve gerek bireyler gerekse de ülkeler açısından büyük yararlar sağlamaktadır. Bununla birlikte, siber ortamda güvenin ve güvenliğin sağlanması da bir sorun olarak ortaya çıkmaktadır. Siber ortamda güveni ve güvenliği olumsuz etkileyen unsurların başında da istek dışı elektronik posta (spam) mesajları gelmektedir.



Tüm dünyada elektronik posta mesajlarının yaklaşık %70'inin spam mesaj olduğu ifade edilmektedir. Spam mesajlar, e-posta sunucularını ve kullanıcıların posta kutularını gereksiz yere işgal ederek hoşnutsuzluk yaratmakta, aynı zamanda kötücül yazılımların yayılmasına da yardımcı olmaktadır. Ayrıca, internet servis sağlayıcıların işletmekte oldukları şebekeleri meşgul etmekte ve şebeke kapasitelerini doldurmaktadırlar.

Dünyadaki spam mesaj yayılımına bakıldığında Türkiye'nin en fazla spam mesaj yayan ülkelerden olduğu görülmektedir. IBM X-Force Trend İstatistiklerine göre 2007 yılında dünya sıralamasında %3,9'luk pay ile 8. sırada bulunan ülkemiz, 2008 yılında %8'lik pay ile 2. sıraya yükselmiştir. İşletmeciler açısından bakıldığında ise TTNET'in dünya işletmeciler sıralamasının en başında yer aldığı müşahade edilmektedir. Gerek Ülkemizin gerekse de Türk Telekom A. Ş.'nin bu durumu muhtelif zamanlarda ve zeminlerde hem ITU hem de OECD yetkililerince şikayet konusu olmuştur.

Bu hususlar göz önüne alınarak 2009 yılı başında BTK koordinatörlüğünde TTNET, Çizgi Telekom, Doruk Net ve Mynet'in işbirliğiyle "Spam ile Mücadele Pilot Projesi" uygulamaya geçirilmiştir. Pilot proje çıktılarının olumlu olması sonrasında Koç.net, Borusan, Superonline ve Türk Ticaret Net başta olmak üzere diğer ilgili tarafların da katılım ve katkılarıyla Spam ile Mücadele Projesi 15 Haziran - 19 Ekim 2009 tarihleri arasında tüm Türkiye'de 3 fazda uygulanmıştır. Proje sonucunda spam mesaj yayan IP sayısının % 99 civarında düşüş gösterdiği ve TTNET'in yaydığı günlük spam mesaj sayısının 6.5 milyar düzeyinden 394 milyon düzeyine indiği görülmüştür. Bu gelişme ülkemizin en fazla spam e-posta yayan ülkeler listesinden çıkmasını sağlamış olup, proje arzulanan amaçlarına ulaşmıştır.

Öte yandan, Ülkemizde mobil haberleşme hizmetlerinden (GSM ve 3G) yararlanan vatandaşlarımızın sayısı 65 milyonu aşmıştır. Ülkemizde son yıllardaki ekonomik gelişmeler ticari hayata önemli ölçüde canlılık kazandırmıştır. Vatandaşlarımızın büyük çoğunluğunun mobil hizmetlerden yararlanması ticari işletmelerin ürün ve hizmetlerini tanıtım için SMS, MMS gibi mesaj servislerini kullanmalarına yol açmıştır. Ülkemizde kişisel verilerin korunması konusunda yasal koruyucu tedbirlerin yeterli düzeyde olmaması sebebiyle vatandaşlarımızın mobil iletişim numaraları elden ele dolaşabilmekte ve bu numaralara vatandaşlarımızın rızası ve bilgisi dışında mesaj gönderilmektedir. Bu durum vatandaşlarımız açısından ciddi bir rahatsızlık haline gelmiştir.

5809 sayılı Elektronik Haberleşme Kanununun 50' nci maddesinin 5' inci fıkrasında; "Abonenin önceden izni alınmadan otomatik arama makineleri, faksler, elektronik posta, kısa mesaj gibi elektronik haberleşme vasıtalarının kullanılması suretiyle doğrudan pazarlama, siyasi propaganda veya cinsel içerik iletimi gibi maksatlarla istek dışı haberleşme yapılması halinde, abone ve kullanıcılara gelen her bir mesajı bundan sonrası için almayı reddetme hakkı kolay bir yolla ve ücretsiz olarak sağlanır." hükmü yer almaktadır.

Bu hükme göre abonelerin kendilerine gelen spam mesajları kolay bir yolla ve ücretsiz olarak reddedebilmeleri gerekmektedir. Ancak işletmecilerin uygulamalarına bakıldığında mezkur hükmün tam olarak karşılanmadığı görülmüştür.

5809 sayılı Elektronik Haberleşme Kanunu ile işletmecilerin istek dışı haberleşme hususu düzenlenmiştir. Ancak, bu düzenleme elektronik haberleşme sektöründe faaliyet gösteren işletmeciler ile sınırlı bulunmaktadır. Ülkemizde bu konuda genel bir düzenleyici işlem tesis etmek ve AB müktesebatına uyum çalışmaları bağlamında 2000/31 sayılı Elektronik Ticaret Direktifini uyumlulaştırmak amacıyla Adalet Bakanlığı'nca "Elektronik Ticaretin Düzenlenmesi Hakkında Kanun Tasarısı" hazırlanmış olup, bahse konu Tasarı ile işletmeciler dışındaki ticari işletmelere gönderdikleri mesajların kolay bir yolla ve ücretsiz olarak reddedebilmesini sağlama yükümlülüğü getirilmektedir.

