



T.C.
ULAŞTIRMA DENİZCİLİK VE HABERLEŞME BAKANLIĞI
Strateji Geliştirme Başkanlığı

7/1905
GK 70

27 Haziran 2012

Sayı :B.11.0.SGB.0.01.00.610.02/1607

Konu : Bursa Milletvekili
Sayın Sena KALELİ'nin
yazılı soru önergesi

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

- İlgi: a) TBMM Başkanlığı'nın 19.12.2011 tarihli ve KAN.KAR.MD.A.01.0.GNS.0.10.00.02.00-7/1905-58920 sayılı yazısı.
b) Başbakanlığın 23.12.2011 tarihli ve B.02.0.KKG.0.12/610-2-491/4223 sayılı yazısı.

Bursa Milletvekili Sayın Sena KALELİ tarafından Sayın Başbakanımıza yöneltilen ve Sayın Başbakanımızın da kendileri adına Bakanlığımız koordinatörlüğünde cevaplandırılmasını tensip ettikleri 7/1905 esas sayılı yazılı soru önergesinin cevabı hazırlanarak ekte sunulmuştur.

Bilgilerinize arz ederim.


Binali YILDIRIM
Bakan

EK :

- 1) Cevap formu (3 Sayfa)
- 2) Bilgi Notu (3 Sayfa)

DAĞITIM:
TBMM Başkanlığına
Başbakanlığa



BURSA MİLLETVEKİLİ SAYIN SENA KALELİ'NİN
7/1905 ESAS SAYILI YAZILI SORU ÖNERGESİ VE CEVABI

Türkiye Avrupa Konseyi'nin "Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşmeyi" 1981 yılında imzalamıştır. Siber suçlara ilişkin düzenlenen ilk belge olma özelliğini taşıyan "Avrupa Siber Suçlar Sözleşmesi" ise geçtiğimiz yıl Strasbourg'da ülkemiz adına Dışişleri Bakanı Ahmet Davutoğlu tarafından imzalanmıştır. 48 maddeden oluşan Avrupa Siber Suçlar Sözleşmesi, özellikle telif haklarının ihlalleri, bilgisayarlarla ilgili sahtekarlık eylemleri, çocuk pornografisi, ağ güvenliğine ilişkin suçları tanımlamaktadır. Sözleşme, taraf olan ülkelere tanımlanan suçların işlenmesi ve söz konusu suçların işlenmesine yardım veya yataklık yapılmasını ulusal mevzuatta cezai bir suç olarak tanımlanma ve gerekli yasama işlemlerini ve diğer yükümlülükleri getirmektedir. Sözleşme, söz konusu suçlara yönelik soruşturma ve kovuşturmaların yanı sıra suçlara delil teşkil edebilecek verilerin toplanması, saklanması, araştırılması ve el konulması gibi ulusal düzeyde alınması gereken önlemleri de içermektedir.

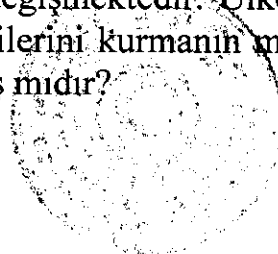
İmzalanan sözleşmeler gereği dolan yasal yükümlülükler ile alınması gereken önlemler konusunda ise ne yazık ki bugüne kadar hiçbir düzenleme gerçekleştirilmemiş ve atılan imzalar sembolik olmaktan öteye gidememiştir. Bu suçların en önemli yansımaları ise, hard disklerde bulunan bilgi ve belgelerin, çeşitli spekülasyonlara rağmen son yıllarda yürütülmekte olan birçok davaya delil teşkil etmesidir. Bu bağlamda;

SORULAR:

1-1981 yılında imzalanan "Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşmenin" üzerinden 30 yıl, Kasım 2010 tarihinde imzalanan "Avrupa Siber Suçlar Sözleşmesinin" üzerinden 1 yıl geçmesine karşın bu sözleşmelerin iç hukukumuzda uyarlanması konusunda neden adım atılmamaktadır?

