**TÜRKİYE BÜYÜK MİLLET MECLİSİ**

| YASAMA DÖNEMİ | YASAMA YILI |
|---|---|
| 24 | 2 |

# (10/108, 155, 156, 157, 158, 159, 160) ESAS NO'LU BİLGİ TOPLUMU OLMA YOLUNDA BİLİŞİM SEKTÖRÜNDEKİ GELİŞMELER İLE İNTERNET KULLANIMININ BAŞTA ÇOCUKLAR, GENÇLER VE AİLE YAPISI ÜZERİNDE OLMAK ÜZERE SOSYAL ETKİLERİNİN ARAŞTIRILMASI AMACIYLA KURULAN MECLİS ARAŞTIRMASI KOMİSYONU

# TUTANAK DERGİSİ

***17 Mayıs 2012 Perşembe***

# (10/108, 155, 156, 157, 158, 159, 160) ESAS NO'LU BİLGİ TOPLUMU OLMA YOLUNDA BİLİŞİM SEKTÖRÜNDEKİ GELİŞMELER İLE İNTERNET KULLANIMININ BAŞTA ÇOCUKLAR, GENÇLER VE AİLE YAPISI ÜZERİNDE OLMAK ÜZERE SOSYAL ETKİLERİNİN ARAŞTIRILMASI AMACIYLA KURULAN MECLİS ARAŞTIRMASI KOMİSYONU

# GÖRÜŞME TUTANAKLARI

**17 Mayıs 2012 Perşembe**

----0----

**K O N U**



**İ Ç İ N D E K İ L E R**



**Açılma Saati: 12.05**
**Kapanma Saati: 13.45**

BİRİNCİ OTURUM

Açılma Saati: 12.05

BAŞKAN : Necdet ÜNÜVAR (Adana)

BAŞKAN VEKİLİ : Yıldırım M. RAMAZANOĞLU

SÖZCÜ : İlhan YERLİKAYA (Konya)

----0----

BAŞKAN – Bilişim ve İnternet Araştırma Komisyonunun çok değerli üyeleri, değerli konuklarımız, değerli uzmanlarımız ve değerli basın mensupları; hepinizi saygıyla selamlıyorum.

Bugün 17 Mayıs Dünya Telekomünikasyon Günü. Öncelikle Bilişim ve İnternet Araştırma Komisyonu olarak bunu kutluyoruz.

Tabii, bugün çok üzüntülü de bir günümüz. Hatay'da 3 askerimiz şehit oldu, Allah'tan onlara rahmet diliyoruz. Birisi Binbaşı olmak üzere 3 askerimizi kaybettik. Cenabıhak makamlarını yüce etsin, cennetiyle kavuştursun. Tabii, böyle bir acılı günde de olsa Bilişim ve İnternet Araştırma Komisyonu olarak çalışmalara maalesef devam etmek durumundayız. Çünkü ülkemiz açısından son derece önemli konular gündeme geliyor. Bugün de iki önemli kurum, TÜBİTAK ve TÜRKSAT sunum yapacak. Özellikle TÜBİTAK'ın sunumu siber güvenlik çalışmaları ağırlıklı bir sunum olacak.

Bu sunum için bugün basın mensuplarımızdan özür diliyoruz. Görüntü alıp onları bugün için dışarıya davet edeceğiz. Daha sonra bir basın bülteniyle bilgileri onlara takdim edeceğiz.

Evet, çok teşekkür ediyorum. Basın, görüntülü kaydı aldıktan sonra sunumumuza başlayacağız.

İlk sunumu TÜBİTAK yapacak.

Buyurun.

TÜBİTAK BİLGEM UEKAE MÜDÜR YARDIMCISI DR. HAYRETDİN BAHŞİ – Sayın Başkanım, sayın vekillerim ve saygıdeğer arkadaşlar; TÜBİTAK'ta Ulusal Elektronik Kriptoloji Araştırma Enstitüsünde siber güvenlikten sorumlu Müdür Yardımcısıyım. Bugün aslında siber güvenlikle ilgili yapılan çalışmaları, yaptığımız bazı çalışmaları anlatacağım ve ülkede yapılması gereken çalışmalara değinmek istiyorum. Aslında yaptığımız çalışmalara da değinirken aslında onlar bizim siber güvenlikle ilgili yapılması gereken bazı çalışmaların çekirdeği ya da altyapısı olduğu cihetiyle değineceğim. O çalışmaların daha nasıl büyütülmesi gerekiyor, ne yapılması gerekiyor, onları anlatmaya çalışacağım.

Şimdi siber güvenliğin önemini anlatmadan hemen geçiyorum. Çünkü onlar zaten size anlatıldı. Belki siber güvenlikteki asıl problem, doğrudan yapılanların anlatılması ve yapılacakların acilen hayata geçirilmesi. O sebeple önlem meselesini atlıyorum sunumumda.

İlk olarak bizim yaptığımız, dediğim gibi, ülke açısından önemli, büyük ölçekli ve ülkenin siber güvenliğini etkileyen çalışmalara değineceğim. Daha sonra da bir siber güvenlik yol haritası önerimiz var. Burada ülkede neler yapılması gerektiğine kısaca değinmeye çalışacağım.

Bir slaytla çok kısa bizim yaptığımız çalışmaları anlatacağım genel olarak bir özet geçmek açısından.

Biz ulusal bilgisayar olaylarına müdahale ekibini yönetiyoruz. Bu ekip bir bilgisayar güvenlik olayı olduğu zaman farklı kurumlar arasındaki koordinasyonu gerçekleştiren, aynı zamanda önleyici tedbirler

açısından da kurumları gerektiği zaman uyaran ve onların da bilgisayar olaylarına müdahale cevap mekanizmalarını etkin olarak kurmaları konusunda danışmanlık yapan, aslında aynı zamanda önleyici mekanizmalar konusunda da bilgilendiren bir yapı. Aynı zamanda bu ulusal bir kontakt noktası. Uluslararası diğer ülkelerle ilgili bir siber güvenlik olayı olduğunda onlarla bir temas noktası olarak da çalışıyor. Örneğin Hollanda'yla bir ihtiyacınız var, orada bir saldırı var, bu saldırının kaynağının önlenmesiyle ilgili bilgi isteğini bu ulusal kontakt noktasına iletebilirsiniz, onlar da Hollanda'nın ulusal kontakt noktasına ileterek bu şekilde koordine ediliyor.

Bunlar ne kadar etkin oluyor? Kanuni mevzuat ülkeden ülkeye değiştiği için, diğer meselelerde olduğu gibi, her zaman yüzde 100 etkili olmuyor ama ortada böyle bir denenebilecek. mekanizma var en azından.

Bizim grubumuz bilişim sistem güvenliği danışmanlığı konusunda özellikle kamu kurumlarına, isteyen özel sektöre, aynı zamanda diğer güvenlik kurumlarına yardımcı oluyor. Özellikle sistemlerin bir hacker bakış açısıyla denetlenmesi, test edilmesi, bu konularda eğitimler verilmesi ve sadece olayın teknik boyutu değil aynı zamanda kurumların bilgi güvenliği yönetiminin politikasını ve prosedürlerini ortaya koymasıyla ilgili çalışmalara da destek veriyoruz.

Aynı zamanda siber güvenlik alanında şöyle bir konsept vardır, o da bir IT bilişim sistem ürününün güvenlik olarak değerlendirilmesi. Bununla ilgili de çalışmalarımız var. Uluslararası olarak kabul edilen değerlendirmeleri yapıyoruz.

Aynı zamanda büyük ölçekli, ülkedeki mesela botnet ağlarının tespit edilmesi, yayılan kötücül yazılımların tespit edilmesi gibi daha geniş ölçekli proje çalışmalarımız da var.

Aslında siber güvenlik adına en büyük çalışma Ulusal Bilgi Sistemleri Güvenlik Programı'ydı. Bu Devlet Planlama Teşkilatının yayınladığı Bilgi Toplumu Stratejisi'nin 88'inci maddesiydi. Burada bilgisayar olayları müdahale koordinasyon merkezînin kurulması öngörüldü. Burada aynı zamanda biz bir portal hazırladık bilgi güvenliği kapısı, www.bilgiguvenligi.gov.tr içerisinde. Burada özellikle teknik anlamda güvenlik tedbirlerinin nasıl alınacağıyla ilgili bilgiler yayınlıyoruz. Aynı zamanda detaylı kılavuzlar yazıyoruz ki, bir bilgi sistem uzmanı bunları alıp sistemlerini güvenli hâle getirebilsin diye. Aynı zamanda sistemlerde bulunan kritik açıklıkları, belirli yazılımlarda kullanılan, onları da yayınlıyoruz. Bu kapı aslında bütün ülkenin teknik ekspertizlerinin yazı yazabileceği şekilde oluşturulmuş. Yüzde 50-60'ına biz katkı veriyoruz ama bu önemli bir şey.

Bilgi sistemleri güvenlik eğitimleri verildi kamu kurumlarına. Yaklaşık olarak 131 personele burada eğitim verdik, değişik danışmanlık çalışmaları yaptık. O zaman sanal ortam demiştik, şu anda belki siber güvenlik diyoruz. Kamu kurumlarıyla birlikte çalışarak bir taslak, ulusal sanal ortam güvenlik politikası metni de hazırlandı 2007 yılında.

En önemli, yaygın çalışmalarımızdan biri Ulusal Siber Güvenlik Tatbikatıydı. Bu BTK'yla birlikte yapıldı Ocak 2011'de. Gerçekten büyük bir tatbikat, gerçek saldırıların yapıldığı. Ve özellikle burada kurumların böyle saldırılara karşı tepkilerini ne kadar hızlı gösterebildikleri ve ne kadar etkin bunlara müdahale ettikleri ölçülüyor bu tür tatbikatlarda. Daha çok güvenlik açıklarının tespiti yerine bu reaksiyon

mekanizmasının etkinliği ölçülüyor. Burada 500 üzerinde deneme yapıldı. Bunun hem gerçek tarafı vardı hem de yazılı ortamda, işte böyle bir durum olursa ne yaparsınız gibi bir yazılı kısmı da vardı. O çalışmaları da yaptık ve bunun her bir kuruma özel onların sonuçlarının raporlarını ilettik ve aynı zamanda genel bir tatbikat sonuç raporu yayınladık. Bu TÜBİKAK ve BTK'nın sitelerinden ulaşılabilecek bir rapor. Ve bunun yenisini 2013 Ocakta planlamaya başladık. 39 kurum ve kuruluş katılmıştı. Bunu çok daha genişleteceğiz, yaklaşık olarak 80'e yaklaştıracağız. Aynı zamanda üniversitedeki gençlerin de yeteneklerini ölçen bir yarışmayı da önümüzdeki senenin başında yapacağımız çalışmada ele alacağız.

Aslında çok önemli bir konu, bizim siber güvenlik adına bu ülkede yapılması gereken en önemli işlerden biri olarak özellikle regülasyon yapan kurumların, denetleme ve düzenleme yapan kurulların siber güvenliği denetleme olarak ele alması gerektiğini düşünüyoruz. Mesela BDDK gerçekten bu konuda etkin bir mekanizma kurdu. BTK da bu konuda iyi çalışmalar yaptı. Yani BDDK, bankaların uyması gerektiği siber güvenlik kanunları konusunda onlara kurallar belirledi. Mesela yapılması gereken çalışmalardan biri, bankacılık sistemlerinin üçüncü bir farklı göz tarafından incelenmesi ve gerçekten sistem güvenlik açıklıkları var mı yok mu, bunların raporlanması üzerine. Her sene yapmak zorunda. Bunu bağımsız kurumlar yapmak durumunda. 2011 yılında BDDK "Siz bunu yapın." dedi bize bütün bankaları test etme amacıyla. 32 bankayı gerçekleştirdik. Bu da aslında aktifler açısından yüzde 97'yi kapsıyor. Ve bunların her birine sızma testi yaptık. Bunların yapılmasından ziyade aslında bankacılık sektöründeki genel durumu da özetleyebildik siber güvenlik açısından ve bununla ilgili bir raporu da BDDK'ya sunduk. BDDK bu rapor sonucunda da siber güvenlikle ilgili alınması gereken tedbirleri ya da uygulanması gereken ek tedbirleri belirliyor, belirleme aşamasında. Aynı zamanda bir çalıştay düzenleyeceğiz bütün bankalarla birlikte. Genel değerlendirme yapmak açısından BDDK düzenleyecek bunu, biz de katılacağız. Ve şu anda bu çalışmalar devam ediyor. Hem bu sektörde biz sızma testi yapma açısından bir standart yakalanmasını sağlamaya çalışıyoruz hem de bankacılık sektörünün genel resmini görmeye çalışıyoruz. Aslında yapılması gereken şey, bunun diğer sektörlerde de gerçekleştirilmesi. BDDK telekomünikasyon alanında bunu gerçekleştirdi. Belki enerji sektöründe bunu yapmak, sağlık sektöründe bunu yapmak gerekli.

Özellikle şu anda siber güvenlik adına kritik altyapı tanımı var. Yani bizim kritik altyapılarımız, sağlık sistemlerimiz, ulaştırma sistemlerimiz siber güvenlik açısından önemlidir. "Bunların gerekli tedbirleri alması gerekir." şeklinde bir çalışma var. Özellikle Amerika'da şu anda Cyber Security Act, bu konuda bir kanun hazırlığı içerisinde, Temsilciler Meclisinin onayını bekliyor. Belirli aşamalardan geçti. Orada da özellikle bu kritik altyapılar ki, sivil taraf tarafından şey yapılan, diğer özel şirketler tarafından da yönetilen. Aslında bu altyapıların ülkenin güvenliği açısından çok önemli olduğu ortaya konuluyor ve bunların gerekli tedbirlerini alması gerektiği… Orada kanun mevzuat açısından öyle bir yapı yapılıyor. Aslında bizim bu faaliyetlerimizi buna bir altyapı olarak düşünebilirsiniz. Biraz sonra ele alacağım DPT'nin verdiği bir kritik altyapı projesi var. Burada da diğer sektörlerdeki durumun genel resmini çekmeye çalışacağız TÜBİTAK olarak ve burada da o sektörlerde alınması gereken minimum güvenlik tedbirlerinin ortaya konulmasını ve sektörel risk analizini gerçekleştireceğiz. Yani bunu o işin somut bir başlangıcı olarak düşünebilirsiniz.

Evet, Kalkınma Bakanlığı tarafından finanse edilen ve bize verilen bir program bu. Burada aslında ülkede hangi kritik bilgi sistemleri var. Bunlardaki altyapı nedir ve bunlardaki riskler nedir? Sektörel risk çalışması yapacağız. Bunun sonunda da her sektörde alınması gereken tedbirler belirlenecek.

Bu işin sektörel olmasının şöyle bir avantajı var. Aslında güvenlik dediğimiz şey güvenlik ile kullanılabilirlik arasındaki bir denge. Yani bu regüle ederken de, düzenlerken de sizin bu dengeyi de gözetmeniz lazım. Öyle kurallar manzumesi koyarsınız ki sistem çalışmaz ve gerçekten aslında oradaki altyapının çalışmaması da regülasyon kurumu için de önemli bir nokta. Yani orada kullanılabilirlik-güvenlik dengesini sektörel anlamda düşünüp, oradaki riskleri sektörel anlamda ele alıp öyle düzenleme yapmakta fayda var ve bu düzenleme yönteminin uygulanması gerçekten ülkede siber güvenliğin sağlanması açısından bizde çok kritik bir faktör. Onlar işi ele aldı mı ve biliyoruz ki bu regülatör kurumlarımız hızlı çıkartabiliyorlar, denetleme yapabiliyorlar. Bunu hem o tarafa adapte bir şekilde yapabilirler hem de etkin olarak ilerleyebilirler.

