7/37802
6.K.93

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

Sayı : 44697349-610[01]/23506
Konu : İstanbul Milletvekili
Sayın Mustafa Sezgin TANRIKULU'nun
yazılı soru önergesi

20 Mayıs 2014

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

İlgi: a) TBMM Başkanlığı'nın 28.01.2014 tarihli ve KAN.KAR.BŞK.43452547-120.00-7/37802-275325 sayılı yazısı.
b) Başbakanlığın 30.01.2014 tarihli ve 31853594-610-2-7375-791 sayılı yazısı.

İstanbul Milletvekili Sayın Mustafa Sezgin TANRIKULU tarafından Sayın Başbakana yöneltilen ve Sayın Başbakan tarafından da kendileri adına Bakanlığımız koordinatörlüğünde cevaplandırılması tensip edilen 7/37802 esas sayılı yazılı soru önergesinin cevabı hazırlanarak ekte sunulmuştur.

Bilgilerinize arz ederim.

Lütfi ELVAN
Bakan

EK: 1) Cevap formu (5 Sayfa)

DAĞITIM:
TBMM Başkanlığı'na
Başbakanlığa

Hakkı Turayliç Caddesi No:5 06338 Emek / Çankaya / ANKARA
Telefon: 203 13 45 Faks: 213 07 60
E-posta: sgb1@udhb.gov.tr Internet Adresi: www.udhb.gov.tr
Ayrıntılı bilgi alınacak kişi:
C. Tanfer TEMİZKAN
Şef

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

İSTANBUL MİLLETVEKİLİ SAYIN MUSTAFA SEZGİN TANRIKULU'NUN 7/37802 ESAS SAYILI YAZILI SORU ÖNERGESİ VE CEVABI

International Data Corporation'ın (IDC) Mayıs 2012'deki Küresel Korsan Yazılım Kullanımı raporunda Türkiye'de lisanssız yazılım kullanım oranının yüzde 62 olarak görüldüğü, Türkiye'nin siber korsanların adeta hedefi haline gelme riskini olduğu belirtilmektedir. Ayrıca, tüm dünyaya duyurulan 'Siber Güvenlik Bildirisi' ile güvenlik güçlerini hedef alan siber saldırıları savaş sebebi sayıldığı, ülkemizde ise bu konuda henüz yeterli adımların atılmadığına dikkat çekiliyor.

Türkiye'de Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın bulunduğu, ama bu planın öncelikli olarak kamu kurum ve kuruluşlarını içine aldığı, telekomünikasyon, enerji ve finans gibi kritik sektörlerde, henüz zorunluluk noktasında bir aksiyon alınmadığı belirtilmektedir. Bu konuda şirketlerde de düşük bir farkındalık seviyesi olduğu, bunun da bu konudaki riski arttırdığı ifade edilmektedir.

Bu bağlamda;

SORULAR:

1-Kamu veya özel sektör kurum ve kuruluşlarının siber saldırılara maruz kalmamaları, maruz kaldıkları takdirde en az zarar görmeleri, bu saldırılardan çıktıktan sonra en kısa zamanda normale dönülmesi için yapılan herhangi bir çalışma var mıdır? Varsa, bu çalışma ilgili kurumlara bildirim yapılmış mıdır ve hangi yolla yapılmıştır?

2-lnternational Data Corporation'ın (IDC) yayınladığı veriler doğruyu yansıtmakta mıdır? Doğruyu yansıtıyorsa, bu verinin neden olduğu risklerin bertaraf edilmesi için yapılan herhangi bir çalışma var mıdır?

3- Kamu kurumlarında herhangi bir korsan yazılım kullanılmakta mıdır?

4-Kamu kurumlarında herhangi korsan bir yazılım kullanılmaması için yapılan bir çalışma var mıdır?

5-Stratejik konumdaki bir kamu kurumu veya özel sektör işletmesine bir siber saldırı olması durumunda, bu saldırıyı yapanların nasıl cezalandırılacağı yönünde alınan bir karar var mıdır?

6-Siber saldırı farkındalığının kamu kurumları veya özel sektör firmalarında yaratılması için herhangi bir çalışma yapılması öngörülmektedir?

CEVAPLAR:

Siber güvenlikle ilgili alınacak önlemleri belirlemek, hazırlanan, plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla kurulan Siber Güvenlik Kurulu, yaptığı ilk toplantısında Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planını kabul etmiştir. Söz konusu eylem planı 20/06/2013 tarihinde Bakanlar Kurulu kararı olarak 28683 sayılı Resmi Gazetede yayımlanmıştır. Eylem planı 2013-2014 döneminde gerçekleştirilmesi planlanan işleri tanımlamakla birlikte bu yılları aşan periyodik faaliyetler ile eğitim ve bilinçlendirme çalışmaları gibi sürekli yürütülmesi gereken faaliyetlere de yer vermektedir. Ulusal Güvenlik Stratejisi ve 2013-2014 Eylem Planı, kamu bilişim sistemlerini ve kamu ya da özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerini kapsamaktadır.