2- Kaspersky Lab'in 2011 yılı 3. çeyrek kötü amaçlı yazılım raporuna göre, Türk bilgisayar kullanıcıları siber suçlar konusunda korumasız olup, gittikçe daha sık görülmeye başlanan siber suç vakaları kurumların mali durumları için her geçen gün daha fazla tehlike oluşturmaya başlamıştır? Bu konularla ilgili ülkemizdeki mevcut mevzuat ve yaptırımlar yeterli midir?

3- Ponemon Institute yıllık maliyet araştırmasına göre, siber suçların yol açtığı zarar dünyada yılda ortalama 5,9 milyon dolar, siber saldırıların neden olduğu kayıplar ise yılda 1,5-36,5 milyon dolar arasında değişmektedir. Ülkemizdeki maddi kayıpları önemli ölçüde azaltacak güvenlik teknolojilerini kurmanın maliyeti ne kadardır? 2012 bütçesinde bu konu için bir ödenek ayrılmış mıdır?



CEVAPLAR:

Adalet Bakanlıđından alına bilgilere gre; 108 sayılı Avrupa Konseyi Szleşmesinin onay srecinin tamamlanabilmesi iin, halen Bařbakanlık'ta bulunan "Kiřisel Verilerin Korunması Hakkındaki Kanun Tasarısı"nın kanunlaşması, kiřisel verilerin korunması ile grevli tam bağımsız bir denetim makamının ihdas edilmesi gerekmektedir. Diđer yandan 95/46/EC sayılı Avrupa Birliđi Direktifi de Szleşme ile paralel hkmler iermekte ve Avrupa Birliđi ile yrtlen mzakere srecinde i hukuka aktarılması gerekmektedir. Dolayısıyla hem 108 sayılı Avrupa Konseyi Szleşmesinin onay sreci, hem de adı geen Direktifinin i hukuka aktarılması birbiriyle eř zamanlı olarak yrtlmesi gerekmektedir. Zira Kiřisel Verilerin Korunması Hakkındaki Kanun Tasarısının kanunlaşması ile her iki hukuk metninin i hukukta ngrdđ dzenlemeler kabul edilmiř olacaktır.

Adalet Bakanlıđınca; "Kiřisel Verilerin Korunması Hakkındaki Kanun Tasarısı"nın, Avrupa Birliđi Mktesebatına uyumlu bir řekilde kanunlaşmasını temin etmek zere, Hollanda Ekonomi Bakanlıđınca finanse edilen ve Considerati-Van Doome firmalarının oluřturduđu ortaklık ile yrtmekte olan "Kiřisel Verilerin Korunması Hakkındaki Kanun Tasarısının Desteklenmesi Projesi G2G10/TR/9/1" kapsamında birtakım faaliyetler gerekleřtirilmiřtir. ncelikle, Proje Grubu, Avrupa Birliđinin Adli Yardımlaşma Birimi olan Eurojust'a, Hollanda Veri Koruma Kurumuna ve Telekomnikasyon Kurumuna bir alıřma ziyareti dzenleyerek, bu kurumların veri koruma politikalarını ve uygulamaya dnk alıřmalarını yerinde inceleme ve uzmanlarla grř alıřveriřinde bulunma imkanı elde etmiřtir. Proje kapsamında yapılan bařka bir faaliyet de mevcut tasarının AB Mktesebatına uyumunu deđerlendirmek amacıyla Van Doorne Hukuk Firması ve Proje ortađı akademisyenlere taslak incelettirilerek grřleri alınmıřtır. Bir bařka nemli faaliyet ile de, Proje ortaklarını, Trk akademisyenlerin ve bađı saygıdeđer Milletvekillерimizin katılımıyla 6 Ekim 2011 tarihinde Ankara' da, kamu kesimine ynelik bir seminer ve hemen ardından 7 Ekim 2011 tarihinde de zel sektre ynelik İstanbul' da ikinci bir seminer dzenlenmiřtir.