Gerek işletmecilerin gerekse de diğer ticari işletmelerin gönderdikleri mesajların kolay bir yolla ve ücretsiz olarak reddedebilmesini teminen mobil haberleşme hizmeti sunan işletmecilerle birlikte çalışmalara başlanmıştır.

Bu çerçevede, mobil haberleşme hizmeti sunan işletmecilerle 3 Mart 2010 tarihinde çalışmalara başlanmış olup, şu ana kadar 4 toplantı gerçekleştirilmiştir. Çalışmalar neticesinde uygulanacak yöntem üzerinde işletmecilerle mutabakat sağlanmıştır. Mutabık kalınan yöntemin hukuki geçerliliğe kavuşturulmasını teminen bir Kurul Kararı alınması düşünülmektedir. Konu ile ilgili son görüş alışverişi yapılmakta olup, mezkur Kurul Kararının alınmasını müteakiben, mutabık kalınan yöntemin uygulanabilmesi için işletmecilerin belli bir miktar yatırım yapması gerektiğinden uygulamanın 01 Ocak 2011 tarihinde başlatılması düşünülmektedir.

Mobil haberleşme hizmeti sunan işletmecilerle yapılan çalışmanın bir benzeri Türk Telekom ile de başlatılmış olup, görüşmeler devam etmektedir.

Ayrıca, bilgi ve iletişim teknolojilerinin (BİT), sunduğu imkanları suistimal etmeyi amaçlayan taraflar; virüs, solucan (worm) , truva atı (trojans) gibi kötücül yazılımları ve istekdışı e-posta (spam) ve Köle Bilgisayar Ağları (KBA) gibi araçları kullanarak, bilişim sistemlerine yetkisiz olarak erişebilmekte, sistemlere zarar verebilmekte, sistemde bulunan bilgilere erişebilmekte, bu bilgileri çalabilmekte, değiştirebilmekte ve silebilmektedir. Teknolojik gelişmelere paralel olarak kötü niyetli kişilerin elindeki araçların sayısı ve niteliği ile bu kişilerin yol açtığı zararlar katlanarak artmaktadır.

Siber güvenlik ile ilgili çalışmalar yapmakta olan uluslararası kurum, kuruluş ve şirketlerin yaptığı araştırmalar incelendiğinde, ülkemizin gerek kötücül yazılımlara gerekse de KBA'lara (Köle Bilgisayar Ağları) kaynaklık eden ülkeler sıralamasında ön sıralarda yer aldığı tespit edilmiştir. Bu itibarla BTK bünyesinde siber güvenliğin sağlanması ve kötücül yazılımlarla mücadele edilmesini teminen ilgili tüm paydaşların katılım ve katkılarıyla çalışmalar başlatılmıştır.



Bu doğrultuda "Kötücül Yazılımlarla Mücadele Pilot Projesi (KYMP)'nin uygulamaya geçirilmesi düşünülmüştür. "Kötücül Yazılımlarla Mücadele Pilot Projesi" (KYMP) ile, İnternet ortamındaki kötücül yazılımlardan ve bu yazılımlar kullanılarak gerçekleştirilen saldırılardan etkilenen kurumsal ve bireysel kullanıcıların uyarılması, bilgisayar sistemlerine bulaşmış kötücül yazılımların temizlenmesi ve bu sistemleri hedef alan saldırıların bertaraf edilmesi için gerekli önlemlerin alınması hususlarında kullanıcılara destek olunması hedeflenmektedir. Bu çerçevede, "Kötücül Yazılımlarla Mücadele Pilot Projesi (KYMP)'nin Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı (BTD)'nin koordinasyonunda, İnternet Dairesi Başkanlığı (İDB)'nin katkı ve destekleriyle uygulamaya geçirilmesi, mezkûr Projenin ilgili kurum ve kuruluşlar ile işletmeciler dahil edilerek genişletilmesi için BTD tarafından gerekli çalışmaların yapılmasını müteakiben 13 Mayıs 2010 tarihinde BTK İstanbul Bölge Müdürlüğünde, Proje Bilgilendirme Toplantısı yapılmıştır. Toplantıya 33 erişim sağlayıcının temsilcisi katılmıştır. Toplantıda katılımcılara pilot proje hakkında bilgi verilmiş ve proje konusunda görüş alış verişinde bulunulmuştur. Toplantı sonunda projeye katılmak isteyen gönüllü tarafların 20 Mayıs 2010 tarihine kadar BTK'ya bilgi vermeleri talep edilmiş olup, bu talep doğrultusunda 4 işletmeci (Türk Telekom, TTNET, Turkcell ve Avea) pilot projeye katılacaklarını belirtmişlerdir.

Pilot Proje, sözkonusu İnternet Dairesi Başkanlığı'nın gerekli altyapıyı hazır hale getirmesini müteakip , ilk aşamada erişim sağlayıcıların katılımıyla başlayacak olup, ileriki aşamalarda büyük bilişim sistemi (MERNİS, UYAP gibi) işleten kurum ve kuruluşlar, TÜBİTAK gibi araştırma ve geliştirme kuruluşları, kolluk kuvvetleri ile IMPACT ve FIRST gibi uluslararası kuruluşların katılımıyla nihai yapısına kavuşacaktır. TÜBİTAK ve IMP ACT ile işbirliği sağlanması hususunda çalışmalar başlamış olup, kısa sürede tamamlanması planlanmaktadır.