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının 4 numaralı eylemi kapsamında, ülkemizde yaşanabilecek siber olaylara müdahale edebilecek ve ulusal ve uluslararası koordinasyonu sağlayacak olan Ulusal Siber Olaylara Müdahale Merkezi (USOM) 27 Mayıs 2013'de kurulmuştur. Yine aynı eylem maddesi kapsamında herhangi bir siber saldırıya uğrayan kurum ve kuruluşların USOM ile işbirliği içerisinde çalışarak bu saldırıya müdahale etmek ve kurumun siber güvenliğini sağlamak amacıyla kamu kurum ve kuruluşları bünyesinde Kurumsal Siber Olaylara Müdahale Ekiplerinin (Kurumsal SOME) kurulması çalışmaları devam etmektedir. Özel sektörde özellikle kritik sektörlerde faaliyet gösteren kuruluşlar bünyesinde Kurumsal SOME kurulması çalışmaları ilgili sektörü düzenlemekten ve denetlemekten sorumlu kurumlar vasıtasıyla yürütülmektedir.

USOM'un koordinasyonunda 7/24 müdahale esasına göre çalışacak SOME'ler (Siber Olaylara Müdahale Ekipleri) için 11 Kasım 2013 tarihinde ' SOME Çalışma Usul ve Esasları Hakkında Tebliğ " Resmi Gazetede yayımlanmıştır. Kurumsal SOME'ler Bakanlıkların bünyesinde, hizmet gereklerine göre, Bakanlık birimlerini, bağlı, ilgili ve ilişkili kurumlarını, Sektörel SOME'ler ise kritik altyapılara sahip düzenleyici ve denetleyici kurumların bünyesinde kendi sektörlerinde faaliyet gösteren kurum, kuruluş ve işletmeleri kapsamaktadır. Sektörel SOME'lerin bulunduğu sektörlerdeki özel kurumlar ve diğer kuruluşlar kendi bünyelerinde kurumsal SOME kurabilmektedir. Tebliğde geçen Kurumsal SOME kurmak yükümlülüğünde olan kurumların faydalanması amacıyla, Kurum temsilcilerinin katılımı ile birlikte "Kurumsal SOME Kurulum ve Yönetim Rehberi Dokümanı" hazırlanmıştır.

Söz konusu dokümanda, Kurumsal SOME'lerin siber olay öncesi, siber olay esnası ve siber olay sonrasındaki temel görev ve sorumlulukları belirtilmektedir. Rehber ayrıca SOME'lerin kurum içi farkındalık çalışmalarının gerçekleştirilmesi, kurumsal bilişim sistemleri sızma testlerinin yapılması / yaptırılması, kayıtların düzenli olarak incelenmesi çalışmalarını yürütmelerinin gerekliliği ile Kurumda herhangi bir siber olayın gerçekleşmesi durumunda görevlerini nasıl yerine getireceklerini, siber olaya müdahale ederken yapmaları gereken prosedürler, siber olay gerçekleştikten ve olaya müdahale edildikten sonra yapmaları gereken görevler hakkında detaylı bilgiler ve formlar içermektedir. Ayrıca, eş zamanlı olarak Sektörel SOME'ler için "Sektörel SOME Kurulum ve Yönetim Rehberi Dokümanı" hazırlanmıştır.

Ayrıca siber saldırılara karşı önlem alınması, kurumların bilgi ve iletişim sistemlerinin güçlendirilmesi amacıyla; Ulusal Siber Güvenlik Tatbikatları ve Gelişmiş Siber Saldırıları Tespit etmeye yönelik Analiz çalışmaları da yapılmaktadır.

20/06/2013 tarih ve 28683 sayılı Resmi Gazetede yayımlanan, Ulusal Siber Güvenlik Stratejisi ve 2013-2013 Eylem Planı çerçevesinde kamu kuruluşlarına yönelik siber saldırıların önlenmesi ve zararlı yazılımların etkisinin azaltılması adına yürütülen projeler aşağıda sunulmuştur:

a) Yazılım Güvenlik Programı,
b) Siber tehditleri tespit amacıyla Balküpü sistemi kurulması,
c) Siber Tehditleri Önleme Projesi (STOP) yürütülmesi, siber tehditlerinin tespit edilmesi, izlenmesi ve önlenmesine ilişkin gerekli mekanizmaların geliştirilmesi,
d) Kamu kurum ve kuruluşlarının internet sayfalarının yerli veri merkezlerine taşınması,
e) Dışarıya veri sızması olayların tespite yönelik test altyapısı geliştirilmesi ve uygulamaya alınması.

Ayrıca, Bilişim suçu işleyen kişilerin nasıl cezalandırılacakları ile ilgili düzenleme 5237 sayılı Türk Ceza Kanununun 243. ve 244. maddelerinde düzenlenmiştir. Ayrıca, Siber Güvenlik Kanun Taslağı çalışmaları, Adalet Bakanlığı'nın koordinasyonunda Bakanlığımız ve diğer ilgili kurum ve kuruluşların da katılımıyla devam etmektedir.