Tasarının Avrupa Birliđi Mktesebatına uyum sađlaması halinde 108 sayılı Avrupa Konseyi Szleşmesine de uyum sađlamıř olacađı ve onay srecinin bařlatılabileceđi deđerlendirilmektedir.

Halihazırda, lkemizde, siber sular, 5237 sayılı Trk Ceza Kanunu'nun "Biliřim Alanında Sular" bařlıklı 10'uncu blmnde yer alan hkmler ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Dzenlenmesi ve Bu Yayınlar Yoluyla İřlenen Sularla Mcadele Edilmesi Hakkında Kanun hkmleri bařta olmak zere diđer bađı kanunlarda da kısmen dzenlenmektedir.

Ayrıca, Bilgi Teknolojileri ve İletişim Kurumu Başkanlığınca; 2009 yılında, internet servis sağlayıcı ve yer sağlayıcı firmaların katılımıyla birlikte, siber güvenliğe yönelik tehdit oluşturan ve internet kaynaklarını gereksiz meşgul eden istek dışı (spam) e-postaların engellenmesine yönelik olarak bir pilot proje yürütülmüştür. Söz konusu pilot projenin başarılı olması sonrasında ise e-posta gönderiminde kullanıcı kimlik doğrulaması için kullanılan 25'nci Portun kapatılarak yerine 587'nci Portun açılması çözümü tüm Türkiye geneline 3 faz halinde yaygınlaştırılmıştır.

Proje sonrasında,

- Spam e-posta yapan IP sayısı % 99 oranında azalmış,
- Spam e-posta yayan ülkeler sıralamasında ilk 3'te yer alan ülkemiz ilk 10'un gerilerine düşmüş,
- Dolayısıyla ülkemizin uluslararası bilişim arenasındaki imajı güçlendirilmiştir.

Bilgi Teknolojileri ve İletişim Kurumu'nun son yıllarda, ulusal çapta bir siber güvenlik kültürünün oluşturulması ve farkındalığın arttırılması, teknik kapasitenin arttırılması ve uluslararası işbirliğinin sağlanmasına yönelik olarak yürütmekte olduğu ve yürütmeyi planladığı birçok benzeri çalışma bulunmaktadır.

Ülkemizde, birçok kurum ve kuruluşu, internete açık kurumsal şebekelerinin güvenliğini arttırmak amacıyla saldırı tespit sistemi (IDS), saldırı önleme sistemi (IPS), güvenlik duvarı (firewall), antivirüs yazılımları ve benzeri güvenlik araçları kullanılmaktadır.

Öte yandan Ulusal siber güvenliğin sağlanması amacıyla TÜBİTAK tarafından gerçekleştirilen ve gerçekleştirilmesi planlanan çalışmalar hakkında bilgi notu Ek 1'de sunulmaktadır.

ULUSAL SİBER GÜVENLİĞİN SAĞLANMASI AMACIYLA TÜBİTAK TARAFINDAN GERÇEKLEŞTİRİLEN ÇALIŞMALAR

1. Tamamlanan Çalışmalar

a) Kalkınma Bakanlığı (Devlet Planlama Teşkilatı) Bilgi Toplumu Dairesi tarafından hazırlanan Bilgi Toplumu Stratejisi Eylem Planı 2006 - 2010 belgesinin 88 numaralı maddesinde tanımlanan "Ulusal Bilgi Sistemleri Güvenlik Programı" isimli projede sorumlu olarak TÜBİTAK-UEKAE belirlenmiştir. Bu projenin kapsamı "Siber alemdeki güvenlik tehditlerini sürekli olarak takip edecek, uyarılar yayınlayacak, bu risklere karşı ne şekilde tedbir alınabileceğine dair bilgilendirme yapacak, risklerin ortaya çıkması durumunda karşı tedbirleri koordine edebilecek bir "bilgisayar olaylarına acil müdahale merkezi (CERT)" kurulacaktır. Kamu kurumları için gerekli minimum güvenlik seviyeleri kurum ve yapılan işlem bazında tanımlanacak, kurumlar tarafından kullanılan sistem, yazılım ve ağların güvenlik seviyeleri tespit edilecek ve eksikliklerin giderilmesi yönünde öneriler oluşturulacaktır." ifadesi tanımlanmıştır. Bu proje 2006 - 2010 yılları arasında yürütülmüştür. Programın bütçesi 5.248.000 TL'dir. Program kapsamında gerçekleştirilen çalışmalar aşağıda özetlenmiştir:

