2. AĞ VE BİLGİ GÜVENLİĞİ ULUSAL SEMPOZYUMU

16-18 Mayıs 2008
Girne , KIBRIS

"E-Devlette Güvenlik"

Panel

Panel Yöneticisi
Doç Dr. Kadri Büründcük
Yakın Doğu Ünversitesi Elektrik Elektronik Mühendisliği Bölümü

Panelistler
Doç. Dr. İbrahim Soğukpınar
GYTE Bilgisayar Mühendisliği Bölüm Başkanı

Eralp Curcioğlu
K.K.T.C. Başbakanlık Bilişim Danışmanı

Ersin Gülaçtı
TUBİTAK UEKAE
Kamu Sertifikasyon Merkezi Yöneticisi

Zafer Babur
Eczacıbaşı Bilişim A.Ş.
İş Geliştirme Müdürü

Ömer Yurdagül
Kamu Yönetimi Araştırma Derneği başkanı
Sosyal Güvenlik Kurumu

KTMMOB Elektrik Mühendisleri Odası
TMMOB EMO Kocaeli Şubesi
KTMMOB Bilgisayar Mühendisleri Odası

EMO Yayın No: PN/2008/5
ISBN 978-9944-89-593-4

TMMOB ELEKTRİK MÜHENDİSLERİ ODASI 1954
TMMOB ELEKTRİK MÜHENDİSLERİ ODASI KOCAELİ ŞUBESİ
KTMMOB ELEKTRİK MÜHENDİSLERİ ODASI
KTMMOB BİLGİSAYAR MÜHENDİSLERİ ODASI

2. AĞ VE BİLGİ GÜVENLİĞİ ULUSAL SEMPOZYUMU

16 Mayıs 2008
Girne , KIBRIS

"E-Devlette Güvenlik"

Panel Yöneticisi
Doç Dr. Kadri Büründcük
Yakın Doğu Ünversitesi Elektrik Elektronik Mühendisliği Bölümü

Panelistler
Doç. Dr. İbrahim Soğukpınar
GYTE Bilgisayar Mühendisliği Bölüm Başkanı

Eralp Curcioğlu
K.K.T.C. Başbakanlık Bilişim Danışmanı

Ersin Gülaçtı
TUBİTAK UEKAE
Kamu Sertifikasyon Merkezi Yöneticisi

Zafer Babur
Eczacıbaşı Bilişim A.Ş.
İş Geliştirme Müdürü

Ömer Yurdagül
Kamu Yönetimi Araştırma Derneği başkanı
Sosyal Güvenlik Kurumu

KTMMOB Elektrik Mühendisleri Odası
TMMOB EMO Kocaeli Şubesi
KTMMOB Bilgisayar Mühendisleri Odası

EMO Yayın No: PN/2008/5
ISBN 978-9944-89-593-4

panel

TMMOB
Elektrik Mühendisleri Odası

2. AĞ ve BİLGİ GÜVENLİĞİ ULUSAL SEMPOZYUMU
PANEL
"E-Devlette Güvenlik"
16 Mayıs 2008

Yayıma Hazırlayan: Elektrik Mühendisleri Odası Kocaeli Şube
1. Basım, Kıbrıs
Temmuz 2008

EMO YAYIN NO: PN/2008/5
ISBN 978-9944-89-593-4

Adres
ÖMERAĞA MH. ANKARA CD. NACİ GİRGİNSOR SK. NO:15/4 İzmit/KOCAELİ
Telefon: +90 262 3254122
Faks: +90 262 3245456

004.65 AĞ
Ağ Bilgi Güvenliği Ulusal Sempozyumu [2: Kıbrıs: 2008]
E-Devlette Güvenlik Paneli Kitabı: -- 1.bs. -- Kocaeli : Elektrik Mühendisleri Odası Yayınları, 2008.
48 s. ; 20 cm
(Emo Yayınları ; - PN/2008/5) 978-9944-89-593-4
İletişim Telekomünikasyon
İletişim Teknolojileri-Ağ Güvenliği