Bir de bunun tabii kamu tarafı var. Kamu bilgi sistemleri güvenliğiyle ilgili bir program da başlattık. Burada özellikle bu alandaki en önemli problem, bu konuda bilgi sahibi, tecrübe sahibi sistem personelinin olmamasıdır. Bu çok kritik bir problemdir. Hatta Amerika bile kendi içerisinde bunu çözmeye çalışıyor. Özellikle federal kurumlarda vesaire "Böyle adamları ben nasıl yerleştiririm, nasıl tutarım, nasıl yetiştiririm?" üzerine çalışıyor. Şu andaki Cyber Security Act'de bir alt başlık "Federal kurumlarda bunları geliştiririm?" Bu proje kapsamında biz BT sistemleri güvenliği sertifikasyonu ortaya koymaya çalışacağız. Yani bir sistem yöneticisi belirli eğitimleri almak durumunda, belirli bir seviyede bilgi birikimi olup, evet, bu kişi siber güvenlik konusunda bu kurumda etkin olarak çalışabilir gibi bir çalışma yapacağız, onlara sertifika vereceğiz. Aynı zamanda kamu kurumlarının sistemlerinin test edilmesi de bu kapsamda öne alınacak. Ayrıca Bilgi Bankası Projesi var. Bizim bilgiguvenligi.gov.tr adı altında yaptığımız çalışmaları genişleteceğiz.

Avrupa Birliğiyle bir projemiz var yedi üniversiteyle birlikte çalıştığımız. Onlarla birlikte de geleceğin İnternet tehditleri nedir, onlar üzerinde çalışıyoruz.

NATO'yla bazı çalışmalarımız var. Bunu çalıştık diye anlatmak istemiyorum. NATO'da nasıl yapılıyor bu işler, onu anlatmak için koydum. NATO'da eğer siz kritik bir sistem geliştiriyorsanız, bunun geliştirme aşamasından itibaren güvenlik tedbirlerine uyup uymadığını kontrol eden bir mekanizma geliştirmiş. Yani siz yazılımcılara sadece "Git yazılımı yap getir." demiyorsunuz, aynı zamanda bunun paralel bir güvenlik sertifikasyonu var. STM şu anda "Air Command and Control Information System" adı altında bir proje gerçekleştiriyor. Biz onlara bilgi güvenliği, siber güvenlik konusunda danışmanlık veriyoruz ki, NATO akreditasyondan geçsin. Bu NATO'ya yapılan bir proje. Bunun başka bir şeyi de Afganistan için "Afghanistan Mission Network Integration Core" diye bir sistem var, onu yapıyorlar. Yani burada özellikle temel mantalite şu NATO'nun da uyguladığı: Bir sistemi en sonunda oluşturduktan sonra test yapmak değil. Sistemin daha gereksinim aşamasından itibaren bu sistemin gerekli güvenlik fonksiyonları nedir, tasarlarken gerçekten bunlar uygulanmış mı gibi çalışmalar yapılması gerektiğini… Öyle bir akreditasyon sistemi kurmuş.

Biz de şöyle bir şey öneriyoruz: Eğer gerçekten bu *kritik* altyapıda kullanılacak bir bilgi sistemi varsa, bunun başından itibaren güvenlik kriterlerine uyup uymadığını akredite edecek bir yapının oluşturulmasının gerektiğini düşünüyoruz. Bu altyapının yapılması gerekiyor. Biz bu tür danışmanlık, yani çalışmalar yapıyoruz.

Bunun bir fizibilite çalışması yapılıp büyük bir program hâline getirilmesi lazım. Yani gereksinim aşamasında şu yapılır, tasarım aşamasında şu yapılır, test aşamasında şu yapılır ve sadece bir sistemi geliştirme değil. Aslında siz onu hayata koyduktan sonra onda her zaman yeni bir açıklık çıkabilir. Onu da yönetilecek mekanizmaya koymanız gerekiyor. Bu yapı onu da kapsıyor. Mesela bir ürün aldınız. Ortak kriterler laboratuarı bunu yapıyor. Mesela güvenlik duvarı dediğimiz, sistemlerimizde kullanılan önemli bileşen var. Gerçekten bu isteneni yapıyor mu, gerçekten fonksiyonlarını icra ediyor mu, bunun değerlendirilmesini yapan bir standart var. Bu standart uluslararası bir standart ve kurumlar bunları şey olarak kullanıyorlar. Mesela ben bir güvenlik duvarı alacaksam şu seviyede değerlendirilmiş bir güvenlik duvarı alacağım gibi genel kurallar koyuyorlar. Böyle kuralların da özellikle kritik sistemler için kullanılması gerektiğini düşünüyoruz. Şu anda bizim verdiğimiz sertifikalar... Biz aslında laboratuarız, TSE bunun sertifikasını veriyor. Teknik laboratuarı biziz. Biz testlerimizi yapıyoruz, sonucunu TSE'ye veriyoruz, o da akredite ediyor. Böyle bir durumda işte aslında kritik sistemler için şu bileşenler geliştiriliyorsa, bizim "En az şu derecelendirmeyle değerlendirilmesi gerekir." dememiz gerekiyor. Bunun altyapısı da şu anda Türkiye'de var. Bu kuralları koyması gerekiyor. Örnek vereyim, Gelir İdaresi Başkanlığı şu anda bir IP bazlı yazarkasa çalışması yapıyor. Yani şu anda her kurum… Belki normal yazarkasalarımızı network'a bağlayacağız, ağa bağlayacağız ve bunun birçok siber güvenlik tehdidi olacak ve ülkeyi de etkileyebilir bir açıklık çıktığı zaman. Şu anda işin başından itibaren bu sistemlerin uyması gerektiği güvenlik kurallarını belirliyoruz ve bunların şu anda akredite edilmesi, öyle kullanılması gerektiğiyle ilgili bir protokol imzaladık, o çalışmaları yapıyoruz. Mesela, özellikle yurt dışında, Amerika'da bu elektrik sistemlerini yöneten, işte sizin ne zaman hangi elektriği tükettiğiniz, gerekirse bunu yönetmekle ilgili çalışmalar var. Yani size diyoruz ki: Mesela "Ütü yapacaksanız gece yapın ki, minimize olsun." gibi. Mesela bunları yönetmek için akıllı sistemler geliştiriyorlar ve uyguluyorlar. Şimdi onların da en temel problemi, hem kişisel gizlilik problemini çözmek hem de güvenlik problemlerini çözmek. Buna yavaş yavaş biz de adapte olacağız, biz de bu sistemleri muhtemelen kullanmaya başlıyoruz. İşte başlarken eğer biz baştan güvenlik tedbirlerini ve önlemleri alarak yaparsak daha sağlıklı bir süreç olur. Yani aslında bazı şeyleri biz takip edici pozisyondayız ama takip ediciliğin şöyle bir avantajı var: Eğer siz oradan öğrenirseniz hataları, çok daha hızlı ve çok daha sağlıklı bir şekilde adapte edebilirsiniz. Güvenlik açısından bunu da yapabiliriz. Mesela bizim geliştirdiğimiz kimlik kartlarıyla ilgili alt bileşenlerin testleri burada yapıldı. Bazı başka bize taleple gelen ürünlerin de değerlendirilmeleri gerçekleştirildi. Biz değişik kurumlara güvenlik danışmanlığı vermeye devam ediyoruz.

Aynı zamanda, tabii, siber güvenlikle ilgili bilgilendirme, bilinçlendirme faaliyetleri çok önemli. Bu konuda etkinlikler ve sempozyumlar düzenliyoruz. Bunları çok uzun geçeceğim.

BAŞKAN – On dakikada bitiriyorsunuz.

TÜBİTAK BİLGEM UEKAE MÜDÜR YARDIMCISI DR. HAYRETDİN BAHŞİ – Tabii, bitiyor şu anda Başkanım.

Ulusal bilgi güvenlik kapısı var. Şu anda burada, dediğim gibi, Türkiye'deki bütün güvenlik uzmanları yazı yayımlayabiliyor. Burada "güvenlik bildirisi" dediğimiz güvenlik açıklıkla ilgili bilgilendirme de yapıyoruz.

Aslında güvenlikteki en zayıf halka kullanıcılar ve hackerlar genelde bu en zayıf halkayı hedef alırlar. Mesela bir bankacılık sisteminde bankalar tedbirlerini önemli bir şekilde alıyorlar özellikle İnternet bankacılığı kısımlarında. Ama kullanıcıların aslında bilgi güvenliği tedbirlerini alması hayati öneme sahip. Bu konuda www.bilgimikoruyorum.org.tr isimli bir site geliştirdik. Burada akademik destek de aldık. Burada akademik destek de aldık. Akademik destek dediğim, o işin öğrenme tarafı, nasıl yapılır? Bir son kullanıcı acaba bunu görsel ve ses öğelerle nasıl daha iyi algılayabilir? Böyle bir site oluşturduk. Burada bir kullanıcının izlemesi gereken tedbirleri anlatıyoruz. Mesela bazı kurumlar bunları bizzat kendi kurumlarına, kendi iç sayfalarına alabilir miyiz diye bizden izin aldılar. Biz alabilirsiniz referansı verdik ki, problem değil, zaten bunun için yapıyoruz. Yani kurum içerisinde de, bakın siz siber güvenlikle ilgili tedbirleri bu şekilde öğrenebilirsiniz gibi, bunlar da kurum tarafından da kendi içlerinde kullanılıyor.

Bu sene, iki üç gün önce haberleri de yayınlandı, bir siber güvenlik yaz kampı düzenleyeceğiz. Burada 50 tane genci, özellikle üniversite 3'üncü ve 4'üncü sınıflarda ve master seviyesindeki gençleri alıp, onlara sekiz günlük bir eğitim vereceğiz, onlarla birlikte bir yarışma düzenleyeceğiz. Bunun amacı şu: Sonuçta burada teknik, bu işi bilen insanların azlığını biliyoruz. Bu konuda yardımcı olacağını düşünüyoruz. İkinci gün şu anda bize yaklaşık olarak 430 tane başvuru geldi. 50 kişiyle bu işi yapacağız diye… Daha 6 Hazirana kadar da devam edecek. Burada aynı zamanda bu sektörde çalışan, bu sektörde uzman olan kişilerin de konuşma yapmasıyla ilgili bir ortam hazırlayacağız. Bunu, Gebze'de TÜSSİDE var bu tür eğitimlerin yapıldığı, TÜBİTAK ve Millî Eğitim Bakanlığının ortaklaşa kurduğu bir kurum, orada gerçekleştireceğiz.

Siber güvenlik tatbikatını da 2013 başında tekrar yapacağız.

Ben siber güvenlikle ilgili ülkede yapılması gereken yol haritasını sunacağım. Şimdi bizim yaptığımız faaliyetler aslında büyük işlerin alt başlıkları ya da altyapıları ya da belki bazıları çekirdekleri. Şimdi bizim bunun üst yapısını kurmamız gerekiyor ülkede. Yani burada bir ulusal siber güvenlik koordinasyon kurulu kurulması gerektiğini düşünüyoruz ki, diğer ülkeler böyle yapıyorlar. Siber güvenlik dediğimiz şey bir kurumun uhdesinde olan bir şey değil. Her bakanlığın bu işin içerisinde olması gerekiyor ve siber güvenlikle ilgili çalışmalara eğer kendileri destek olmazsa zaten önemli bir problem var. Yani standartlar der ki: Aslında bilginin sahibi gerçekten bunun korunmasını sağlamalıdır ve bunun yönetimi de bunu sağlamalıdır. Dolayısıyla, burada her bir ilgili bakanlığın temsil edildiği, ilgili düzenleyici kurumların temsil edildiği bir koordinasyon kurulu kurulması gerektiğini düşünüyoruz. İlk olarak bir siber güvenlik politikası oluşturulması gerektiğini düşünüyoruz. Böyle bir taslak doküman hazırlandı üç sene önce. Hızlıca bunun revize edilebileceğini ve hızlıca bu dokümanın yayınlanabileceğini düşünüyoruz. Bu doküman kapsamında da bir ulusal siber güvenlik eylem planı oluşturulması gerektiğini ve bunun da koordine edilmesi ve gerçekten bu kurulun da icrai yetkisinin olması gerektiğini düşünüyoruz. Gerçekten bu planı da takip etmeli; yani gerçekleştirdi mi, gerçekleştirmedi mi, ilgili raporlama mekanizmaları da kurulmalı.

Peki, burada eylem planında neler olabilir? Özellikle kritik altyapıları düzenleyen ve denetleyici kurumların siber güvenliği ele almalarının çok kritik bir faktör olduğunu düşünüyoruz. Yani eğer onlar ele alırlarsa çok hızlı bir şekilde *diffüz* edebilir siber güvenlikle ilgili önlemler.

Kamu Bilgi Güvenliği Programı'nın, bizim başlattığımız bu çalışmanın köklü, devam eden bir program hâline gelmesi gerektiğini düşünüyoruz.

Ulusal İnternet Sürekliliği Programı. Siber güvenlikle ilgili alınması gereken tedbirlerin aslında çoğunlukla kurum bazlı değil, birçok paydaşın birlikte koordine edebilerek alabileceği tedbirler. Bir kurumda siz 100 tane uzman koysanız belirli saldırıları o 100 tane kişiyse yapamazsınız. Mesela servis sağlayıcılarla koordine olmanız gerekir, diğer ülkelerdeki servis sağlayıcılarla koordine olması gerekir. Yani siber güvenlikle ilgili konferanslara gittiğiniz zaman söylenen ilk şey "koordinasyon, koordinasyon, koordinasyon." Dolayısıyla, burada bizim Ulusal İnternet Sürekliliği Programı önerimizde hem servis sağlayıcıları, bunları düzenleyen kurum ve ilgili birimler yer alıp, bir ülkede çok geniş kapsamlı bir saldırı olduğu zaman biz bunu nasıl önleyeceğiz, mesela nasıl o anda minimize edeceğiz, kalıcı olarak yapabilir miyiz ya da bunu minimize edebilir miyiz, bizim hangi sistemlerimiz var kritik ve bunları nasıl koruyabiliriz, bunların bir planlaması gerekli ve bu planın da hep belirli periyotlarla, belki tatbikatlarla net olarak test edilmesi gerekiyor. Ve bu çok paydaşlı bir iş. Belki de kanuni olarak da bir yerlerde bunun sorumluluğunun verilmesinde fayda var.

Yazım Güvenliği Programı. Biraz önce söylediğimiz bunu aslında sadece yazılım değil genel olarak ele alabiliriz. Bizim bir sistem geliştirirken sonunda değil başından itibaren güvenlik tedbirlerinin uygulandığı mantaliteyi yerleştirmemiz lazım. Bunu yerleştirmek için de bir program öneriyoruz. Bunun alt başlıklarıyla ilgili çalışmalar yapıyoruz ama çok daha kapsamlı yapılmalı, insanlar bu konuda bilgilendirilmeli, bilinçlendirilmeli ve biraz önce söylediğim gibi, eğer kritik bir bilgi sistemi varsa ve bu geliştirilecekse bunların bir akreditasyon yapısı olmalı.