- Ulusal Bilgi Güvenliği Kapısı www.bilgiguvenligi.gov.tr adresinden hizmet vermeye başlamıştır. Halihazırda üçbinin üzerinde üye ve 135 adet yazar yer almaktadır. Yazarların %40'ı TÜBİTAK dışıdır.
- Yirmi kamu kurumundan 131 personele 21 farklı alanda bilgi güvenliği eğitimleri verilmiştir.
- 71 üniversiteden 93 bilgi işlem personeline bilgi güvenliği eğitimleri verilmiştir.
- Dokuz kamu kurumuna, BOME (Bilgisayar Olaylarına Müdahale Ekibi) kurma danışmanlığı verilmiştir. BOME kurulum danışmanlığının bitmesine müteakip bu kurumlar ile birlikte Kasım 2008'de BOME-2008 Siber Güvenlik Tatbikatı yapılmıştır.
- Dört kamu kurumuna ISO 27001 tabanlı Bilgi Güvenliği Yönetim Sistemi (BGYS) kurulum danışmanlığı verilmiştir. Beş kamu kurumuna sızma testi yapılmıştır.
- Bilgisayar kullanıcılarına yönelik hazırlanmış, multimedya içerikli, interaktif bölümlerin olduğu bilgi güvenliği bilincinin artırılmasına yönelik portal www.bilgimikoruyorum.org.tr adresinden yayına başlamıştır.
- **Ulusal Siber Güvenlik Tatbikatı 2011**, yaklaşık bir yıl süren hazırlık sürecinin ardından 25-28 Ocak tarihlerinde 39 kurum/kuruluşun katılımıyla gerçekleşmiştir. Tatbikat organizasyonunu BTK ve TÜBİTAK yapmıştır. USGT 2011 kapsamında 500'ün üzerinde yazılı enjeksiyona ilave olarak port taraması, dağıtık servis dışı bırakma saldırıları, web uygulamalarının denetimi ve kayıt dosyası (log)

analizinden oluřan gerek saldırılar yapılmıřtır. Kurumlara zel tarama ve analiz raporları resmi olarak iletilmiřtir. Kurumlara zel olmayan tatbikat sonu raporu hazırlanmıřtır.

- b) Bankacılık Dzenleme ve Denetleme Kurumunun řubat 2011'de yaptıėı dzenleme ve TBİTAK'a yaptıėı talep sonucunda Trkiye'de faaliyet gsteren 31 bankanın (sahip oldukları aktifler asında Trkiye'nin %96'sına sahip) bilgi sistemlerine sızma testi yapılmıřtır. Halihazırda, BDDK'nın talebi doėrultusunda Trkiye Bankacılık Sektr Siber Gvenlik Analiz Raporu hazırlanmaktadır.

2. Gerekleřtirilecek alıřmalar

- a) 2012 Yatırım Programı'nda "**Kamu Bilgi Gvenliėi Programı**" ve "**Kritik Altyapılarda Bilgi Gvenliėi Ynetimi – Tespit, Analiz, nlemler**" isimli iki adet siber gvenlik projesinin yer alması planlanmaktadır. Her iki proje de Kalkınma Bakanlığı Bilgi Toplumu Dairesi ile birlikte bir seneye yakın bir srede yapılan deėerlendirmeler sonucunda oluřturulmuřtur. Her iki projenin temell ilkesi, siber gvenlik konusunda kurumsal kapasite geliřtirmek olarak benimsenmiřtir. Projeler hakkında zet bilgi ařaėıda sunulmuřtur.