Dizgi Tasarım
Elektrik Mühendisleri Odası

Baskı
Dizgi, Tasarım, Baskı: Mattek Matbaacılık
G.M.K. Bulvarı 83 / 23 Maltepe - Ankara
Tel: 0312. 229 15 02 pbx
mattekmatbaa@yahoo.com

ÖNSÖZ

Mobil elektronik ortamlarda bilgi güvenliğinin tartışılması, e-devlet, e-ticaret, uzaktan eğitim, e-güvenlik, ve tüm diğer bilgi erişim, paylaşım ve ağ uygulamalarında, kişisel veya kurumsal bilginin gizliliğinin ve doğruluğunun korunması, doğruluğunun teyidi, güvenliğinin sağlanması hususlarında geliştirilen yeni yaklaşımların sunulması, yeni uygulamaların geliştirilmesi, doğabilecek problemlerin giderilmesi, yapılabilecek yeni araştırmalara ve uygulamalara katkılar sağlaması açısından oldukça önem arz etmektedir.

Ağ ve bilgi güvenliği alanında çalışan akademisyenlerin, araştırıcıların ve uygulayıcıların bir araya gelmesi sağlanmakta, çalışmaların sunulması ve tartışılması için uygun bir alan yaratma amacı ile Ağ ve Bilgi Güvenliği Ulusal Sempozyumu (ABG 2008), bu yıl ikinci kez TMMOB Elektrik Mühendisleri Odası (EMO) Kocaeli Şubesi, Kıbrıs TMMOB Elektrik Mühendisleri Odası, Kıbrıs TMMOB Bilgisayar Mühendisleri Odası tarafından 16 – 18 Mayıs 2008 tarihleri arasında Kıbrıs Girne'de düzenlenmiştir.

ABG 2008'de güncel tartışma konularını kapsayan 2 ayrı panel programlanmıştır. Bu paneller sırasıyla I) E-Devlet'te Güvenlik, II) Bilişim Hukuku : Kişisel Hakların İhlali konularında gerçekleşmiştir.

E-Devlette Güvenlik Paneli 16 Mayıs 2008 tarihinde Yakın Doğu Üniversitesi Elektrik-Elektronik Mühendsiliği Bölümü'nden Doç Dr. Kadri Büründcük yönetiminde Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği Bölüm Başkanı Doç Dr. İbrahim Soğukpınar, K.K.T.C. Başbakanlık Bilişim Danışmanı Eralp Curcioğlu, Eczacıbaşı Bilişim A.Ş. İş Geliştirme Müdürü Zafer Babur, TUBİTAK UEKAE Kamu Sertifikasyon Merkezi Yöneticisi Ersin Gülaçtı ve Kamu Yönetimi Araştırma Derneği Başkanı Ömer Yurdagül'ün panel sunumlarıyla gerçekleşmiştir. Panele 98 kişi katılım sağlamıştır.

Bilişim Hukuku Paneli 17 Mayıs 2008 tarihinde TMMOB EMO Başkanı Musa Çeçen yönetiminde İstanbul Emniyeti Asayiş Şube Müdürlüğü Bilişim Suçları Büro Amirliği'nden Başkomiser Dinçer Ay, İstanbul Teknik Üniversitesi Bilgisayar Mühendisliği Bölüm Başknı Eşref Adalı, Ankara Barosu'ndan Avukat Özgür Eralp, Doğu Akdeniz Üniversitesi Bilgi İşlem Merkezi Müdürü Necdet İcil, Sanal Banka Mağdurları Derneği Yönetim

Kurulu Başkanı L. Cem Polatoğlu, Telekom Üst Kurulu Daire Başkanı Osman Nihat Şen'in panel sunumlarıyla gerçekleşmiştir. Panele 118 kişi katılım sağlamıştır.