Tabii bu "kritik" tanımı çok önemli. Yani bunu çok basit sistemler için yapmamak lazım. O zaman iş gücü kaybı var. Şu anda Amerika'da Temsilciler Meclisine sunulan Cyber Security Act'te tanım direkt olarak ülkenin güvenliğini doğrudan çok etkileyecek sistemler, güvenlik problemi olduğu zaman bir vatandaşın hayatına mal olacağı sistemler, aynı zamanda ülkenin çok büyük ekonomik kayba uğrayabileceği sistemler. Yani böyle gerçekten kritik yani sistemleri tanımlayıp, onun üzerinde bu sistemlerin geliştirilme sürecindeki akreditasyonu ortaya koymamız lazım.

Kötücül yazılımlar şu anda çok önemli. En önemli problem siber güvenlikle ilgili budur. Özellikle artık sizin virüs tespit sistemlerinizle tespit edemeyeceğiniz hedefe odaklı kötücül yazılımlar yazılıyor ve bilgilere erişiliyor. Bu konuda çok daha geniş kapsamlı mücadele programı yapılması gerekiyor. Biz şu anda TİB'le bir proje başlattık. Ülkedeki kötücül yazılımların tespit edilmesi, onların bir haritasının çıkarılması ve bunun kaynaklarının neler olduğunun tespit edilmesi ve onların belki de kara listelere alınması konusunda bir çalışma başlattık. Bu çalışma hızlı bir şekilde devam ediyor.

Siber güvenlik uzmanları yetiştirmemiz gerekiyor. Bu konuda çok destekleme programı oluşturmamız lazım. DPT'nin bize verdiği o şey aslında çekirdek olacak. Biz bir sertifikasyon ortaya koyacağız ve belki her kamu kurumundan en az 2 kişi, 3 kişi belki böyle bir destekleme programına üye olmalı ya da böyle bir sertifikayı alması lazım diyebiliriz.

Üniversitelerde siber güvenlik eğitimi. Şunu çok net söyleyebilirim. Ben de doktorum, akademik çalışmalar yaptım ama gerçekten siber güvenlikle ilgili akademik personel sayısı çok az. Ben bir elin beş

parmağını geçmez diyebilirim bu konuda. Özellikle yeni çıkan bu kötücül yazılımlarla ilgili, yeni çıkan siber tehditleri anlayan, kavrayan ve bunu anlatan ne yazık ki akademik personel sayısı çok çok az. Yani çok eskiden gelen bilgi güvenliğinin çok önemli konuları anlatılıyor tekrar tekrar ama mesela bir web uygulaması geliştirmede alınması gereken tedbirleri öğrencilere anlatma konusunda çok büyük problemlerimiz var ve bu konuda ARGE eksikliği var. Amerika'da üniversitelere bu tür ARGE fonları sağlandı. "Siz böyle bir siber güvenlik laboratuarı kurun, en az şu kadar ders verin, şu kadar öğrenciniz olsun, biz şu kadar finans edeceğiz." şeklinde böyle laboratuarlar kuruldu. Türkiye'de de bu tür çalışmaların kesinlikle yapılması lazım.

Son kullanıcıların siber güvenlik konusunda eğitilmesi gerekiyor. Bizim kurduğumuz bir portal "bilgimikoruyorum.org.tr" sadece bunun bir başlangıcı. Kurumlar çok daha farklı şeyler yapmalı, çok daha fazla tanıtımı gerçekleştirilmeli.

Aynı zamanda sistem güvenliğini test yapan firmalar var. Yani siz o firmaya gidiyorsunuz, benim güvenlik açıklıklarım var mı yok mu bir test et diyorsunuz. Bu firmaların teknik yeterliliği, aynı zamanda da güvenilirliği önemli. Çünkü o firmalar buldukları açıklıkları söylemeyebilirler, başka yere satabilirler, kendileri bir bilgiyi alabilirler. Güvenilirlik konumu önemli. Aynı zamanda onların teknik yeterliliğin de bir *certified* edilmesinde fayda var.

Tabii, özellikle açık kaynak kodlu sisteminin teşvik edilmesinde yarar var. Hani içerisinde ne olduğu, gizli bir şey var mı yok mu? Önemli.

Kritik sistemlerde, kritik alanlarda millî ürünlerin geliştirilmesinin kesinlikle desteklenmesi lazım. Bu konuda çalışmaların gerçekleştirilmesi gerekiyor.

Aslında şöyle bir şey de var. Bizim bu siber güvenlik kampımız, yazın 2-8 Temmuz arasında yapacağımız önemli bir çalışma. 8 Temmuzda mezuniyet törenimiz olacak. Komisyonumuzu da davet ediyoruz. Eğer gelmek isterlerse onları orada misafir etmekten şeref duyarız. Gebze TÜSSİDE'de. Biz davetimizi de bu şekilde yapmış olalım.

Yani burada aslında gençleri alacağız, sekiz gün boyunca siber güvenlikle ilgili bilgiler vereceğiz. Sadece teknik bilgiler olmayacak, aynı zamanda bu uzmanı onlara vizyon verecek. Böyle bir çalışma. Aslında talep de çok. Yani iki gün içerisinde 400'den daha fazla kişi başvurdu. Herkes telefonla arıyor. Mesela birisinin çocuğu Bulgaristan'da okuyormuş. Annesi aradı bizi: "Benim çocuğum bu konuyla çok ilgili. Yurt dışından katılabilir mi?" vesaire… "Zaten bu açık. On-line olarak bir test edilir." dedik. Yani ilgi çok yüksek seviyede.

BAŞKAN – Çok teşekkür ediyoruz Sayın Bahşi.

Sayın Yerlikaya, buyurun lütfen.

İLHAN YERLİKAYA (Konya) – Ben, Hayrettin Bey'e sunuşlarından dolayı teşekkür ediyorum.

Şimdi burada siber güvenlik yol haritası önerisinde ulusal siber güvenlik koordinasyon kurulunu öneriyor, işte ulusal siber güvenlik politikası dokümanını öneriyor. Bunlar acaba Avrupa'da –gerçi Amerika'dan biraz bahsettiniz ama- oralarda nasıl? Sivil inisiyatif şeklinde mi, kamu inisiyatifi şeklinde mi? Çünkü koordinasyon olacağına göre oralarla eş güdümlü yapmak lazım. Yani bizde sivil, orada kamu kuruluşu gibi olursa veya bu kurula seçilen kimselerin niteliği bakımından nasıl? Onları da araştırdınız mı? O konuda bilgi alabilir miyiz?

TÜBİTAK BİLGEM UEKAE MÜDÜR YARDIMCISI DR. HAYRETDİN BAHŞİ – O konuda araştırdık. Genel olarak zaten burada bu koordinasyon kurulu aslında sivil tandanslı oluyor. Elbette diğer tarafın temsilcileri de oluyor ama genelde bakanlıkların, her bir bakanlığın, mesela ilgili kritik bilgi sistemlerine sahip bakanlıkların, mesela bir enerji bakanlığı, sağlık bakanlığı vesaire, bunların temsilcilerinin olduğu bir kurul oluşturuluyor. Diğer ülkelerde bu şekilde yapılıyor. Ve bunun altında mesela tabii ki alt komisyonlar kuruluyor. Mesela bir şeyin teknik olarak araştırılması, öneriler geliştirilmesi gerektiğinde de teknik alt komisyonlar kuruluyor. Bunun genelde bir koordinatörü oluyor ya da buna teknik bir kurum destek ediyor. Teknik otorite gibi bir şey. Mesela Almanya'da BSI, Fransa'da DCSSI, İngiltere'de CESG diye bir kurum var. Bunlar kamu tarafından kurulmuş ve bunlara teknik bilgi veriyor yani teknik standartların belirlenmesi konusunda bu kuruma destek oluyor. Bir teknik otorite tanımı yapılıyor. Böyle bir kurul kapsamına çalışmalar gerçekleştiriliyor diğer ülkelerde.

Amerika biraz daha karışık. Orada NSA bunu yapıyor. Department of Homeland Security kritik şeyleri yaptılar, özellikle sivil ayağı, kritik altyapılarını düzenliyorlar ve şu anda Cyber Security Act'te daha çok Department of Homeland Security bu sivil ayak üzerinden ilerliyor.

BAŞKAN – Teşekkür ediyoruz.

Buyurun Sermin Hanım.

SERMİN BALIK (Elâzığ) – Hayretdin Bey'e sunumlarından dolayı teşekkür ediyorum.

Şimdi sunumunuzda bir ulusal siber güvenlik tatbikatı yapıldığını söylediniz. Bu daha önce firmalara haber veriliyor mu "Şu gün bir siber saldırı yapılacak, hazırlıklı olun." diye yoksa herhangi bir zamanda kendi belirlediğiniz kurumlara mı yapıyorsunuz?

Bir de mesela RedHack… Geçenlerde de bir şey oldu. Anneler Günü kutlaması için bile girdi sitelere, Anneler Günü mesajı bıraktı. Bu bu kadar basit mi? Bu kadar çabuk… Yani anladığım kadarıyla, zaten kötü niyetli bir hacker grubu değil bunlar. Ama bunlar istedikleri zaman Anneler Günü mesajı bile bırakabiliyorlar. Bu şeyin sonuçları ne oldu? Yaptığınız bu tatbikatın sonucu ne oldu, ne durumdayız?

Bir de, bankalara da bir sızma testi yapmışsınız. Bu bankalar da yine kendileri mi talep ettiler yoksa siz mi bankaları belirliyorsunuz? Aynı şekilde haber veriyor musunuz? Ve sistemine girebildiyseniz, hack'leyebildiyseniz ne kadar çabuk organize olup bunu püskürtebiliyorlar?

TÜBİTAK BİLGEM UEKAE MÜDÜR YARDIMCISI DR. HAYRETDİN BAHŞİ – Şimdi siber güvenlik tatbikatında aslında genelde bunun zamanı bellidir, kurumlar da bellidir, gönüllülerdir. Aslında yapılacaklar da aşağı yukarı belli. Tam zamanını belki belirli aralıkta, mesela üç gün içerisinde tam net saldırı değil ama öyle bir şey var. Yani tatbikat dediğimiz şey, hani yangın tatbikatı yaparız ya ne zaman olacağı tam belli olmaz, o şekilde değil. Çünkü burada amacımız aslında bir test etme değil, genelde şu anda bir bilinçlendirme oluşturma. Ki mesela böyle bir tatbikat yapacağız, kurum gerekli tedbirleri alsın önceden şeklinde. Yani siber güvenlikte önemli olan, karşı tarafı işin içine çekebilmek. Korkutmak, ben seni test ediyorum şeklinde yaklaşmak doğru değil. Hatta şu anda Amerika'da bile -çok sık verdim ama çok güncel olduğu için- şu kurallara uyacaksın şeklinde bir şey yok. Dolayısıyla, biz orada içeri çekiyoruz, önceden belirliyoruz. Siber güvenlik tatbikatının genel sonuçları olarak gerçekten problemler var. Yani reaksiyon,

gerçekten saldırı olup olmadığını tespit edebilen kurum var edemeyen kurum var, ettikten sonra bunun tekrar geri dönmesini önleyebilen şeyler var. Dolayısıyla, oradaki sonuçlar raporda daha çok detaylı var ama burada tabii büyük eksiklikler var. Yani bir kurumun aslında böyle bir olaya reaksiyon vermesi sadece teknik taraf değil, yani bunun idari tarafı var, farklı birimlerinin koordine edilmesi gereken bir şey. Önceden planlanması, nasıl yapılması gerektiği var. Hatta hack edildikten sonra hangi basın açıklamasının yapılması gerektiğinin de tanımlanması gerekiyor. Bunu kurumların geliştirmesi gerektiği ortaya çıktı.

Şimdi RedHack vesaire, bunlar yapabiliyor. Evet, bu kadar basit her yerde değil. Ama çok fazla sisteminiz var. Bu sistemlerin bir çok açıklıkları var ve bunlar içerisinde bazı delikleri bulup elbette bu şeyleri yapabilirler. Bazı saldırılar çok kolay. Mesela biz "servis dışı bırakma" diyoruz. Yani şöyle düşünün: Sizin 10 kişilik bir salonunuz var, ancak 10 kişiyi misafir edebilirsiniz. Bir arkadaşınız muziplik yapıyor, 100 kişiyi aynı anda davet ediyor. Yani o anda siz servis dışı kalırsınız, yapacak bir şeyiniz yok. Aynen bunun gibi. Aslında sistemlerde de ele geçirilmiş, otomatik olarak ele geçirilmiş, farklı yerlerde bulunan hackerlar tarafından, bilgisayarlar tarafından size kaldıramayacağınız kadar istek geliyor. Bunların önlenmesi gerçekten çok zor. Yapması kolay, önlenmesi zor. Ve bunun koordinasyonu gerekiyor. Yani biz bir kurum olarak bunu yapamayız. Onun mesela servis sağlayıcılarıyla koordine edilmesi gerekiyor. Ama şöyle kritik bir nokta var: Bu servis dışı bırakma, RedHack vesaire, bunlar biraz basit işler, bizi biraz bilinçlendirmesi gereken şeyler ama şu anda mesela gelişmiş ülkelerdeki en büyük dert, knowhow'larının çalınması. Mesela Amerika "Benim savunma sistemleriyle ilgili geliştirdiğim planlarım Çinliler tarafından çalınıyor." gibi bir şeyi… Buna da "gelişmiş, kalıcı tehdit" diyorlar. Yani orada bir sistemi hack etmek "Ben yaptım, web sitesini ele geçirdim." değil, yani yavaş yavaş sızılıyor ve oradan daima bilgi çekiliyor ve hiçbir zaman da karşı tarafa -tabiri caizse- çaktırılmamaya çalışılıyor. Böyle bir şey çok daha önemli onlar için mesela. Bizim için de. Biz ne kadar knowhow üretiyorsak onları korumak da bizim için önemlidir.

SERMİN BALIK (Elâzığ) – Şimdi bizim ya da herhangi bir ülkenin millî savunmasına girilse sürekli bir bilgi sızması olabilir mi yoksa fark edilebilir mi bu?

TÜBİTAK BİLGEM UEKAE MÜDÜR YARDIMCISI DR. HAYRETDİN BAHŞİ – Yani şöyle: Eğer çok iyi bir uzman ekip yapıyorsa, karşısında çok iyi bir uzman ekip ancak bunun savunmasını yapabilir. Eğer gerçekten gerekli tedbirler alınmazsa ve karşısı gerçekten çok uzmansa gerçekten kolay değil. Size net cevap veremem, açıkçası bunun net cevabı yok. Karşı tarafın ve sizin uzmanlığınıza bağlı diyebilirim.

SERMİN BALIK (Elâzığ) – Zaten çok uzman olsalar sızamazlar.

TÜBİTAK BİLGEM UEKAE MÜDÜR YARDIMCISI DR. HAYRETDİN BAHŞİ – Şöyle: Saldırganlığın çok profilleri var. Bazıları az uzman ama işte sağa sola böyle çok da kritik olmayan yerlere işte ben kendimi göstermek için yaptım diyor. Bunlar ayrı. Bir de mesela İran'daki STAKSNET gibi. Yani bizzat bir nükleer tesisi hedef alan bir kötücül yazılım geliştirmek ki, mesela onu inceleyen güvenlik uzmanları bunun arkasında gerçekten birkaç kişi yok, bunda kurumsal bir yapı var şeklinde sonuca ulaşıyorlar. Dolayısıyla, böyle bir hedefi şey yapmak için gerekli tedbirlerin çok ciddi olarak alınması lazım.