Kamu Bilgi Gvenliėi Programı

- Toplam proje btesi 4.119.400 TL'dir.
- TBİTAK UEKAE Biliřim Sistemleri Gvenliėi Grubu deneyimlerinden ve Ulusal Siber Gvenlik Tatbikatı 2011'in sonuları incelendiėinde siber gvenlik asından lkemizdeki problemin en genel ifadeyle yetenek eksikliėi olduėu grlmektedir. Kamu kurumlarında alıřan bilgisayar mhendisleri ve biliřim uzmanlarında siber gvenlik bilinci ve bilgisinde grlen eksikliėi gidermek ve kamu kurumlarında alıřan mhendis ve uzmanları siber gvenlik konusunda kurumsal ihtiyaları karřılayacak seviyeye getirmek amacıyla Kamu Bilgi Gvenliėi Programı hazırlanmıřtır. Kamu Bilgi Gvenliėi Programı, **Eėitim, Bilgi Bankası Oluřturulması ve Risk Analizi** olmak zere  projeden oluřmaktadır.
- Eėitim projesi kapsamında halihazırdaki eėitimler geliřtirilecek, yeni siber gvenlik eėitimleri hazırlanacak ve bu eėitimlerin verilmesi suretiyle kapasite artırımı saėlanacaktır.
- Bilgi Bankası Oluřturulması Projesi kapsamında kamu kurumlarının ihtiyaı olan bilgi birikimi, kılavuzlar, teknik kontrol listeleri, saldırılardan korunma ve saldırılarla mcadele el kitapları hazırlanarak artırılacaktır.
- Risk Analizi Projesi kapsamında, kamu kurumlarının sahip olduėu bilgi gvenliėi risklerinin 6 ayda bir yapılacak testlerle tespit edilmesi ve nceki sonularla karřılařtırılarak hem kurumun geliřiminin hem de ihtiyalarının tespitinin yapılması

amaçlanmaktadır. Eğitim ve Bilgi Bankası Oluşturulma Projelerinin etkinliğinin ölçülmesi de bu projeyle sağlanacaktır.

Kritik Altyapılarda Bilgi Güvenliği Yönetimi – Tespit, Analiz, Önlemler

- Toplam proje bütçesi 1.590.780 TL'dir.
- Kritik altyapılar devlet düzeninin ve toplumsal düzenin sağlıklı bir şekilde işlemesi için gerekli olan ve birbirleri arasında bağımlılıkları olan fiziksel ve sayısal sistemlerdir. Enerji üretim ve dağıtım sistemleri, telekomünikasyon altyapısı, finansal servisler, su ve kanalizasyon sistemleri, güvenlik servisleri, sağlık servisleri ve ulaştırma servisleri en başta gelen kritik altyapılar olarak sıralanabilir. OECD üyesi ülkeler, Avrupa Birliği, ABD, Kanada gibi gelişmiş ülkeler kritik altyapıların korunması ile ilgili çalışmalara başlamışlar ve ciddi yol almışlardır. Bütün kritik altyapılar içerisinde bilgi teknolojileri yoğun olarak kullanılmaktadır. Bu durum ise, kritik altyapıları siber tehditlere karşı açık hale getirmektedir. Bu proje eğer kapsamında, kritik altyapıların tespiti ve analizi amacıyla ülkemizde gerçekleştirilen ilk çalışma olacaktır. Proje kapsamında, Türkiye'nin kritik altyapılarının tespiti yapılacak ve bilgi teknolojilerinden kaynaklanan açıklıkların kritik altyapılara etkisi analiz edilecektir. Sektör bazlı pilot çalışma gerçekleştirilecektir. Proje kapsamında kritik altyapılarda kullanılan SCADA bilgi sistemleri için simülasyon ortamı oluşturulacaktır. Proje sonucunda toplam 10 adet doküman hazırlanmış olacaktır. Bu dokümanların en önemlileri Türkiye'de kritik altyapılar ve kritik altyapıların BT güvenlik durumu dokümanı ve diğer kritik altyapılara yaygınlaştırılma için yol haritası dokümanıdır.