Ağ ve Bilgi Güvenliği Sempozyumu'na bildiri gönderen ve sunan katılımcılara, onur konuklarımıza, panel yöneticilerine ve panelistlere, oturum başkanlarına, EMO Kocaeli Şubesi Yönetim Kurulu , Kıbrıs EMO Yönetim Kurulu, Kıbrıs BMO Yönetim Kurulu üyelerine ve çalışanlarına, ABG 2008 Yürütme Kurulu, Bilim Kurulu ve Danışma Kurulu üyelerine özverili katkıları nedeniyle teşekkürü bir borç biliriz. ABG 2008'in katılımcılara ve izleyicilere yararlı olmasını, ülkemizdeki araştırıcıların, bu alanda bilgi alışverişinde bulunmasına ve konuyla ilgili birikimn oluşmasına katkıda bulunmasını dileriz.

ABG 2008 Yürütme Kurulu

SEMPOZYUMU SONUÇ BİLDİRGESİ

TMMOB Elektrik Mühendisleri Odası Kocaeli Şubesi, Kıbrıs TMMOB Elektrik Mühendisleri Odası, Kıbrıs TMMOB Bilgisayar Mühendisleri Odası tarafından "Ağ ve Bilgi Güvenliği Sempozyumu" 16 - 18 Mayıs 2008 tarihleri arasında Kuzey Kıbrıs Türk Cumhuriyeti Girne'de düzenlenmiştir. Sempozyuma ilişkin genel bilgiler;

1- 9 - 11 Haziran 2005'te İstanbul'da TMMOB Elektrik Mühendisleri Odası İstanbul Şubesi'nce gerçekleştirilen Ağ ve Bilgi Güvenliği Ulusal Sempozyumu (ABG 2005), alanında ilk kez Türkçe sunum yapılan ulusal bir etkinlikti. O zamandan bugüne ilgi alanlarda ülkemizde hem ulusal hem de uluslararası anlamda pek çok bilimsel etkinlik düzenlendi. ABG 2005 ile ABG 2008 karşılaştırıldığında aşağıdaki değerlendirmeler yapılabilir:

- İlk sempozyumda 2 çağrılı konuşma, 26 bildiri ve 1 özel sunum yapılmış, 3 panel düzenlenmişti. O sempozyumda poster sunumları yoktu. ABG 2008'de ise 2 çağrılı konuşma, 33 bildiri, 16 poster sunumu yapılmış, 2 panel düzenlenmiştir. Sunumlardaki artış sevindiricidir. Bildirilerin % 16 kadarı araştırma kurumları ve özel sektörden gelmiş; % 84'ü akademisyenler tarafından hazırlanmıştır. Bu oran ABG 2005'te benzer biçimde % 20 - % 80 şeklindeydi.

- ABG 2005'in 3 panelinde elektronik imza, açık işletim sistemlerinde bilgi güvenliği ve RFID uygulamaları tartışılmıştı. ABG 2008'in 2 panelinde ise e-devlette güvenlik ve bilişim hukuku: kişisel hakların ihlali konuları ele alınmıştır. Panel konularındaki bu değişim, ağ ve bilgi güvenliğinde teknik anlamda yeterli bir olgunluk düzeyine ulaşıldığı; tartışmaların güvenlikle ilgili uygulamaların yaygınlaşmasına ve yaşamımıza etkilerine odaklandığı şeklinde yorumlanabilir.

- ABG 2005'te, 8 ayrı oturumda Telsiz Ağlarda Güvenlik, Taşınabilir Kod Güvenliği, Saldırı Belirleme, Tasarsız Ağlarda Güvenlik, Bilişim Hukuku ve Güvenlik, Biyometri Uygulamaları, Şifreleme Yöntemleri, Asıllama, Veri Bütünlüğü, Akıllı Kart Uygulamaları, Bilgi Güvenliği Yönetimi, Güvenli Örün Uygulamaları ve Güvenlik Araçları konularındaki bildiriler tartışılmıştı. ABG 2008'de ise toplam 8 oturum Bilgi Güvenliği, Kriptoloji, Kablosuz Ağlar,

Performans Değerlendirmesi, Ağ Güvenliği, Sektör Uygulamaları, Güvenlik Yönetimi konularındaki sözlü ve poster sunumlara ayrılmıştır. Ele alınan konularda belirgin bir farklılaşma göze çarpmamıştır.