SERMİN BALIK (Elâzığ) – Peki, bankalar kendileri mi talep ettiler? Durumlarını görmek için mi talep ettiler yoksa siz mi yaptınız bunu?

TÜBİTAK BİLGEM UEKAE MÜDÜR YARDIMCISI DR. HAYRETDİN BAHŞİ – Yok, BDDK şart koşuyor bankalara. "Her sene bir kez bağımsız bir kuruluşa -kendi içinizde değil- farklı bir kuruluşa böyle bir sızma testi yapın." şeklinde zorlamaları var. Bunun sonucu olarak bankalar bunu yaptırıyorlar. Belki kendileri de yaptırıyorlardır, ayrı bir şey ama BDDK'ya hesap vermek zorundalar bu konuda. Yani bunu yapmazlarsa cezaları var.

SERMİN BALIK (Elâzığ) – Sonuçları için de hesap veriyorlar mı peki,?

TÜBİTAK BİLGEM UEKAE MÜDÜR YARDIMCISI DR. HAYRETDİN BAHŞİ – Elbette. Biz sonuçları veriyoruz. Mesela BDDK diyor ki: "Siz bu sonuçların hepsini elimine edeceksiniz, ortadan kaldıracaksınız." Bir sene sonra zaten bunlar, takip denetimi denen bir kavram var, o kavramda bu açıklıklar, önceki denetimde bulunan açıklıklar kapatıldı mı kapatılmadı mı kontrol ediliyor.

SERMİN BALIK (Elâzığ) – Cezai bir işlemi var mı peki? Geçen defa yapılan yapılmadı mesela, hiçbir eksiği tamamlanmadı. Bunun cezai bir işlemi var mı?

TÜBİTAK BİLGEM UEKAE MÜDÜR YARDIMCISI DR. HAYRETDİN BAHŞİ – Açıkçası o mevzuatı bilmiyorum. Yani BDDK…

BAŞKAN – BDDK'yı çağıracağız. O zaman bazı soruları oraya da saklayalım Sayın Balık.

SERMİN BALIK (Elâzığ) – Teşekkür ederim, sağ olun.

TÜBİTAK BİLGEM UEKAE MÜDÜR YARDIMCISI DR. HAYRETDİN BAHŞİ – Ama denetim alanında BDDK'nın yaptığı gerçekten çok güzel bir rol model. O şeyi biz kritik altyapı projeleriyle, yaptığımız projelerle diğer sektörlere de uygulaması gerektiğini düşünüyoruz. BTK da bunu yapıyor, belirli standartlar şart koşuyor telekomünikasyon altyapılarını yöneten şirketler için. Ama mesela sağlık sektöründe de, enerji sektöründe de yapılması gerekiyor.

İLHAN YERLİKAYA (Konya) – Kısa bir sorum var.

BAŞKAN – Hayretdin Bey, çok kısa cevap istiyoruz. Çünkü vakitten dolayı sıkıntımız var.

İLHAN YERLİKAYA (Konya) – Ben geç geldiğim için belki dinleyememiş olabilirim. Bu "İran'daki sızma" dediniz. Kısaca onun mahiyeti… Kim kime sızmış, ne olmuş?

TÜBİTAK BİLGEM UEKAE MÜDÜR YARDIMCISI DR. HAYRETDİN BAHŞİ – Yani aslında kapalı bir network var, hatta İnternete bağlı değil ama bu nükleer bir tesis. Nükleer tesiste kötücül bir yazılım…

İLHAN YERLİKAYA (Konya) – İran'ın kendisi…

TÜBİTAK BİLGEM UEKAE MÜDÜR YARDIMCISI DR. HAYRETDİN BAHŞİ – Yok, İran değil. Muhtemelen İran'ın düşmanları olacaktır.

Böylece belirli bir kısmını, belirli bir altyapısını fonksiyonunu icra edemeyecek hâle getirecek bir kötücül yazılım atılmış.

BAŞKAN – Code Flu diye bir hackerla bağlantı kurmuştuk, o şöyle bir şey söylemişti. İran'da İnternet bağlantısı yok ama yine de -siz kötücül yazılım dediniz- hackerlar o nükleer programını aldı. Yani "Hiçbir hackerın ulaşamayacağı bir sistem yoktur ama birazcık zaman alır." gibi bir yaklaşımda bulundu.

TÜBİTAK BİLGEM UEKAE MÜDÜR YARDIMCISI DR. HAYRETDİN BAHŞİ – Yani şöyle: Orada farklı ağlar arasındaki bir iletişim ağ dışındaki mekanizmalarla sağlanabilir. Siz USB'yi getiriyorsunuz takıyorsunuz, orada da USB'de de bulunan bir kötücül yazılım şey yapabilir. Yani her zaman bir…

BAŞKAN – Hatta Wikileaks'ın filan da birazcık aynı mantıkla hareket ettiğini…

TÜBİTAK BİLGEM UEKAE MÜDÜR YARDIMCISI DR. HAYRETDİN BAHŞİ – Tabii, burada aslında söylemek istediğimi şöyle kısaca söyleyeyim: İç tehdit çok önemli. İçeriden yapılan faaliyetler hem çok dışarıya sızdırılmıyor belki, açık edilmiyor ama iç tehdit belki problemlerin yüzde 70'i. İçeriden birisinin bir şeyler elde etmesi, bozması, zarar vermesi gibi.

BAŞKAN – Doğru. Yerli işbirlikçiler yani.

TÜBİTAK BİLGEM UEKAE MÜDÜR YARDIMCISI DR. HAYRETDİN BAHŞİ – İşbirlikçiler olabilir ya da içeri giren dışarıdaki bir adam network bağlantısına girip dışarıya olan mekanizmaları baypas edebilir vesaire.

BAŞKAN – Sayın Ramazanoğlu, buyurun.

YILDIIRIM M. RAMAZANOĞLU (Kahramanmaraş) – Teşekkür ederim Başkanım.

Ben önce iki kısa soru sorup, ondan sonra Sermin Hanım'ın sorduğu bazı şeylere biraz değişik cevap vermek istiyorum.

Birincisi, bir mezuniyet töreninden bahsettiniz. Ben kaçırdım, neyin mezuniyet töreniydi bu Gebze'de?

TÜBİTAK BİLGEM UEKAE MÜDÜR YARDIMCISI DR. HAYRETDİN BAHŞİ – Siber güvenlik yaz kampı yapıyoruz. 50 tane üniversite 3, 4 ve lisansüstü düzeydeki gençleri alıp onlara eğitim veriyoruz siber güvenlikle ilgili ki, geleceğin siber güvenlik uzmanlarını yetiştirmek adına. Onlara aynı zamanda bilgi güvenliği uzmanları eğitim verecek.

YILDIIRIM M. RAMAZANOĞLU (Kahramanmaraş) – Peki, bu yaz kampı her yıl yapılıyor mu?

TÜBİTAK BİLGEM UEKAE MÜDÜR YARDIMCISI DR. HAYRETDİN BAHŞİ – İlk defa yapıldı.

YILDIRIM M. RAMAZANOĞLU (Kahramanmaraş) – Hangi öğrencileri seçeceğinize nasıl karar veriyorsunuz?

TÜBİTAK BİLGEM UEKAE MÜDÜR YARDIMCISI DR. HAYRETDİN BAHŞİ –Hem bir anket yapıyoruz hem de teknik sorular ileteceğiz kendilerine. Yani küçük bir sınav diyelim, öyle bir şey yapacağız.

YILDIRIM M. RAMAZANOĞLU (Kahramanmaraş) – Peki, buna katılım, müracaat hâlen devam ediyor mu?

TÜBİTAK BİLGEM UEKAE MÜDÜR YARDIMCISI DR. HAYRETDİN BAHŞİ – Dün başladı, 6 Hazirana kadar devam ediyor.

YILDIRIM M. RAMAZANOĞLU (Kahramanmaraş) – Peki, ben bu notumu alayım.

BAŞKAN – Komisyona Sayın Ramazanoğlu'nu da davet edebilirsiniz uzman olarak.

TÜBİTAK BİLGEM UEKAE MÜDÜR YARDIMCISI DR. HAYRETDİN BAHŞİ – Tabii ki.

YILDIRIM M. RAMAZANOĞLU (Kahramanmaraş) – Ben Sayın Başkanıma teşekkür ediyorum.

TÜBİTAK BİLGEM UEKAE MÜDÜR YARDIMCISI DR. HAYRETDİN BAHŞİ – Siber güvenlik şöyle. Çok ilgili insanları çekmeniz lazım. Neyse, çok uzattım bu konuyu.

YILDIRIM M. RAMAZANOĞLU (Kahramanmaraş) – Hayretdin Bey, aslında Sermin Hanım çok önemli sorular sordu. Ben birer cümleyle bir katkıda bulunmak istiyorum. Siz de gayet güzel cevaplandırdınız.

Şimdi, açıkçası biraz önce kısmen bahsetti Hayretdin Bey. Bu sızmalar veyahut da hacker saldırıları ya servis dışı bırakma şeklinde oluyor ki, buna DDoS saldırıları deniyor, bu bir. İki: İçeriğe giriliyor, yani içindeki muhtevaya giriyorsunuz. Üç: Veri tabanına giriyorsunuz. Dolayısıyla, tabii bütün bunlar için… Ben burada durumdan bir vazife çıkarmak istiyorum. Türkiye'de ilk defa yazılım sigortası yapılmasını sağlamıştım ben. Çünkü bu yazılım sigortası içinde aynı bu tehditlere ve saldırılara maruz kalabilecek herhangi bir önemli yazılımın yeniden rejenere edilebilmesi hususunda mutlaka bir *back up'ın* farklı bir mekânda –aynı mekânda da değil, çünkü o mekân yanıp yıkılıp kül olabilir, depremle yerle bir olabilir- mutlaka bütün kamu kurumlarımızın tüm yazılım altyapısının bir *back up'ını* farklı bir mekânda muhafaza etmeleri çok faydalı. Bunu kamu kurumlarımız yapıyor mu yapmıyor mu bilmiyorum.

Şimdi bir başka husus da şu: Bankalara gelelim. Bankaların hemen hemen yüzde 90'ı şu anda Türkiye'de üç boyutlu güvenlik kullanıyor. Bu üç boyutlu güvenlik nedeniyle kolay kolay buralara sızmak mümkün değil. Fakat iki yöntem kullanıyorlar burada; ya fisching yöntemi ya keylogger dediğimiz. Fishing "balık tutmak" demek. Yani o bankanın web sitesinin sayfasını aynen taklit ediyor, sana bir mesajla gönderiyor, senin oradan giriş yapmanı sağlıyor. Bu bir. İki: Keylogger dediğimiz bazı yazılımlar var. Siz farkında olmadan maille bile onu alıyorsunuz. Sermin Hanım, sana bir fotoğraf gönderiyorlar diyelim. O fotoğraf bir hatıra fotoğrafı. O fotoğrafın içine dahi bazı kodları gömmek mümkün. O fotoğraf nasılmış diye açtığın anda gizli kod arkada çalışmaya başlıyor. O gizli kod keylogger dediğimiz senin bütün tuş hareketlerini hafızaya alıyor, onu sana gönderen kişiye gönderiyor, şu şu tuşlara bastı diyor. O tuşlar onun karşısında çıkıyor. O tuşlara girip bankadaki senin hesabını boşaltabiliyor. Yani buna benzer şeyler, buna benzer kod parçacıkları ne yazık ki -Hayretdin Bey de çok iyi bilir- İnternette dolaşıyor. Bunlara exploid denir. Dolayısıyla, hiç bu işleri bilmeyen bir adam bile İnternetin başına otursa, şu nasıl hack ediliyormuş, bu nasıl ediliyormuş gibi buradan dahi birtakım çıkarımlar yapıp bunları neticeye dönüştürebilir. Onun için benim bir önerim var burada, buradan son bir sonuç çıkarmış olmak adına. Şimdi açıkçası kamu kurumlarımızın, siz de tespit etmişsiniz, güvenlik zafiyetleri had safhada. Yani bir özeleştiri yapıyoruz kendi aramızda. Şimdi bunu çözümleyebilmek adına bir merkezî güvenlik sistemiyle, kamu kurumlarını da modüler sistemler hâlinde bu merkezden güvenlik sağlayabilir noktaya getirip bu suretle… Yani aynı mekâna taşımak zorunda değiliz bunları ama en azından bir güvenlik şemsiyesine, tüm kamu kurumlarının bilgi işlem server'larını sisteme dâhil etmek adına böyle bir projeye ihtiyaç var diye düşünüyorum. Detaylarını bilahare konuşabiliriz.

Bu arada son olarak şunu ifade etmek istiyorum. Yani TÜBİTAK'a çok önemli görevler düşüyor arkadaşlar. Yani Pardus'un işlevleştirilememesinden tutunuz, millî güvenlik politikasının bugüne kadar olması gereken noktaya getirilememesinden tutunuz başka eksiklerimize kadar… Ama TÜBİTAK burada bir liderlik üstlenmiş durumda. Bu Bilişim ve İnternet Komisyonumuzun da katkılarıyla inşallah TÜBİTAK'la geleceğe

doğru daha önemli adımlar atmak zorundayız. Bunları da, TÜBİTAK'ın bize vereceği raporları da biz kendi raporlarımızda dikkate almak suretiyle bir bütünleşme sağlayabiliriz.

Teşekkür ediyorum.

TÜBİTAK BİLGEM UEKAE MÜDÜR YARDIMCISI DR. HAYRETDİN BAHŞİ – Ben şöyle çok kısa bazı şeyler söyleyeceğim. Şimdi bizim bölümümüz yaklaşık 60 kişi. Bir siber güvenlik enstitüsü kurulma çalışmaları var. Birkaç ay içerisinde Bilim Kurulundan geçecek. Yani biz bölüm olarak, bir bölüm değil, bir siber güvenlik enstitüsü olacağız. Sizin dediğiniz, özellikle merkezileştirme, şu anda biraz da Bulut Bilişim konusu önemli. Çünkü her kurumda yeterli ekspertiz yok. O tür sistemler, *cloud computing,* güvenliği tartışılıyor ama yönetim açısından, güvenlik yönetimi açısından yaptınız mı da güzel yapabilirsiniz ya da oraya ekspertizlerinizi koyabilirsiniz. Bu model olabilir. Sizin gibi merkezî bir şeyler de yapılabilir ama mesela merkezî bir saldırı tespit sistemi kurmak kolay değil. Çünkü siz genelde kurumlara spesifik bazı bilgilere sahip olmak durumundasınız. O da bütün bilgileri bir merkeze toplamak demek. O sistemleri yönetmek için de kuruma spesifik şeyleri bilmeniz gerekir. O da çok kolay değil merkezileştirmek açısından. Ama *cloud computing*, Bulut Bilişim belki olabilir.