Siber saldırı farkındalığının hem kamu hem de özel sektörde yaratılması amacıyla Ulusal Siber Güvenlik Strateji Belgesi ve 2013-2014 Eylem Planında;

a. Siber saldırı farkındalığının artırılması için siber güvenlik eğitim altyapısının güçlendirilmesi,
b. Siber güvenlik tatbikatlarının düzenlenmesi,
c. Üniversitelerde siber güvenlik eğitimlerinin yaygınlaştırılması,
d. Siber güvenlik uzmanlığına yönlendirme programının yürütülmesi,
e. İlk, orta, lise öğretimi ve yaygın eğitimde siber güvenlik eğitimlerinin yaygınlaştırılması,
f. Bilgisayar kullanıcılarının siber güvenlik konusunda bilinçlendirilmesi,
g. Ulusal ve uluslararası siber güvenlik etkinlikleri düzenlenmesi,
h. Ar-ge faaliyetlerinin teşvik edilmesi

gibi konular eylem olarak yer almakta olup, bu konularda eğitim, ulusal ve uluslararası düzeyde tatbikatlar ve konferans çalışmaları periyodik olarak düzenlenmektedir.

Bu kapsamda, siber güvenlik tatbikatları önemli bir yer tutmaktadır. Ülkemizde de, TÜBİTAK koordinesinde 2008 yılında gerçekleştirilen ilk ulusal siber güvenlik tatbikatından sonra çok daha geniş bir katılımcı grubuyla BTK ve TÜBİTAK koordinesinde 2011 yılında Ulusal Siber Güvenlik Tatbikatı gerçekleştirilmiştir.

Ulusal Siber Güvenlik Tatbikatı 2011 finans, bilgi teknolojileri ve iletişim, eğitim, savunma, sağlık sektörlerinin; adli birimlerin, kolluk kuvvetlerinin ve çeşitli bakanlıkların ilgili birimlerinin temsilcilerinden oluşan 41 kamu kurumunun, özel sektör kuruluşunun ve sivil toplum kuruluşunun katılımıyla 25-28 Ocak 2011 tarihlerinde yapılmıştır. Bu tatbikatta katılımcı kurum/kuruluşlardan 200'e yakın personel görev almıştır.

2012 yılının Mayıs ayında BTK koordinasyonunda elektronik haberleşme sektöründe faaliyet gösteren 12 işletmecinin katılımı ile gerçekleştirilmiştir. *"Siber Kalkan Tatbikatı 2012"* Tatbikata, sektörde en fazla Pazar payına sahip olan erişim sağlayıcı operatörler katılmıştır. 50'nin üzerinde erişim sağlayıcı personeli ile 30'un üzerinde BTK uzmanının görev yaptığı "Siber Kalkan Tatbikatı 2012", 8-22 Mayıs 2012 tarihleri arasında gerçekleştirilmiş ve Dağıtık Hizmeti Engelleme Saldırıları (DdoS –Distributed Denial of Service) simüle edilmiş, bu saldırılara karşı alınan güvenlik önlemlerinin yeterliliği değerlendirilmiştir. Her bir işletmeciye ayrı ayrı uygulanan bu saldırılar boyunca toplamda 100 Terabit'in üzerinde trafik hedef sistemlere gönderilmiştir.

Sözkonusu trafik yurtiçi ve yurtdışından 150 farklı kaynaktan hedef sistemlere yöneltilmiştir. 23-28 Mayıs 2012 tarihleri arasında ise katılımcılara yazılı senaryolar gönderilerek, bu senaryolara verdikleri tepkiler analiz edilmiştir. Tatbikat ile erişim sağlayıcıların kendi içlerindeki ve bir üst erişim sağlayıcı ile koordinasyon kabiliyetinin belirlenmesi hususlarında başarı sağlanmış, siber olaylara müdahalede ulusal düzeyde koordinasyon yeteneği ile bilgi ve tecrübe paylaşımının geliştirilmesi, bilinçlendirme ve farkındalık oluşturulması ve nihayetinde ulusal siber güvenlik kabiliyetlerimizin arttırılması konusunda önemli bir adım atılmıştır.

Son olarak, 24 Aralık 2012 - 11 Ocak 2013 tarihleri arasında Bakanlığımız koordinasyonunda BTK ve TÜBİTAK tarafından birlikte yürütülen" Ulusal Siber Güvenlik Tatbikatı 2013" , 61 kamu ve özel sektör kuruluşunun katılımıyla gerçekleştirilmiştir. Bu tatbikat, elektronik haberleşme, enerji, savunma, finans ve sağlık gibi kritik altyapıları yöneten ve işleten kurum ve kuruluşları kapsamış, katılımcıların sadece teknik değil, aynı zamanda hukuk ve iletişim birimlerinden de personelleri görev yapmıştır. Tatbikatta gerek katılımcı personel sayısı ve gerekse simüle edilen siber saldırıların çeşitliliği konusunda önceki etkinliklere göre gelişim sağlanmış farkındalığın artırılması yönünde önemli kazanımlar elde edilmiştir.

Ayrıca Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı uyarınca 2014 yılı içerisinde uluslararası bir tatbikatın düzenlenmesi ve ulusal siber güvenlik tatbikatlarının iki yılda bir tekrar edilmesi öngörülmektedir.