2- ABG 2008 katılımcılarının bazılarının belirttiği bir husus ülkemizde bilişim mevzuatındaki koordinasyon sorunlarının üstesinden gelinebilmesi için bilişim sorunlarını doğrudan değerlendirip yönetimsel kararlar almada katalizör olabilecek bir "bilişim bakanlığı"nın kurulması gerekliliğidir. Mevcut durumda bilişim konuları birçok farklı bakanlık tarafından ayrı ayrı ele alınmakta yada bazen konu ile ilgili makam bulunmamakta bu da koordinasyonu zorlaştırmaktadır. Ancak bu konuda meslek odalarının düşüncelerinin de dikkate alınması işleyişin sağlıklı olabilmesi açısından önemlidir.

3- Ülkemizde kurumların güvenlik planlarını oluşturmaya yeterince önem vermedikleri, bunun da güvenlik açıkları yarattığı belirlenmiştir. Gerçekten de çok az kurumda bilgi güvenliği yönetim sistemleri işler durumdadır. Bu eksikliğin giderilmesi için yasal mevzuat ve bilinçlendirme amacıyla gerekli düzenlemelerin yapılması gerekliliği vurgulanmıştır.

4- Ülkemizde e-devlet uygulamaları hızla artmaktadır. Uygulama yazılımlarının sertifikalandırılmasında gözlenen eksiklikler de kullanıcının bilinçlendirilmesi gereğini ortaya çıkarmaktadır. Olası açıkların yaratabileceği bilgi kaçağı kurumların prestijlerini yitirmelerine ve vatandaşın e-devletin kolaylıklarından uzak durmasına yol açabilir.

5- Yakın dönemde yürürlüğe giren "Internet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele" alanındaki yasanın yeterli katılımla hazırlanmadığı ve yetersiz olduğu dile getirilmiştir. Bu ve benzeri yasa hazırlıklarının konunun ilgilendirdiği tüm tarafların geniş katılımı ile gerçekleştirilmesinin önemi vurgulanmıştır.

6- Ülkemizde bilişim suçlarının takibinin mevcut yasalarla layıkıyla yapılmasının zorluğu ortaya koyulmuş; bu bağlamda bilirkişilik müessesesinin de ıslahı gereği öne çıkmıştır. Üniversitelerde hukuk biliminin altında bilişim hukuku anabilim dalının kurulması, ayrıca bilgisayar ve bilişim mühendisliği bölümlerinde seçmeli

olarak bilişim hukuku dersinin okutulmasının yararlı olacağı ifade edilmiştir. Bilirkişi atamalarında, mevcut bilirkişilik mevzuatında aksamalar görülmekle birlikte, diğer meslek disiplinlerinde olduğu gibi bilişim alanında da uzmanların meslek odalarından talep edilmesinin bu konuda yaşanan sorunların aşılmasında çözüm olacağına değinilmiştir. Bilirkişilik sorununun aksayan yönlerinin doğru tespit edilmesi doğru çözüm için önemli olacaktır.

7- Kablosuz ağların dünyada olduğu gibi ülkemizde de hızla yaygınlaştığı, kullanıcıların güvenli ağ kullanımına dikkat ettikleri istatistiklerle ortaya koyulmuştur.

8- KKTC'de ağ güvenliği alanında kısa zamanda önemli yol kat edildiği, yavru vatanın gerekli mevzuat değişikliklerini gerçekleştirmede ve tek elden koordinasyonun sağlanmasında bilinçli bir yol izlediği memnuniyetle kaydedilmiştir.