Dediğiniz gibi, özellikle hackerlar zaten kullanıcı hedefliyor. Yani bir banka sistemi ya da server sistemi yerine direkt olarak zayıf halka kullanıcıdır. Fishing (balık tutma), zaten "Ben bin kişiye oltayı atarım, eğer 5 kişi gelirse zaten işimi görürüm." diyor. Olta atmak da kolay İnternette.

YILDIRIM M. RAMAZANOĞLU (Kahramanmaraş) – Bir de son bir cümle ilave edeyim, Sermin Hanım onu da sordu. Yani hakikaten işinin uzmanı ciddi bir hacker herhangi bir sisteme sızdığının sistem yöneticileri tarafından fark edilmesini istemiyorsa fark edilmeden bu işleri yapabilir, bu bir. İki: Eğer fark edilmeyi istiyorsa işaret bırakır. Üç: Ancak, o sisteme sızma bir netice vermişse, hesaplarda anormal bir değişikliğe yol açmışsa veya dikkat çekici başka bir duruma neden olmuşsa fark edilebilir. Yoksa sadece sisteme sızıldığı için fark edilmesi mümkün değil.

Son bir örnek vereyim: İsviçre bankaları çok ciddi güvenli. Ben İsviçre bankalarının güvenlik sistemlerini bizzat inceledim İsviçre Cumhurbaşkanının izniyle arkadaşlar. İsviçre Posta İdaresinin network'unu, güvenlik sistemlerini bizzat inceledim. Dolayısıyla, şimdi İsviçre'deki bankalardan birinde çalışan… Küsurattan sonraki iki rakam var ya, hesaplarda sadece küsurattan sonraki iki rakam kuruş olarak gözüküyor. Fakat aslında orada çok uzun bir rakam var, noktadan sonra belki dokuz tane küsurat var. Fakat onu hesap tanıyor ama *ignore* ediyor yani görmüyor. Ne yapıyor? Sadece o iki rakamı görüyor. O görülmeyen, artan rakamları bir banka çalışanı kendi hesabına aktaracak bir yazılım hazırlamış. O hesaplarda görülmeyen o rakam adamın hesabına geçiyor. Fakat İsviçre bankalarının işlem hacmini düşünürseniz, adamın hesaplarındaki ciddi bir artışla… Çünkü zaman zaman banka çalışanlarının kontrolleri oluyor. Buradan yola çıkarak, bu adamın bu hesabı niye artmıştan çıkarak bunu tespit ediyor, yoksa sistemde bir anormallik olduğundan değil. Çünkü o küçücük küçücük küsuratları adam hesabına yönlendirmiş.

BAŞKAN – Bunu siz mi tespit ettiniz?

YILDIRIM M. RAMAZANOĞLU (Kahramanmaraş) – Yok, bunu bana anlattılar.

TÜBİTAK BİLGEM UEKAE MÜDÜR YARDIMCISI DR. HAYRETDİN BAHŞİ – Önemli bir iç tehdit yöntemi.

YILDIIRIM M. RAMAZANOĞLU (Kahramanmaraş) – Yani sizin biraz önce bahsettiğinize önemli bir örnek. Açıkçası ben böyle bir tehdide maruz kaldım, benim hesabımla oynandı ve ben burada –bankanın ismini vermeyeyim- bankanın içinden bu tehdidin gerçekleştiğini tespit ettim ve bankaya suç duyurusunda bulundum, genel müdürün dahi ifadesini aldırdım. Ondan sonra hesaplarımdan bütün boşaltımlar iade edildiği gibi, şimdi banka özür dileme adına bana limitsiz bir kredi kartı hesabı açtı. Demek istediğim şey şu: Birçok vatandaşlarımız bunun iç tehdit olduğunu bilmiyorlar.

AYTUĞ ATICI (Mersin) – Adam salak mıdır nedir ya! Benim hesabımla oynasa neyse de... (Gülüşmeler)

BAŞKAN – Yalnız, banka sana daha büyük bir kötülük yapmış! Limitsiz kredi kartı hesabı demek limitsiz harcama demektir. Ödemesiz değil yalnız, limitsiz!

Çok teşekkür ediyorum.

Ben bir iki tane şey söylemek istiyorum. Türkiye'ye özgü bir e-posta, bir antivirüs, bir güvenlik duvarı çalışmanız var mı? Yani böyle bir çalışmanız yoksa büyük bir eksiklik, önce onu söyleyeyim.

Sektörel analiz yaptığınızı ifade ettiniz, sağlık, enerji filan gibi. Bunlarla ilgili bir sistem tedbiriyle ilgili bir öneriniz oldu mu?

Bir de şunu soracağım: Kamu kurumları web sitesi oluşturuyor. Bunlarla ilgili sizin bir öneriniz var mı? Yani bunların daha güvenlikli İnternet siteleri olmasına yönelik bir öneriniz var mı? Çünkü her kamu kurumu bir yazılımcı buluyor ve o yazılımcının kafasına göre bir web sitesi oluşturuyor. Böyle bir standardınız var mı veya size başvuran var mı? Başvuran yoksa sizin onlara bir öneriniz var mı? Mesela *checklist* yapmak falan gibi bir öneriniz var mı? Yoksa o da büyük bir eksiklik, bence onu da yapmak lazım bir mihmandarlık anlamında.

TÜBİTAK BİLGEM UEKAE MÜDÜR YARDIMCISI DR. HAYRETDİN BAHŞİ – Şimdi şöyle: Özellikle askerî sistemlerde kullanılabilecek bir e-posta sistemi var. Ürün geliştiriliyor. Ben çok fazla detayını bilmiyorum.

BAŞKAN – Gerçi biraz sonra TÜRKSAT da sunum yapacak, onlara da bu soruyu sormuş olalım.

TÜBİTAK BİLGEM UEKAE MÜDÜR YARDIMCISI DR. HAYRETDİN BAHŞİ – Bizim bölümümüzde açık kaynak kodlu bir *firewall'u* yöneten bir yazılım geliştirildi. Temelinde açık kaynak kodlu bir *firewall* var ama bunun yönetim modülünü vesaire geliştirdik. Bu *firewall'le* ilgili bazı değişiklikler de yaptık. Bunu birçok kritik kuruma kuruyoruz çünkü içeriğinde ne olduğu biliniyor hem de diğer yönetim yazılımını da biz geliştirmiş durumdayız. Sektörel analiz çalışmaları yeni başladı. Dolayısıyla buradaki nihai hedefimiz sektörel anlamda alınması gereken minimum güvenlik tedbirlerinin belirlenmesi. Kamu kurumlarının web sitesi konusunda bizim bilgiguvenligi.gov.tr'da web uyguluma güvenliği ve web sonucu sıkılaştırılmasıyla ilgili kılavuzlarımız var. O konuyu kullanabilirler ve onları da güncellemeyi bu DPT projesinde yapacağız. Şu anda öyle kılavuzlarımız var.

BAŞKAN – Çok teşekkür ediyoruz.

Bu sunumdan sonra komisyonumuza hem soruları da aldınız hem yaklaşımları aldınız, detaylı bir rapor istiyoruz sizden yani bir sistem kurmaktan bahsettiniz üst yapı oluşumuyla ilgili, siber güvenlikle ilgili; onunla ilgili detaylı önerileri bekliyoruz.

Şimdi TÜRKSAT'ı dinleyelim.

Nihat Bey, buyurun.

TÜRKSAT GENEL MÜDÜR YARDIMCISI NİHAT OKTAY – Sayın Başkanım, sayın vekillerim; hepinizi saygıyla selamlıyorum. Ben de şehitlerimize Allah'tan rahmet diliyorum sunumuma başlamadan önce.

Türksat AŞ'de bilişim ve uydu pazarlamadan sorumlu olarak görev yürütüyorum. Öncelikle şirketimizin altyapısıyla ilgili kısa bir bilgi vermek istiyorum. Şirketimiz genel itibariyle iletişim ve bilişim alanından faaliyet göstermektedir. Daha sonra uydu, kablo ve coğrafi bilgi sistemleriyle ilgili kısa bilgi vereceğim, ondan sonra bilişim hizmetleri, neden e-devlet ve bilgi toplumu, e-devlet kapısı hakkında bilgilendirme yapacağım. Yurt dışı uygulamalarla ilgili bazı karşılaştırmalar ve spesifik olarak hangi bilişim projeleriyle uğraşıyoruz onlarla ilgili kısa bilgilendirme yapacağım.

Şirketimiz 5189 sayılı Kanun ile 22 Temmuz 2004 tarihinde özel hukuk hükümlerine tabi ve ticaret kanunu hükümleri uyarınca faaliyet göstermek üzere anonim şirket ve sermayesinin tamamı hazineye ait olarak kurulmuştur. 21 Nisan 2005 tarih ve 5335 sayılı Kanun ile Kablo TV hizmetleri ve altyapısı da Türksat A.Ş.'ye devredilmiştir. Türkiye'de e-devlet hizmetleri altyapısının kurulması, işletilmesi ve yönetilmesi görevi Ulaştırma Bakanlığı koordinasyonu ile 2006 yılında Türksat A.Ş.'ye verilmiştir. 5809 sayılı kanun ile Türksat A.Ş.'ye e-devlet ve bilişim hizmetleri görevi verilmiştir.

Zaman çizelgesinde görüldüğü üzere 2008 yılı önem arz etmekte şirketimiz açısından. Kurulduktan dört yıl sonra bu tarihte Türksat 3A uydusu uzaya fırlatıldı. Bilişim hizmetleriyle ilgili görevi devraldık ve e-devlet kapısının açılışını 18 Aralık 2008 tarihinde gerçekleştirdik ve kablo TV'de de sayısal yayıncılığa geçtik. 2009 yılında da iki tane önemli proje var tamamladığımız. Birincisi LRIT dediğimiz uzak mesafe gemi tanımlama ve takip projesi. Bu proje Uluslararası Denizcilik Örgütünün dünya ülkelerine artık gemilerle ilgili takip mekanizmasının geliştirilmesi yönünde yazılım geliştirme ve bunu kullanma zorunluluğu getirilmesiyle birlikte başlamıştır. Dünyada dokuz ülke bu yazılımı geliştirebilmiştir. Bir tanesi de Türkiye'dir. Diğer bütün ülkeler kullanıcı pozisyonundadır. Dolayısıyla biz kendi milli yazılımımızı geliştirerek bu projeyle ilgili kullanıcı pozisyonundan çıkıp yazılımı üreten ve kullandırtan pozisyonuna geldik. Bu projeyle ilgili Suriye bizim müşterimiz oldu. Suriye ile bir anlaşma yaptık. Maalesef son durumlardan dolayı proje devam edemiyor. İran müşterimiz oldu, proje devam ediyor. Gürcistan talep ediyor ve Tunus talep ediyor. Ülkemizin bölgedeki politikalarıyla paralel olarak bu proje de ciddi bilişim anlamında etkinlik kazandırmakta. Diğer önemli bir proje coğrafi bilgi sistemleri alanında Türkiye Ulusal Coğrafi Bilgi Sistemi Altyapısının Kurulması Projesi. Şu anda mevzuattaki son değişiklikle bu projenin koordinasyonu Çevre ve Şehircilik Bakanlığımıza bağlı Coğrafi Bilgi Sistemleri Genel Müdürlüğü koordinasyonunda yürüyor. Biz de bu projenin fizibilite etüdünü tamamlayarak teslim ettik, uygulama aşamasında da görev alacağız.

İletişim alanında uydularımız üzerinden TV ve radyo yayınlarını iletiyoruz. Acil durum haberleşme sistemleri kuruyoruz ve network oluşturuyoruz. Uplink ve teleport hizmetleri veriyoruz bölgemiz için. Uydu

üzerinden geniş bant İnternet erişimi sağlıyoruz ve ses hizmeti verebiliyoruz. Yine VSAT uygulamaları dediğimiz uydu terminalleriyle coğrafyadan bağımsız olarak uydunun kapsama alanlarının bulunduğu bütün bölgelerde, Çin'den İngiltere'ye kadar, İngiltere dâhil olmak üzere haberleşme hizmeti, data, veri transmisyonu ve ses transmisyonu hizmeti verebiliyoruz.

Kablo TV hizmetlerinden kısaca bahsedeceğim. 21 ilde fiber optik kablo ağına sahibiz ve bu ağı işletiyoruz. 3 milyon haneye erişim var, 140 megabite kadar internet hizmeti sunabiliyoruz. Teledünya markasıyla dijital-sayısal yayıncılığa geçtik. 130'un üzerinde sayısal yayın kablo TV abonelerine sunuluyor. Şu anda 2,4 milyon aboneye sahibiz. 2007 yılında girmiş olduğumuz bir alan GIS dediğimiz Türkiye Coğrafi Bilgi Sistemi hizmeti, bu çerçevede Amerika Birleşik Devletlerinde faaliyet gösteren uydu görüntü hizmeti üreten firmayla bir anlaşma yaparak uydu görüntülerini alıp Türkiye'de kamu kurum ve kuruluşlarının, belediyelerin ve özel sektörün ihtiyaç duyduğu uydu görüntülerini temin etmek, bu uydu görüntülerini işlemek, bu görüntülerle ilgili yazılım geliştirmek, kurum ve kuruluşlarda coğrafi bilgi sistemi altyapısını kurmak ve işletmek faaliyetlerini yürütüyoruz. Burada önemli olan, yazılımın geliştirilmesi ve entegre proje üretilebilmesi aynı zamanda kamu kurum ve kuruluşlarının coğrafi bilgi sistemi tabanlı projelerinin birlikte çalışabilirliğini sağlamaya yönelik entegre çalışabilecek çözümler üretiyoruz.

Türksat bilişim hizmetleri anlamında E-Devlet Projeleri, Entegre Bilişim Projeleri, Yazılım Geliştirme ve Birlikte Çalışabilirlik Çözümleri üzerinde yoğunlaşıp hizmet sunuyoruz. Altyapı Geliştirme ve İşletme Hizmetleri, Veri Merkezi Hizmetleri, Kimlik Yönetimi Çözümleri, E-Ödeme Çözümleri konusu da projelerimizin birer parçası olarak bu servisleri sağlıyoruz.

Türksat bilişim hizmetleri dediğimizde sınıflandırırsak bir altyapıdan bahsedebiliriz. kamu güvenli ağı dediğimiz bir altyapı, sayın vekilimiz biraz önce bir soru sordu, açıklama yaptı, o çerçevede Türkiye'nin ihtiyacı olan ana konulardan birisi bu kamu güvenli ağının oluşturulması, evet, kurum ve kuruluşlar kendi başlarına bazı bilişim projelerine imza atıyorlar, bilişim seviyelerini belirli noktalara getirebiliyorlar. Birlikte çalışılabilirlikle ilgili bazı çalışmalar var ama fiziksel olarak bunun iletişimini sağlayacak kamu güvenli ağı hem iletişim anlamında hem bilişim anlamında entegre bir şekilde henüz kurulmuş değil. Bunun kurulması en stratejik konulardan bir tanesi. Diğeri dönüşüm diyebileceğimiz e-kurum dönüşüm danışmanlığı, bu hizmeti biz veriyoruz kamu kurum ve kuruluşlarımıza. E-devlet kapısı bize verilen görev çerçevesinde hizmete açıldı ve bu kapıdan kamu kurumlarında üretilen elektronik hizmetler sunulmaktadır. Yine sayın vekilimizin sorduğu bir soru vardı, felaket kurtarma merkeziyle ilgili bir backup oluşturma, yedeklilik oluşturma kamu kurumlarının bilişim sistemi altyapıları ve ürettikleri servislerle ilgili ve veri tabanlarıyla ilgili. Şirketimiz Gölbaşı'nda faaliyet göstermektedir. Kendi şirket merkezimizde felaket kurtarma merkezi oluşturduk. Bazı kamu kurum ve kuruluşlarına bu hizmeti veriyoruz yani yedeklilik hizmetini veriyoruz. Aynı zamanda Konya'ya bu anlamda bir felaket kurtarma merkezi ve uydu kontrol merkezi anlamında her ikisinin de yedekliliğini sağlayacak bir altyapı projemiz var, onu kuracağız. Standardizasyon hem hizmetlerin standardizasyonu hem de kurumların birbirleri arasında veri paylaşırken verilerin standardizasyonu çok önemli kurumların birbirleriyle haberleşmesi anlamında. Bu tabii Türksat'ı aşan bir konu, daha yukarıda yapılması gereken bir çözüm. Ortak çağrı merkezi hizmeti arzu eden kamu kurum ve kuruluşlarına sunuyoruz.

