7-4433
GK.113

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

25 Nisan 2012

Sayı : B.11.0.SGB.0.01.00.610.01/1225
Konu : Ankara Milletvekili
Sayın Emine Ülker TARHAN'ın
yazılı soru önergesi

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

İlgi: 27.02.2012 tarihli ve A.01.0.KKB.0.10.00.00-50441 sayılı yazınız.

Ankara Milletvekili Sayın Emine Ülker TARHAN'ın 7/4433 esas sayılı yazılı soru önergesinin cevabı hazırlanarak ekte sunulmuştur.

Bilgilerinize arz ederim.

Binali YILDIRIM
Bakan

EK :
1) Cevap formu (2 Sayfa)

Hakkı Turayliç Caddesi No:5 06338 Emek / Çankaya / ANKARA
Telefon: 203 13 45
Faks: 203 13 86
E-posta: sgb1@ubak.gov.tr
Internet Adresi: www.ubak.gov.tr

Ayrıntılı bilgi alınacak kişi:
Şakir ÖZDEMİR
Şube Müdürü

ANKARA MİLLETVEKİLİ SAYIN EMİNE ÜLKER TARHAN'IN 7/4433 ESAS SAYILI YAZILI SORU ÖNERGESİ VE CEVABI

Telekomünikasyon sektörünü düzenleme ve denetleme fonksiyonunun bağımsız bir idari otorite tarafından yürütülmesi amacıyla kurulmuş olan Bilgi Teknolojileri ve İletişim Kurumu'nun (BTK) veritabanının, Anonymous hacker grubu tarafından ele geçirildiğini ve sosyal paylaşım sitesi Twitter üzerinden yayınlandığını, basına yansıyan haberlerden öğrendik.

BTK'nın 4 farklı veri tabanını ele geçiren grubun Vodafone, TurkNet, Superonline, Avea, Turkcell gibi uzaktan erişen firmaların bilgilerini kriptolu bir biçimde yayınladığı; veritabanlarının dördüncüsündeki bilgilerin en açık bilgileri barındırdığı ve bu veri tabanının BTK çalışanlarının kullanıcıların tam isimleri, kullanıcı adları, e-postaları, açık biçimde şifreleri, ev-cep-iş telefonları, doğum tarihi, TC kimlik numaralarından oluştuğu, yine basındaki haberlere yansıdı.

Bu bağlamda;

SORULAR:

1-Bilgi Teknolojileri ve İletişim Kurumu, hacker saldırısına ne zaman uğramış ve veri tabanındaki bilgiler ne zaman çalınmıştır?

2-Hackerlerin elde ettiği bilgiler arasında, şirketlerin ve özel kişilerin "kişisel" nitelikteki bilgileri bulunmakta mıdır?

3-Heckerların BTK veritabanlarını ele geçirmek için kullandıkları sistemdeki açık tespit edilebilmiş midir?

4-Adı "Bilgi Teknolojileri" olan bir kurum, kendine ve bağlı olan şirketlere ait bilgileri neden koruyamamıştır? Kurumda teknolojik açıdan bir zaaf mı vardır?

5-Türkiye'de, internet üzerinde adeta bir sansür kurumu gibi çalışan BTK'nın, mesaisini sansürlenecek web sitesi aramaya harcamak yerine sistemlerini daha güvenli hale getirmek için harcamasına yönelik yapılan bir çalışma var mıdır?

6-Kurum bu güvenlik açıklarını kapatmak üzere ne gibi önlemler almış ve almayı planlamaktadır?

CEVAPLAR:

Bilgi Teknolojileri ve İletişim Kurumu internet siteleri sürekli siber saldırıya maruz kalmaktadır. tuketici.btk.gov.tr adresinde tüketici şikayetlerini almak ve çözmek amacıyla işletime açılan site de açıldığı günden itibaren yoğun saldırı altındadır. 12.02.2012 saat 10:30 civarı tuketici.btk.gov.trinternet sitesinin ana sayfasının değiştirilmeye çalışıldığı tespit edilerek anında müdahale edilmiş, sistemin erişimi kesilmiştir.