9- Diğer mühendislik projelerinde olduğu gibi bilişim tabanlı projelerin hazırlanma, kontrol ve onayı ile ilgili kanuni süreçlerin yetersiz olduğu, bu projelerde onay mekanizmasına ilgili meslek kuruluşlarının dahil edilmesi, bu alanda eğitim almış kişilerin yönetiminde bu projelerin yapılması ve bununla birlikte, bilgisayar ve bilişim mühendislerinin henüz ayrı bir meslek odası olmadığı vurgulanmıştır. Halen Elektrik Mühendisleri Odası içinde yer alan Bilgisayar ve Yazılım Mühendislerinin meslek odasının gerekli koşullar oluştuğunda KKTC'de olduğu gibi Anavatanda da ayrı bir oda olarak kurulmasının önemi vurgulanmıştır.

10- ABG2008'i izlemek ve katkı sunmak üzere Zonguldak'tan yola çıkan TMMOB Elektrik Mühendisleri Odası Kocaeli Şubesine bağlı Zonguldak İl Temsilcisi Vehbi ASLAN'ı 15 Mayıs 2008 sabah saatlerinde Ereğli ile Alaplı ilçeleri arasındaki yolun Göktepe mevkiinde meydana gelen trafik kazasında kaybettik. Vehbi ASLAN'ı kaybetmenin derin üzüntüsünü yaşıyoruz. ASLAN'ın ailesine, arkadaşlarına ve EMO camiasına başsağlığı, kazada yaralananlara acil şifalar diliyoruz. ABG2008 Sempozyumu'nu Vehbi ASLAN'nın anısına ithaf ediyoruz.

Ağ ve Bilgi Güvenliği Ulusal Sempozyumu 2
Yürütme Kurulu

-PANEL-

"E-DEVLETTE GÜVENLİK"

16 Mayıs 2008 / KIBRIS

Doç. Dr. KADRİ BÜRÜNCÜK (Panel Yöneticisi)- Değerli konuklar; "E-Devlette Güvenlik" konulu panelimize hepiniz hoş geldiniz.

İlk sunumu yapmak üzere, Doç. Dr. Sayın İbrahim Sogukpınar'ı kürsüye davet ediyorum.

Doç. Dr. İBRAHİM SOĞUKPINAR-

Değerli Katılımcılar, öncelikle günün geç saatinde panele katıldığınız için teşekkür ediyorum. Öncelikle kendimi tanıtayım. İbrahim SOĞUKPINAR, Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği Bölümünde Öğretim üyesi ve Yönetici olarak görev yapıyorum.

Sunumum şu başlıkları içerecektir. Giriş, E-Devlet Nedir? Dünyada ve Türkiye'deki Durum, E-Devlet Güvenliği Neden Önemlidir?, Kurumsal Bilgi Güvenliği Yönetimi(KBGY), KBGY, Güvenli E-Devlet Neden Önemli?, Sonuç ve Öneriler

E-Devlet'i kısaca, "Devletin hizmetlerini elektronik ortamda vermesi" olarak tanımlayabiliriz. Uygulamaları, Nüfus ve Kimlik, Başvurular, Beyannameler, Ödemeler, Sağlık Hizmetleri, Bilgi edinme vs olarak özetleyebiliriz. Uygulama maddelerini daha da arttırmak mümkündür.

1990'lı yıllarda, ülkemizde devlet kurumları son derece yavaş hizmet verirken bugün, işlemlerimizi dakikalar mertebesinde kısaltmış bulunuyoruz. Ancak buna rağmen Birleşmiş milletlerin yaptığı ve sayfasında yayınlanan 2008 yılı araştırmasında, 192 adet BM üyesi ülkede Türkiye, E-devlete hazır olmada 0.4834 oranıyla 76. sırada, E-Devlete katılımda ise, 0.1364 oranını ile 86. sırada bulunmaktadır.