E-devlet ve e-devlet kapısından bahsetmek istiyorum. E-devlet hizmeti nedir? Kamu kurum ve kuruluşlarının bilgi ve iletişim teknolojilerinden yararlanarak iş süreçlerini hızlandırmak, etkinliği arttırmak, harcamalarda tasarruf sağlamak, vatandaş memnuniyeti sağlamak amacı ile elektronik ortama geçirmiş oldukları her bir uygulama e-devlet uygulamasıdır. Bunu kamu kurumlarının portallerinden görebilirsiniz elektronik ortama aktardıkları ve sundukları hizmetleri. E-devlet kapısı nedir? E-devlet hizmetlerinin ortak ve tek bir yerden kullanıcıya hızlı ve güvenli bir şekilde sunulduğu bir platformdur. E-devlet kapısı, kamu kurumlarının daha fazla e-devlet hizmeti uygulamasını geliştirmesine katkıda bulunmaktadır. E-devlet kapısının arkasının kamu kurumlarınca e-devlet hizmetleri ile doldurulması çok önemlidir, etkinliğini artırmaktadır.

Neden e-devlet ve bilgi toplumu? Devletin hızlı ve etkin bir şekilde işleyişinin sağlanması, vatandaşın her düzeyde yönetime katılımı, kurumlar arası bilgi alışverişinin sağlanarak iş ve veri yinelemesinin önlenmesi, kamunun hizmet verdiği vatandaşların yaşamalarının kolaylaştırılması, karar vericilerin bilgiye dayalı karar verme süreçlerinin geliştirilmesi ve hızlandırılması devletin daha şeffaf bir yapıya kavuşması e-devlet ve bilgi toplumunun amaçları olarak tariflenebilir.

Dünyada e-devlet ve e-dönüşümle ilgili bazı gelişmeler hakkında bilgilendirme yapmak istiyorum. Özellikle Amerika'da 1998 yılında başlayan e-dönüşüm çalışmaları 2007 yılında tamamlanmıştır. Gerek eyalet bazında gerekse ulusal anlamda hizmet sunumu ve veri paylaşımı platformları olgunluk düzeyinin üst seviyelerindedir. İnternet kullanıcılarının %60'ı e-devlet hizmetlerini ortak bir platformdan kullanmaktadır.

Avrupa'da 2005 yılında yayımlanan teknoloji stratejileri ve devlet dönüşüm programı ile İngiltere'deki e-devlet çalışmalarının çerçevesi çizilmiştir. Dönüşümün gerçekleşmesi ile birlikte vatandaşlar ve iş dünyası için iki ayrı portal hayata geçirilmiştir. İnternet kullanıcılarının %60'ı e-devlet hizmetlerini ortak bir platformdan kullanmaktadır.

Uzakdoğu'da e-dönüşüm çalışmaları 2001 yılında başlayan dönüşüm çalışmaları Güney Kore e-devletinin merkezi bir sistemde kamu sistemlerinin birleştiği bir yapı olarak ortaya çıkmıştır. Hizmetler ortak ve merkezi bir yerden sunulmaktadır. İnternet kullanıcılarının %60'ı e-devlet hizmetlerini ortak bir platformdan kullanmaktadır.

Karşılaştırma yapmak gerekirse Güney Kore ve İngiltere'de kamu kurum ve kuruluşları e-dönüşüm çalışmalarını tamamlayarak hizmetleri tek bir noktadan sunma safhasına geçmişlerdir. Her iki ülke 2012 yılında ülkemizdeki e-devlet kapısı yapısında tek bir platformdan e-devlet hizmetlerini sunma çalışmalarına başlamıştır. Türkiye'de e-dönüşüm çalışmaları ve bunların e-devlet kapısından ortak platformda sunumu ise 18 Aralık 2008 tarihinden beri eş zamanlı olarak yürütülmektedir.

E-devlet kapısı, kamu hizmetlerine tek bir noktadan erişim imkânı sağlayan büyük bir internet sitesidir. Kapı'nın amacı kamu hizmetlerini, vatandaşlara, işletmelere, kamu kurumlarına bilgi ve iletişim teknolojileriyle etkin ve verimli bir şekilde sunmaktır. Bize bu görevi veren, altyapıyı sağlayan kararları geçeceğim. Önce Ulaştırma Bakanlığında, akabinde Ulaştırma Bakanlığının Türksat'a bir protokolle devrettiği yetkilendirme.

BAŞKAN – Karar size Türksat olarak ne diyor?

TÜRKSAT GENEL MÜDÜR YARDIMCISI NİHAT OKTAY – E-devlet kapısının kurulması, işletilmesi ve e-devlet kapısına entegre olacak olan kamu kurum hizmetlerinin geliştirilmesi.

BAŞKAN – Sizden başka giden var mı e-devlet kapısının kurulmasıyla ilgili kurumsal yapı?

TÜRKSAT GENEL MÜDÜR YARDIMCISI NİHAT OKTAY – Yok Sayın Başkanım.

E-devlet kapısıyla birlikte çalışacak olan kurum ve kuruluşlar öncelikle Bakanlıklar, tüm kamu kurum ve kuruluşları, belediyeler, hastaneler, bankalar olarak algılanabilir. Merkezi altyapı Türksat AŞ yerleşkesinde kurulmuştur ve vatandaşlarımıza bütün kamunun elektronik ortamda sunduğu hizmetler e-devlet kapısı vasıtasıyla sunulabilmektedir. Kapı Sayın Başbakanımızın da teşrifleriyle 18 Aralık 2008'de açılmıştır. 2008'den bu yana istatistiklere bakacak olursak 2008 yılında 22 hizmet sunuluyordu kapıdan. 6.990 kullanıcı vardı. 2009'da hizmet sayısı 42'ye, kullanıcı sayısı 22 bine, 2010 yılında hizmet sayısı 163'e, kullanıcı sayısı 229 bine, 2011 yılında e-devlet kapısı üzerinden sunulan hizmet sayısı 255'e, kullanıcı sayısı 5,8 milyona ulaşmış durumdadır.

Hangi hizmetler veriliyor? Ticari araç sorgulama, dava dosyası sorgulama, İŞKUR'la ilgili sorgulama, PTT ile ilgili, Milli Eğitim Bakanlığında e-okul, sınav sonucu, SGK'dan 4/A hizmet dökümü gibi birçok hizmet sunulabilmekte. Mayıs 2012 şu an itibarıyla sunulan hizmet sayısı 311'e ulaşmıştır. 39 kurum ile entegrasyon gerçekleşmiştir bu hizmetlerle bağlantılı olarak ve kullanıcı sayısı 12,7 milyonu aşmış durumdadır.

E-devlet kapısının işletimi nasıl oluyor? Şifre basımı ve PTT üzerinden bu şifrelerin dağıtımı şeklinde vatandaşlarımıza şifreleri ulaştırılıyor. 7/24 sunulan hizmet ve e-devlet kapısının performansı izleniyor. Kamu kurumlarının e-devlet hizmetlerinin e-devlet kapısına entegrasyonu süreci takip ediliyor. Kurumlarla güvenli ağ altyapısıyla veri paylaşımı sağlanıyor ve bu çerçevede bir çağrı merkezi oluşturuldu, bu çağrı merkezinin faaliyetlerini yürütüyoruz.

E-devlet kapısına nasıl giriliyor? E-devlet şifresiyle giriş sağlanabilir, mobil imzayla giriş sağlanabilir, elektronik imza dediğimiz sertifikayla giriş sağlanabilir. Bir de TÜBİTAK tarafından geliştirilen kimlik kartı pilot uygulaması Bolu'da devam ediyor. Bu kimlik kartıyla da e-devlet kapısına giriş sağlanacak. Hangi portaller var? Birisi internet üzerinden sunulan web portali, türkiye.gov.tr adresinden erişilebilir. Yine IOS ve Android işlemcilerde çalışabilecek mobil yazılımlar geliştirildi, mobil cihazlarla e-devlete ulaşmak mümkün. E-devlet şifresini PTT'den kimlik numarası ibrazı karşılığında kullanıcılar alabilir ve bu şifrelerle e-devlet kapısına giriş gerçekleştirilebilir.

En çok kullanılan hizmetler nelerdir? Mahkeme dava dosyası sorgulama, 4/A hizmet dökümü SGK'nın sunduğu bir hizmet, Emniyet Genel Müdürlüğünün araç sorgulama hizmeti, Devlet Meteoroloji İşlerinin günlük hava tahminleri, Tapu ve Kadastro Genel Müdürlüğü tarafından sunulan tapu bilgileri sorgulama bilgisi ve Milli Eğitim Bakanlığı tarafından sunulan öğrenci bilgi sistemi en çok erişilen hizmetler.

Kullanımına bakacak olursak, aylık ortalama sisteme giriş sayısı 5 milyondur. Aylık hizmet kullanım sayısı 30 milyon civarındadır. Mesai saatleri içerisinde hizmet ortalama alan anlık bir saniyede kullanıcı sayısı 6 bindir. Kullanıcıların detayına bakacak olursak, şifre almış ama hiç giriş yapmamış 1,6 milyon kullanıcı vardır. Toplam oranın yüzde 13'ünü oluşturmaktadır. Bir kez giriş yapan, iki kez, en önemlisi burada beş kez ve üzeri

giriş yapan orandır. Bu da 5,4 milyondur, yüzde 43'ünü oluşturmaktadır. Aslında bu seviyenin yüzde 60'ın üzerine geldiğinde biz de diğer ülkeler seviyesine erişebileceğiz.

E-devlet kapısının faydaları nelerdir? Standardizasyonu sağlamaktadır vatandaşa sunulan hizmetler açısından. Kamu hizmetlerinin entegre bir biçimde sunulmasını sağlamaktadır ve sunulan hizmetlerin vatandaş odaklı olmasını sağlamaktadır. Yine devlet hizmetlerine elektronik ortamda erişim konusunda yaygınlaştırma çalışmalarının merkezî olarak yapılması ortak iletişim altyapısıyla kamuda kaynak tasarrufu sağlamaktadır. Bağlı kurumlar arası veri iletişiminin vatandaş ile devlet arasında bağlantının ödemelerin kapı mimarisi ile güvenli bir şekilde yapılmasını sağlamaktadır.

Yine vatandaşa ve işletmelere faydaları nelerdir? Bürokrasinin azaltılması, vatandaşı devlet kapısına değil, devleti vatandaşın ayağına gitmesi; daha hızlı, düşük maliyetli ve 24 saat hizmet şeffaflığın sağlanması ve hizmette eşitlik imkânı tanımaktadır.

Kamuya faydaları: Kurumlar arası İletişimde hız ve zaman kazanılması; doğru, tutarlı ve güncel bilgiler sunulması; bilgi paylaşımı ve katılımcılığı artırarak kararların hızlı, tarafsız ve doğru alınması; mükerrer yatırımların önlenmesi, kamu hizmetlerinde tasarruf sağlanmasına aracılık etmektedir. E-devlet kapısının hedefi güvenli bir altyapı ile tüm kamu kurum ve kuruluşlarının e-devlet kapısına entegre olmasının sağlanmasıdır. Şu anda tüm kamu kurum ve kuruluşları elektronik hizmet üretip bunu e-devlet kapısına entegre etmiş vaziyette değildir. Hedef, tamamının bu yapı üzerinden hizmet sunuyor olması. Kesintisiz ve kaliteli hizmet sunumu ile kullanıcı memnuniyetinin en üst düzeye taşınması hedefidir.

AB 2007-2011 karşılaştırma analizini sizlerle paylaşmak istiyorum, sunmak istiyorum Türkiye ile Avrupa Birliği arasında. Birinci grafikte 2007 yılında 20 temel kamu hizmetinin elektronik ortamda sunulmasıyla ilgili olarak Avrupa Birliğindeki erişim oranı yüzde 58 iken Türkiye'de yüzde 55 civarında. İkinci grafikte 2007 yılında verilen hizmetin olgunluk seviyesi nedir denildiğinde olgunluk seviyesi yüzde 75, Türkiye'de yüzde 68, 2010 yılına bakıldığında hizmet sunulması noktasında Avrupa Birliğinde bu oran yüzde 82'de kalırken Türkiye Avrupa Birliğini yakalayıp öne geçmiş ve yüzde 89'a ulaştırmıştır. Hizmet olgunluk seviyesine bakıldığında Avrupa Birliğini bir puanlık bir geçişle yüzde 91 seviyesinde Avrupa Birliğinin üzerinde hem hizmet sunulması hem olgunluk seviyesi anlamında Avrupa Birliğindeki standartları geçmiş durumdayız Türkiye olarak.

Buradan bilişim hizmetlerine geçmiş istiyorum. Kamu kurum ve kuruluşları tarafından e-devlet hizmetlerinin nitelik ve niceliğinin yüksek seviyelere taşınabilmesi için bu faaliyetler sırasında Türksat tarafından iyileştirilmesi gerekli olan hususlar belirlenmiştir. Bunlar kurumların daha fazla entegre olabilmeleri için kurumlarda gerekli bilişim teknolojileri projelendirmelerinin e-devlet ve kurum stratejilerine uygun yürütülmesi, kurum bilişim altyapısının geliştirilmesi, eğitimler sağlanarak çalışan yetkinliğinin yukarı seviyelere taşınması, uzun vadeli teknoloji yol haritalarının oluşturulması, bu amaçla Türksat bilişim sektörüyle birlikte çalışması fırsatı bulunmuş fakat yukarıdaki ihtiyaçlara çözüm getirirken sektördeki başka temel sorunlar ile karşılaşılmıştır. Genel hatlarıyla bu zaman çizelgesindeki faaliyetlerimizi anlattım.

Bilişim teknolojileri yetkinliğinin kazanımı için gerekli olan üç temel hususa dikkat çekmek istiyorum; birincisi yetkin insan kaynağının yetiştirilmesi, etkin standart ve süreçlerin oluşturulması, teknoloji

üretme kabiliyetinin kazanımı. Uluslar arası örnekleri var Amerika'da, Avrupa'da bu standartların nasıl oluşturulduğu ve hangi kurum ve kuruluşlar tarafından yürütüldüğüyle ilgili.

BAŞKAN – Ben baktım, bunları anlatmayın, bunlar sizin yapacağınız şeyler. Peki, bizim bilişim ve internet araştırma komisyonundan hiç beklentiniz falan yok mu, bu rapora girmesini istediğiniz bir şey yok mu?