5809 sayılı Elektronik Haberleşme Kanununun 4 ve 6 ncı maddeleri ile Elektronik Haberleşme Sektöründe Tüketici Hakları Yönetmeliği'nin 13. Maddesi ile ilgili diğer mevzuat hükümleri kapsamında hazırlanan "Tüketici Şikayetlerinin Çözümüne İlişkin Usul ve Esaslar" uyarınca BTK'na yapılan başvurularda kurum internet sayfasında yer alan tüketici şikayet formunun kullanılması esastır. Bu çerçevede BTK'na yapılacak tüketici şikayet başvurularında tüketicilerden talep edilecek bilgiler içinde 4982 sayılı Kanun referans alınmış olmakla birlikte, bir abone üzerine aynı TC kimlik numarası ile birden fazla hat tanımlı olabildiğinden, başvuran abonenin şikayetinin hangi numaraya karşılık gelen hattıyla ilgili olduğunun tespiti açısından ilgili Kanun'da belirtilen bilgilere ilave olarak abonelerden telefon ve/veya hizmet numaraları da talep edilmiştir. Bu bilgiler şikayetlerin çözümü aşamasında kullanılmak için gerekli olan bilgiler olup sadece bu amaçla kullanılmıştır. Söz konusu bilgiler dışında abonelerden eğitim düzeyi, meslek gibi bilgilerin istenmesi sözkonusu değildir.

tuketici.btk.gov.tr sitesinde yaşanan bahse konu olay sistemsel bir açıktan dolayı gerçekleşmemiştir. Kurum güvenlik sistemlerinde herhangi bir açık söz konusu değildir. Sözkonusu sitenin altyapısını oluşturan ve satın alınan bir paket yazılımın kaynak kodundaki "SQL Injection" a imkan veren yazılımsal hata tespit edilmiştir.

BTK, sadece tuketici.btk.gov.tr sitesi için değil, diğer tüm bilişim altyapısı için gerekli güvenlik önlemlerini almıştır ve almaya devam etmektedir. Ancak siber dünyadaki istihbarat kuruluşlarının, global ölçekli büyük firmaların ve ülkemizdeki siyasi partilerin internet sitelerinin maruz kaldıkları hack olayları dikkate alındığında %100 oranında siber güvenliği sağlandığını iddia edebilmek mümkün değildir. BTK bilgi güvenliğinin bir süreç olduğunun bilincinde olarak gerekli ve güncel güvenlik önlemlerini almak suretiyle maksimum düzeyde siber saldırılara hazırlıklı olmayı amaçlamış, bu yönde gerekli önlemleri almış ve almaya devam etmektedir. Bu açıdan yaşanan bu olayı BTK'da teknolojik açıdan bir zafiyet bulunduğu olarak değerlendirmek doğru bir yaklaşım olarak değerlendirmemek gerekir. Kaldı ki BTK bilişim sistemlerinin güvenliğinin sağlanması amacıyla zaten çeşitli çalışmalar yapmaktadır ve bu çalışmalar yaşanan olayla başlamış değildir.

Yukarıda da belirtildiği üzere saldırganlar tuketici.btk.gov.tr sitesini değiştirmeye çalışırken, bilinen tabiriyle hacklenmeye çalışılırken sistem durdurulmuştur. Yapılan teknik inceleme ile saldırıya imkan veren kod hatası tespit edilmekle birlikte sistem kullanıma kapatılmış bunun yerine yeni sistem hazırlıkları başlatılmıştır. Bu olay sonrasında BTK rutin güvenlik çalışmalarının yanı sıra tüm sistemlerini test etmiş olup zaten var olanların yanı sıra ilave güvenlik projelerini hayata geçirmek üzere çalışmalarına devam etmektedir.