E-Devlette sağlanan hizmetlerde, bilginin gizliliği, bütünlüğü ve erişilebilirliği sağlanmalıdır. Bu açıdan E-devlette bilgi güvenliği

önemlidir ve gelecekte de bu önemi artacaktır. "E-devletten ne bekliyorsunuz?" dersek, bazı farklılıklar olmakla birlikte, bir kere, bilgilere kanunsuz erişim olmamalı; yani sağlanan bilgilere herkes kanun dahilinde erişmeli. Bilgileri kimler alabilecek? Yani aklına esen o bilgileri alamamalı, bunlar kanunlarla belirlenmiş kişilere verilmeli. Bilgilere güvenilir bir erişim olmalı. Bu, altyapı ve doğrulama mekanizmalarıyla sağlanmalı. Bu bilgiler üzerinden yasal amaçlı kontroller yapılabilmeli. Devlet, toplayacağı verileri sadece belli amaçlar için, vatandaşa hizmet veya bazı denetimler için toplamalı ve bunun dışında bilgi toplamamalı, gereksiz bilgileri de toplamamalı.

Kayıtların yönetilmesi, buradaki bilgilerin yönetilmesi neye göre olacak; tabii ki, devletin kanunlarına, kurallarına göre olmalı. Dolaylısıyla, biz vatandaş olarak bunları devletten istemek hakkına sahibiz.

Devlet bilgileri topluyor, hizmet veriyor ve bu hizmetten faydalanırken de bu bilgilere ve sisteme, servislere, hizmetlere bazı tehditler söz konusu olacaktır. Bu tehditler iç ve dış tehdit olarak ikiye ayrılıyor. İç tehdit, genelde kurum içi kullanıcılar, yetkili kullanıcılar. Bir kısmı yasal olarak bu hizmetten faydalananlar, diğeri devlet kullanıcıları veya onun temsilcileri bunlar iç tehdit unsurları. Dış tehdit olarak, yabancı düşmanlar olabilir, suç organizasyonları olabilir, yabancı istihbarat servisleri, ticari organizasyonlar, araştırma acenteleri, terörist organizasyonlar olabilir. Dolayısıyla, buraya konulacak bilgiler ile verilecek hizmetlerde, bu tehditlerin değerlendirilmesi ve ona göre bilgilerin konulması gerekli.

Biliyorsunuz, 11 Eylül 2001'de Amerika'daki İkiz Kulelere yapılan saldırı sonunda, Amerika Birleşik Devletleri teröristlere karşı bir savaş açmış durumda. Yapılan araştırma sonucunda varılan sonuç, teröristlerin, eylem planlamasında, Amerikalıların e-devlet sitelerinden çok fazla faydalandığı yönünde. E-devlet uygulamalarına konulan bilgilerden, planlamaları, kurumların zayıflıklarını anlamaları ve bilgileri birleştirip kendi faaliyetlerini

organize etmeleri sonucuna varılıyor ve şöyle bir yapı kuruluyor. Korunacak olan bilgiler, verilecek olan hizmetlerdeki bütün olaylar ve yapılacak işlemler önce bir denetimden geçiriliyor ve hakikaten bunlar teröristlerin ne kadar işine yarar, teröristler bu bilgilerden ne kadar faydalanır, bunun analizi yapıldıktan sonra bilgi sistemlerine, hizmet servislerine bu bilgileri yerleştiriyorlar. Bunu da yeni bir konsept olarak düşünebiliriz.

Devlet bu hizmeti verdiğine göre, hizmeti kurum olarak verecek. Tabii, kurum bildiğimiz bir şey, ama normal olarak 4688 sayılı Kanunda kurumun kuruluş kanunları var: görev, yetki ve sorumlulukları belirli. Hizmetin niteliği ve yürütülmesi bakımından idari bir bütünlüğe sahip, işyerinden oluşan kuruluşlar olarak tanımlanıyor kurumlar.

E-devlette, devletin kurumları arasında birlikte çalışabilirlik açısından güvenliğin önemini vurgulamak veya buradaki esasları belirlemek amacıyla 2005 yılında 20 sayılı Başbakanlık Genelgesi yayınlanıyor. Temelde Devlet Planlama Teşkilatına bu görev veriliyor. Önemli bir maddesi, 3-2-4'te, "Güvenlik, Elektronik ortamda sunulan hizmetlerde başarı, güven ortamının sağlanmasına bağlıdır. Bu da güvenlikle ilgili politika ve düzenlemelerin geliştirilmesini gerektirir" şeklinde bir hedef koymuş durumda devlet.