TÜRKSAT GENEL MÜDÜR YARDIMCISI NİHAT OKTAY – Asıl beklentimiz kamu kurum ve kuruluşlarının sunmuş oldukları elektronik hizmetlerin e-devlet kapısına bir an önce entegre edilmesi ve bu noktada şirketimizle bilgi paylaşılması, veri tabanlarının bize açılması. Kamu kurum ve kuruluşlarında yürütülen bilişim projelerinde yarım kalanlar var. Birçoğu özellikle küçük ölçekli firmalar tarafından yürütülen projeler, daha büyük entegre çözümler üretilmesi anlamında Türksat AŞ'ye devredilen spesifik projeler var, mesela TAKBİS gibi, hizmete açıldı. Tamamladığımız bir projedir. Asıl e-devlet kapısının altyapısını oluşturan projelerden bir tanesidir TAKBİS.

BAŞKAN – Çok teşekkür ediyorum.

Dikkatimi çeken bir husus var. Acaba bu e-devlet yerine e-türkiye desek daha mı iyi olurdu? Usa.gov'a giriyoruz bakıyoruz, orada özel sektör de var, STK'lar da var. Ama bizim e-devlette sadece kamu kurumları var. Bir de özel sektör var, orada vatandaşın yaptığı işler var. Biz ismi mi yanlış koyduk, uygulamayı mı yanlış yapıyoruz veyahut da bizim yaklaşımımızı mı birazcık düzeltmemiz lazım. Yoksa türkiye.gov.tr'ye özel sektörle ilgili duyurular alsak, STK'yla ilgili duyurular alsak ne mahzuru var, niye yapılmıyor? O siteyi kim yürütüyor, türkiye.gov.tr'nin şeyi kimde?

TÜRKSAT GENEL MÜDÜR YARDIMCISI NİHAT OKTAY – Şirketimizde Sayın Başkan.

BAŞKAN – Buraya niye özel sektörün şeyi yok mesela? Usa.gov'da var mesela.

TÜRKSAT GENEL MÜDÜR YARDIMCISI NİHAT OKTAY – Aslında bu da bir olgunluk seviyesiyle alakalı bir durum. Öncelikle daha büyük çapta yürütülen bilişim projeleri ve vatandaşlara sunulan hizmetler kamu kurumu kaynaklı olduğu için.

BAŞKAN – Ama hayat her yerde akıyor. İnsan uçağa bineceği zaman sadece kamu uçaklarını tercih etmiyor. Kaldı ki o uçak bile kamu veya özel sektör birbirine karıştı yani sonuçta onu birazcık toplumun hizmetine odaklı bir mantığı ortaya koymak lazım. Bu bir gösteridir. Sembolik de olsa oraya özel sektörle ilgili şeyler… Bilişim uzmanımız ne der?

YILDIRIM M. RAMAZANOĞLU (Kahramanmaraş) – Başkanım, çok önemli bir konuya temas ettiniz.

Nihat Bey'in sunumuna teşekkür ediyorum. Gerçekten bazı şeyleri ilk defa söylemiş oldu, ben birazdan değineceğim ama Başkanımızın söylediği bu bütüncül yaklaşım çok önemli yani bölük pörçük yaklaşmak yerine hakikaten şemsiyenin altına her şey girsin. Böyle bir yapıya bizim ihtiyacımız var. Bu şemsiyenin altına girenlerin de niçin o şemsiyenin altına girdiğinin gerekçelendirmemiz lazım. O bakımdan e-türkiye önemli bir düşünce, önemli bir fikir. Bunun üzerinde durmak lazım.

Ben öncelikle bir şeyi merak ettim, yirmi tane temel kamu hizmeti dediniz ama gerek bu basılı olarak bize verdiğiniz dokümanda gerekse sunumunuzda yer almalı. Ben bu yirmi temel kamu hizmeti olarak tanımladığınız kamu hizmetlerini merak ediyorum. Bunları bilahare sizden öğrenmek isterim, bu bir. İkincisi,

bakın bugüne kadar belki kırk tane sunum dinledik ama ilk defa GIS olarak siz ifade ettiniz. Ben kısaca arkadaşlarıma bir cümle beyanda bulunmak istiyorum. Geographic Information System dediğimiz yani Coğrafi Bilgi Sistemleri diye tercüme ettiğimiz sistem arkadaşlar Türkiye'de şu anda her geçen gün daha yoğun bir biçimde kullanılıyor. Burada da bir entegrasyon yok. Biliyorsunuz uydu fotoğrafları çekiliyor. Bunlar fotogrametri yöntemiyle adapte ediliyor ve burada kaçak inşaatlardan tutunuz, göllerin içindeki su hacminin hesaplanmasından tutunuz ormandaki ağaç sayımına kadar bu teknik altyapıdan istifade ediliyor. Burada ne yazık ki her bir kurum ayrı ücret ödüyor bu uydu fotoğraflarına. Halbuki burada bir entegrasyon olsa, alınan bir uydu fotoğrafı herkese paylaşılsa. Biz bunun çilesini çok çektik. Ben Üsküdar Belediyesi Başkan Vekiliyken büyükşehirden uydu fotoğraflarını almakta sıkıntı duyuyordum. O bahsettiğiniz projeler için TASBİS'i ön plana geçirdiniz. O TAKBİS'le ilgili ödülü alırken ben de Tapu Kadastro Genel Müdürümüzle birlikteydim. Orada bizim de çok ayrıntılı katkılarımız oldu. Bu TAKBİS Projesi biliyorsunuz imar koordinatlarından uydu koordinatlarına geçişi temsil eden çok güzel bir çalışma. Ben aynı zamanda Avrupa Birliği Komisyonu üyesiyim. Biz zorunlu olarak uydu koordinatlarına geçmek zorundayız. Bu konu bu sıralarda ihmal edilmiş vaziyette. Onun için bu projenin devam ettirilmesi ve tüm yerel yönetimlerin bu konuda uyarılması son derece önemli.

Şimdi bir şeye daha değineyim. Çok önemli bir konsept daha getirdiniz. Veri standardizasyonu dediniz. Bakın ben oturduğum yerden çok basit bir matematiksel hesap yaptım. "Şile" diye bir kelime var, dört tane harften müteşekkil. Bu "şile" kelimesini matriksel olarak hesapladığımız zaman kırk sekiz farklı şekilde yazabiliyorsunuz. Yani "ş" büyük, "ş" harfi küçük; "ş"nin alt noktası konulmamış, alt noktası konulmuş, yine büyük-küçük. Ondan sonra gelen "i" "ı" olabilir, büyük-küçük. Biz şimdi Üsküdar olarak şöyle bir çalışma yaptık. Üsküdar'daki birinci, ikinci, üçüncü, dördüncü bölge tapu idarelerinin tüm veri tabanıyla belediye olarak ilişki kuralım dedik. Oraya bilgi işlem uzmanlarımızı yerleştirdim, bizzat takip ediyorum. Fakat şunu gördük: İsimler bile çok değişik şekilde yazılmış. Bu isimlerin yer isimleri, şahıs isimleri, bunları standardize edip bu isimlerden aslında şu kastediliyor diyebilmek için çünkü bir de büyük harf, küçük harf hassasiyetini koyduğunuz zaman bunların iki katına çıkıyor. O bakımdan bunu biz özel bir yazılım marifetiyle ancak kendi veri tabanımızı kirletmeden kendi veri tabanımıza aktarabildik. Oradaki emlak beyanlarını anında fark edebilelim diye yaptık. Bunu niçin anlatıyorum. Arkadaşlar, Nihat Bey'in veya Hayrettin Bey'in burada sunmuş oldukları her konunun ayrı bir önemi var. Bunların her biri ayrı uzmanlık alanlarını ilgilendiren konular. Fakat biz burada hep geliyoruz şuraya sonuç olarak bir şekilde karşımıza çıkıyor. Bu Türkiye'deki tüm bilişim stratejisinin merkezî bir yapı bünyesinde takip edilmesi, örgütlenmesi ve bunun merkezî yapı çerçevesinde kurgulanması lazım. Bunu biz başardığımız zaman gerçekten Türkiye bilişim dünyasında global oyunculardan biri olabilir. Aksi hâlde çok iyi yetişmiş beyinlerimiz var. Bakın değerli bürokratlarım ne kadar güzel sunumlar yaptı ama bunların neticeye ulaşabilmesi için buradan çıkan tavsiyelerin de bizim raporlarımıza girmesi, bu raporların da ilgili makamlara arz edilmesi ve bunun da gereğinin yapılması lazım diye düşünüyorum.

Teşekkür ederim.

BAŞKAN – Çok teşekkürler.

Buyurun.

TÜRKSAT GENEL MÜDÜR YARDIMCISI NİHAT OKTAY – Özel sektörle ilgili sorunuza cevap vermek istiyorum. Yansıda gördüğünüz gibi Ulusal Ulaştırma Portali içerisinde tüm özel sektör kuruluşları da var, bu ayrı bir proje. Tabii e-türkiye'nin içerisinde özel sektör yer alacak, nasıl alacak bu ayrı bir konu. Biz kamudan başladık ama yürüttüğümüz diğer proje Ulusal Ulaştırma Portali burada ulaşımla ilgili her şey gerek kamu kurum ve kuruluşları gerek vatandaşlar açısından gerekse ulaştırma sektöründe hizmet veren bütün özel sektör kuruluşlarının bu portale entegrasyonu sağlanacak, bu projemiz devam ediyor.

İkinci konu, sayın vekilim çok önemli bir noktaya temas etti, ben tabii bilişim deyince işin bu tarafı algılanıyor, GIS bilgi sistemi kısmı göz ardı edilmiş, aslında bizim ülkemizde de edilmiş. Aslında bir uydu işi yürütüyorduk haberleşme. Kamu kurum ve kuruluşlarına bu işle ilgili hizmet götürmeye giderken hep şu soruyla karşılaşıyorduk. Uydu görüntüsü yok mu? Sonra ilgimizi çekmeye başladı. 2006-2007 yılından bahsediyorum. Bir de baktık aynı kamu kurumları hatta aynı bakanlığın altındaki genel müdürlükler aynı görüntüyü satın alıyorlar. Örnek veriyorum, Ankara'nın görüntüsünü. Birbirlerinden haberi yok, satın alırken de haberi yok, kullanırken de haberi yok ve ayrı ayrı paralar ödeniyor. Türkiye'de bunu satan sadece bir tane kuruluş var yüksek bir fiyattan. Bu alanlarla ilgili araştırma yapıp oradan girelim dedik görüntü işine, daha sonra CBS konusunun farkına vardık ve kamu kurumlarının birbirleriyle bu konuda bilgileri paylaşamadığını gördük. Aslında belirttiğiniz gibi Türkiye için Türkiye Ulusal Coğrafi Bilgi Sistemi altyapısının kurulması ve tüm kamu kurumlarının bu bilgi sistemi üzerinden hizmetlerini yürütmesi esas olandır. Bununla ilgili veri standartlarının oluşturulması noktasında da Coğrafi Bilgi Sistemi Genel Müdürlüğüne biz hizmet sunuyoruz yani ikinci aşamaya geçtik. Önce fizibiliteyi tamamladık, tasarımı tamamladık nasıl kurulacağına yönelik. Şimdi o standartların oluşturulmasıyla ilgili çalışmalarımız var ama ayriyeten şirkette bu geçiş sürecinde de ülkemizde kaynak israfı olmasın adı altında Türksatmaps isimli bir portal oluşturduk. Bu portalde Türkiye'nin tüm uydu görüntülerini sunuyoruz biz. 2007 yılı başlamak üzere, 2008, 2009, 2010, 2011 ve 2012 olmak üzere ihtiyacı olan kuruluşlar buraya abone olup alabiliyorlar ve birinci ödenen parayla beşinci sırada ödenen para artık aynı değil. Ciddi anlamda yurt dışına kaynak çıkışının önüne geçmiş durumdayız. Googlemaps'ten daha iyi bir portaldir bu. Tanıtım noktasında tabii eksikliklerimiz var. Başka özellikler de var Googlemaps'te olmayan. Ayriyeten Türksatmaps API diye bir yazılım geliştirdik. Kamu kurumları bu portali kullanırken oradaki coğrafi bilgileri alırken yazılım geliştirmelerine ihtiyaç yok. Bizim uygulama yazılımını kullanarak, bizim verilere ulaşarak kendi veri tabanını oranın üzerine koyup kendi sistemlerini kurabilirler, çok önemli bir projedir.

YILDIRIM M. RAMAZANOĞLU (Kahramanmaraş) – Sizinkini outlook olarak kullanmış oluyor.

TÜRKSAT GENEL MÜDÜR YARDIMCISI NİHAT OKTAY – Kullanabilir ve entegre bir çözüm olabilir Türkiye açısından. Önemli olan, kurumların ikna edilip bu sistemi kullanıyor olabilmeleri.

BAŞKAN – Kurumları ikna etmek diyoruz da Googlemaps'ten daha iyi bir altyapımız var dedik. Google, Yandex filan kurumları ikna mı ediyor? Hayır. Bizleri ikna ediyor. Siz de öyle bir sistem kurun, bizleri ikna edin biz de onu kullanalım. Googlemaps yerine, Yandex yerine onları kullanalım. Niye böyle bir yol izlemiyoruz?

TÜRKSAT GENEL MÜDÜR YARDIMCISI NİHAT OKTAY – Kurduğumuz bu altyapıları cazip hâle getirmenin yolları bazı kamu kurum ve kuruluşlarındaki verileri paylaşabilmek, bu portal üzerinden sunabilmek. O zaman cazibe merkezi hâline gelir.

BAŞKAN – Çok özür diliyorum yani Yandex, Google onlardan mı alıyor da yapıyor? Herhalde onlardan almıyordur. Onlara veren size haydi haydi verir.

TÜRKSAT GENEL MÜDÜR YARDIMCISI NİHAT OKTAY – Yandex konusu biraz daha farklı bir konu Sayın Başkanım.

BAŞKAN – Google kamu kurumlarından mı alıyor?

TÜRKSAT GENEL MÜDÜR YARDIMCISI NİHAT OKTAY – Yok Sayın Başkanım, orada ilgi çekici olan şey sokak görüntülerini 360 derece çektiği için son kullanıcılar açısından daha cazip.

BAŞKAN – Bence tarzımızı biraz değiştirsek daha iyi olur.

TÜRKSAT GENEL MÜDÜR YARDIMCISI NİHAT OKTAY – Biz de başladık, biz de çekim yapıp koyacağız.

BAŞKAN – Sayın Atıcı, buyurun.

AYTUĞ ATICI (Mersin) – Kamu kuruluşlarının kaç tanesinin ağ sayfasından vatandaşların hangi partiye üye oldukları anlaşılıyor. Bilgi var mı elinizde?

TÜRKSAT GENEL MÜDÜR YARDIMCISI NİHAT OKTAY – Yok efendim.

AYTUĞ ATICI (Mersin) – Biz sorduk da soru önergesiyle. Yargıtay Cumhuriyet Başsavcılığının -eğer yanlış hatırlamadıysam- ağ sayfasından vatandaşlık numaranızı girerek bu bilgiye ulaşabiliyorsunuz. Dehşet verici bir şeydir. Vatandaşlık numarası ve nüfus cüzdanınızın seri numarasını giriyorsunuz, herkes istediği her şeyi kimi nereye üye olduğu anlaşılıyor. İş başvurularında da "Falanca yerden kaydınızı silin gelin." gibi yaklaşımlar oluyor.

BAŞKAN – Kaydı silinince kalpten silinmiş olmuyor ki, kalpten silmek lazım onu.

AYTUĞ ATICI (Mersin) – İş başvurularında hep nüfus cüzdanı istendiği için çok ciddi bir sıkıntı var aslında. Tehlikeli bir şey, niye orada var, niçin giriliyor, nasıl oluyor? Hakikaten çok ilginç ama kimse de cevap veremiyor.

BAŞKAN – Buyurun.

İDRİS ŞAHİN (Çankırı) – Ben de sunum için arkadaşımıza teşekkür ediyorum.

Aytuğ Bey'in sormuş olduğu sualle alakalı da ben aynı zamanda AK PARTİ Seçim İşleri Başkan Yardımcısıyım. Bununla ilişkin bir çalışma da oldu, en son genel seçimlerde Cumhuriyet Halk Partisi Yüksek Seçim Kurulundan bu tür bir talepte bulundu ve onlar da bazı şeyleri bildirmişti ama şu an itibarıyla o tarihten sonraki süreç içerisinde Yüksek Seçim Kurulu da dâhil olmak üzere Yargıtayda böyle bir bilgi sunma imkânı yok. Yalnız gizlilik esasına göre mükerrer kayıtları önlemek adına Yargıtay bu bilgilere sahip oluyor. Şu aşamada hem üyelikleri güncelleştirme hem de iki tarafta mükerrer kayıt olmasın diye kendileri silebiliyor ama başvurduğunuz zaman böyle bir yolu tespit etmeniz mümkün değil.

AYTUĞ ATICI (Mersin) – Siteye girince elde ediyorsunuz.

İDRİS ŞAHİN (Çankırı) – Şu an itibarıyla siyasi partilere üye olanlar ancak kendi şeylerinde…

AYKAN ERDEMİR (Bursa) – Ben geçen hafta girdim ve yaptım.

SERMİN BALIK (Elazığ) – Eğer başka bir partiye üye girişi yapmak istiyorsanız size birinin TC'siyle yeni üye girişi yapmak istiyorsanız sistem size "O, başka bir partiye üyedir." uyarısı veriyor.

AYTUĞ ATICI (Mersin) – Yargıtay Cumhuriyet Başsavcılığının sitesine giriyorsunuz. Ben bunu soru önergesi olarak verdim. Denedik, kaldırdılarsa bilmiyorum. TC kimlik, nüfus cüzdanı seri no giriyorsunuz, "Aytuğ Atıcı Cumhuriyet Halk Partisine üye" diye çıkıyor. Herkese açık, çok ilginç değil mi?

AYKAN ERDEMİR (Bursa) – Şu ilçede şu tarihten itibaren diye çıkıyor.

İDRİS ŞAHİN (Çankırı) – O zaman Yargıtaya belki şey yapılabilir, ben Yüksek Seçim Kurulu açısından söylüyorum.

Bir de Sayın Başkanım, bilgi toplumu olma yönünde bilişim sektöründeki gelişmeler başlığımız bizim komisyonumuz. Buradaki bir yansıda şunu gördük: Temiz toplum olma yolunda Türkiye'nin geçirdiği evreleri algıladık. Niye? Birinci sırada Adalet Bakanlığı, Sosyal Güvenlik Kurumu, emniyetin özellikle plaka araştırmaları ve aslında Devlet Meteoroloji, o aslında özel bir konuyu ihtiva ediyor ama Tapu Kadastro. Geçmişte bu ülkenin en büyük çektiği sıkıntılar vatandaşın gittiğinde hizmet almak noktasında aracı kurumlara en fazla avans verdiği kuruluşlar buralardı. İşte bilgi toplumunun büyük bir avantajı e-devlet hizmetlerinden bu tür hizmetleri vatandaş çok daha güvenli alıyor. Özellikle adliyeler açısından söylüyorum. Maalesef Yargıtaydaki bir dosya çıkarma, icra dairelerinde bir dosyayı yerinden çıkartıp vermede arada ödenenlerin hepsini ortadan kaldırdı bu sistem. Onun için bilgi toplumu olmalıyız. Bunu bir sefer daha yenilemek istiyorum. Ben de tamamen Başkanımızın söylediği hususa e-devlet artık devleti değil, milleti ön plana çıkartan bu ülkede bir anlayış var. Dolayısıyla ismi bile belirli kesimlerde rahatsızlık uyandıran bu söylemden ve bu logodan inşallah kurtulur, e-türkiye diyelim.

BAŞKAN – Daha kucaklayıcı olması gerekiyor ve vatandaşın hizmetini kolaylaştırıcı ise sadece kamu değil, bu ülkede hizmet eden herkesin, her kesimin, her kurumun orada yer alması gerekiyor.

Buyurun.

YILDIRIM M. RAMAZANOĞLU (Kahramanmaraş) – Arkadaşlar, Başkanımızın ifade ettiği bütüncül yaklaşıma ben bir başka örnek vermek istiyorum. Değerli hukukçu kardeşimiz İdris Bey de konuya katkıda bulundu sağ olsun. Bakın, bizim birçok projemiz tek bacaklı, bir bacağı topal. Bir örnek vermek istiyorum: Bu MERNİS (Merkezî Nüfus İdaresi Sistemi) Projesi, biliyorsunuz, kişileri yani gerçek kişileri kodifiye etti, bir TC kimlik numarasıyla donattı, unique bir numara bu, bu çok güzel. Burada bir hata vardı, bu kod blokları hiçbir anlam ifade etmiyor, tamamen randomsy'lardan oluşmuş. Fakat takdir edersiniz ki bütün hukuk sistemlerinde kişi iki şekilde tanımlanır. Bir, gerçek kişi; iki, tüzel kişi. Biz gerçek kişileri kodifiye ettik fakat tüzel kişileri kodifiye etmedik. Bu konuda benim iki tane projem vardı, ikisini de ben Sayın Başbakanımıza arz ettim. Kendisi de bunu dikkatle değerlendirmemiz hususunda talimat verdi. Birinci düşüncem şuydu: Bir de kurumsal TC kimlik. Bu bireysel TC kimlik nasıl kişileri kodifiye ediyor, bir de kurumsal TC kimlik kurgulamak suretiyle şirketler, dernekler, vakıflar, büyükelçilikler, spor kulüpleri, tüm tüzel kişilik vasfına sahip olan yapıların kodifiye edilmesi. Bu bir eksiklikti, bu eksikliğin tamamlanması lazım. Fakat bu eksiklik tamamlanırken daha önceki çalışmada yapılan hata tekrarlanmamalı, buradaki kod blokları bir

anlam ifade etmeli yani bir bilgiyle ilişkilendirilmeli. Mesela vakıfta başka bir kod parçası, dernekte başka bir kod parçası, hatta kamu yararı olan dernekte daha başka bir kod parçası.

Son olarak şunu ifade etmek istiyorum: Biraz önce Aytuğ Bey'in ifade ettiği şey daha önce de ben bunu burada ifade ettim ki kayıtlara geçsin diye. Sırası geldi, şimdi tekrar sizinle paylaşmak istiyorum, sizin de düşüncenizi öğrenmek adına. Şimdi arkadaşlar, TC kimlik numaramız ortalarda dolaşıyor. İster istemez orada burada "TC kimlik numaran nedir?" diyor vergi dairesinde, söylüyoruz, biz söylerken başkaları da duyuyor. Nüfus cüzdanı fotokopilerinde TC kimlik numaralarımız yazıyor birçok yere başvururken. Halbuki bizim gerçek TC kimlik numaralarımızı sadece kamu kurumları bilse, biz bile gerçek TC kimlik numaramızı gerektiğinde bilmesek, bir sanal TC kimlik numarası verilse. Şimdi ben gerçek kredi kartı numaramı kullanmıyorum. Sanal bir kredi kartı numarası oluşturdum. Bütün vermem gereken yerlere sanal kredi kartı numaramı veriyorum. Dolayısıyla bu suretle gerçek kredi kartımı birtakım kötü uygulamalardan korumuş oluyorum. Yani bir sanal TC kimlik numarası ürettiğimiz takdirde, hatta şimdi herkesin bildiği TC kimlik numaramız sanal hâle gelebilir. Onun yerine gerçek kimlik numarası üretilebilir Türkiye Cumhuriyeti vatandaşları için. Orada da bu kod bloklarının bir anlamla ilişkilendirilmesi sağlanabilir. O zaman artık bizim sanal TC kimlik numaralarımız çok fazla onun bunun tarafından bilinmesinin bir kıymeti harbiyesi kalmaz. Gerçek kimlik numaralarımız üzerinden ciddi işlemlerin yapılması imkânı doğar. Bunu da ben sizin bilişim uzmanları olarak takdirlerinize sunuyorum.

Teşekkür ederim.

BAŞKAN – Buyurun.

TÜRKSAT GENEL MÜDÜR YARDIMCISI NİHAT OKTAY – TC kimlik numaralarının paylaşılmasıyla ilgili sayın vekilimizin görüşlerine katılıyorum. Asıl sıkıntı yetkilendirmeyle ilgili. TC kimlik numarasına ihtiyacı olan kurum ve kuruluşların yetkilendirilmesi ve veri paylaşımı gerçekleştirilebilirse zaten kimse TC kimlik numarası sormak zorunda kalmayacak. Yetkisi varsa görebilecek. Belki o da söylediğinize bir çözüm oluşturacak.

BAŞKAN – Buyurun.

ALİ ERCOŞKUN (Bolu) – Teşekkür ederim Sayın Başkanım.

Aslında ilk sorumu Sayın Ramazanoğlu söyledi yani TC kimlik numarası dışında, şahıslar dışında, kurumların da bua sahip olması aslında olmazsa olmaz bir şey olmalı yani böyle bir çalışma var mı yok mu, gelecekte böyle bir planınız var mı?

Gelecekteki iş programınız ne? Bizim hazırlayacağımız raporda bunun önemli olduğunu düşünüyorum. Türkiye Cumhuriyeti olarak e-devletin gelişim planı, programı nedir? Bunu öğrenmek önemli diye düşünüyorum.

Bu hizmetleri geliştirirken, bu kurumlarla ilişki içinde olurken diğer kurumları da göz önüne alarak yaşadığınız sıkıntılar neler, nerede engelle karşılaşıyorsunuz ve dolayısıyla şöyle olsaydı daha iyi olurdu diyeceğiniz neler var? Bunların da öneri anlamında ciddi faydası olabilir.

Diğer taraftan Sayın Başkanım "Google, Yandex yerine siz ikna edin." dediniz. Zaten özel sektörle kamu arasındaki fark aslında bu. İşe sadece kamusal hizmetler olarak baktığınız zaman ulaşabileceğiniz,

verebileceğiniz hizmetle ticari anlamda bir özel sektör mantığıyla baktığınız zaman arasındaki fark aslında bu. Dolayısıyla bizim kamudan beklentimiz özel sektörün vereceği hizmetlerden ziyade altyapısal anlamda olmalı. Benim kanaatim de bu ölçüde, teşekkür ederim.

BAŞKAN – Türksat bir kamu-özel sektörlüğü ortaklığı şu anda, tüzel kimliği öyle. O zaman özel sektöre benzer yönünüzü biraz daha öne çıkarabilirsiniz. Bizim yerli ürünümüz olarak onu kullanmak isteriz. Bir uluslar arası devasa kuruluş elimizdeki Ipad'e bir aplikasyon koyuyor ve siz onu kullanıyorsunuz. Siz de koyun, biz de kullanalım.

TÜRKSAT GENEL MÜDÜR YARDIMCISI NİHAT OKTAY – Belki e-devletle ilgili olduğu için Sayın Başkanım yaptığımız sunumlar. Biraz devlete yakın algılandı, aslında şirketimizin ticari yönü piyasaya yönelik ürettiği ürünler çok fazla, onlara değinme fırsatımız tam olmadı. Onlara geçecektik aslında. Bu projelerin tamamı devlet projeleri değil, bizim açımızdan ticari projeler, yürüttüğümüz projeler. Mesela bir tane örnek vereyim, elektronik belge üretim hizmeti hazırladığımız. Bu tamamen millî yazımdır. Bizim 140'tan fazla yazılımcımız var istihdam ettiğimiz. Kendimiz geliştirdik ve kurumlara bunu satmaya çalışıyoruz. Şu anda bunu satın alan ve uygulamaya başlayan kurumlar var. Tamamına yaygınlaştırmak istiyoruz, bizim doküman yönetim sistemi üzerinde yazışmalar yapılsın anlamında. Kişisel olarak baktığımızda da bütün diğer yazılımlardan daha uyumla, daha güzel, daha profesyonel bir şekilde geliştirilmiş bir yazılımdır bu. Görüştüğümüz birçok kurum var TÜBİTAK'tan tutun, bunların kullanıcıları arasında Orman Genel Müdürlüğü, TRT, İçişleri Bakanlığı, Türksat kendisi kullanıyor, Çalışma ve Sosyal Güvenlik Bakanlığı gibi bu bahsettiğiniz ürünlerden bir tanesi aslında. Elektronik doküman yönetim sistemi. Bizim kendimizin ürettiği, millî yazılım olarak geliştirdiğimiz ve piyasaya sunduğumuz. Bu aslında entegrasyonu da hızlandırıcı bir etken. Sormuş olduğunuz soruyla ilgili karşılaştığımız sorunlar kamu kurumlarındaki bilişim altyapısının düzeyiyle ilgili sıkıntılar var. Hepsi aynı düzeyde değil. Dolayısıyla entegrasyonu gerçekleştirmekte sıkıntı yaşanıyor. İnsan kaynağı noktasında ciddi sıkıntı var ve e-devlet kapısına entegrasyonla ilgili bazen sıkıntılar yaşanıyor. Kamu kurumları tabii yıllardır bu hizmetleri verdiği için kendi sitesinden vermeyi tercih ediyor bunu. Aslında e-devlet kapısına geldiğinde oradan sunuluyormuş hissiyatı oluşuyor, bizim hissettiklerimiz. Hâlbuki biz bu hizmeti üreten kuruluş değiliz. Hizmeti üreten kuruluş hangisiyse bizatihi kendisi biz sadece entegrasyonunu sağlıyoruz.

İkinci yaptığımız iş de şu: Eğer kurum bize diyorsa ki ben elektronik hizmet geliştirmek istiyorum, bana orada da yardımcı ol, proje geliştir, mesela TAKBİS'te olduğu gibi. O zaman diğer tarafa geçiyoruz, kurumun içerisine girip bizzat yazılım geliştirerek, tamamen yazılımları bize ait olmak kaydıyla o kurumun projelerini hayata geçiriyoruz.

BAŞKAN – O zaman Nihat Bey sizden e-devlet'in hakiki bir hizmet kapısı olması için ne gerekiyor, ne tür sıkıntılar var ve onları aşmak için neler yapmak lazım? Komisyonumuza böyle bir rapor istiyoruz tez zamanda.

TÜRKSAT GENEL MÜDÜR YARDIMCISI NİHAT OKTAY – Tabii ki Sayın Başkanım.

BAŞKAN – Çok teşekkür ediyoruz değerli arkadaşlar, iyi haftalar diliyorum.

Kapanma Saati: 13.45