Aynı Genelge, Madde 4.1.1'de, "Tüm kurumlarda bilgi güvenliği yönetim sistemi kurulmalıdır" şeklinde bir direktif veriliyor. Ancak direktifte, kurmazsanız bir yaptırım söz konusu değil; yani "Kurulmalıdır" diyor, ama "Şu tarihe kadar kuracaksınız. Kurmazsanız, size şu yaptırımlar uygulanır" gibi bir şey yok. Tabii, yaptırım sözü biraz itici gelebilir; ama kurumları da zorlamak için böyle şeyler yapılıyor.

E-devlette bu hizmetlerin sağlanması için, kurumsal bilgi yönetimi kavramı önemli. Bundan önceki sunumlarda Ufuk hocam bu konuya bir miktar değindi. Bunun devlet kurumlarıyla ilişkisini biraz daha vurgulamak istiyorum.

Tabii, e-devlet güvenliğiyle ilişkisini düşündüğümüz zaman, devlet, hizmetleri sağlarken vatandaşına güven vermeli, vatandaşına bu hizmetleri sağladığı yerlerdeki bilgilerin güvenliğini sağlamalı, vatandaş bu bilgilere her zaman erişebilmeli ve bu hizmetlerden her zaman faydalanabilmeli. Bunu sağlayacak olan yer devletin kurumlarıdır. Dolayısıyla, orada bir yönetim organizasyonu, yönetim planı, bilgi güvenliği yönetim planı yapılmalı ki, bu hizmetler vatandaşın istediği şekilde veya en iyi şekilde verilebilsin.

Tabii, burada birtakım standartlar ve uygulamalar var. Sonraki yansılarda bunlardan bahsedeceğim.

"Kurumsal bilgi yönetimi, bilgi güvenliği yönetimi nedir?" dersek, 1980'lerde kurumlardaki bilgi güvenliği sorumlusu bilgi işlem yöneticileridir. Bilgi işlem yöneticileri, kurumun bilgi güvenliğinden sorumlu durumdadır. Fakat daha sonra bilgi sistemlerindeki varlıklar arttıkça, bu yönetimsel bir platforma kayıyor. Nasıl? Genel müdür, genel müdür yardımcısı bunun önemli olduğunu fark edip, biraz kurumsal yaklaşıma doğru gidiyor ve 95 sonrasında artık tamamen kurumun her bireyinin, en uçtaki kullanıcısından en üst yöneticisine kadar, bilgi güvenliği yönetimi herkesi ilgilendiren bir konu haline geliyor. 2000'lerdeki yaklaşım ise, bütünüyle yönetim hâkimiyeti olmuştur. Buna information security government, Türkçe'de "Bilgi Güvenliği Yönetişimi" olarak ad veriliyor. Artık sadece kurum değil, kurumlar arasında da ilişkiler göz önüne alınmak suretiyle bilgi güvenliği yönetimi ve yönetişim kavramı ortaya çıkıyor.

Bilgi önemli bir varlık haline gelmiş durumda. Bu varlıkların korunması ve bu varlıklara dayanarak verilecek hizmetlerin en iyi şekilde verilmesi esas. Tabii, burada koruma, genellikle tarihteki savunma kalelerini düşünürsek, şehrin çevresine bir kale yapılıyor surlarla, düşmandan kendilerini korumaya çalışıyorlar. Bizim güvenlik duvarı yaklaşımının benzeri. Bizler ağımızı, farklı bağlantılardan tecrit etmeye çalışıyoruz. Oralar da güvenlik duvarı veya başka güvenlik önlemleri alıyoruz. Yani

güvenlikte konsept olarak benzer yaklaşımlar söz konusu.

Temel olarak bilgi güvenliği altyapısında 4 tane temel konu var; risklerin değerlendirilmesi, teknolojik mimari ne olacak, politikalar ne olacak güvenliği sağlamak için, bu politikaları gerçekleştirecek prosedürler ne olacak, bunları değerlendirmek söz konusu. Bunlar için, uluslararası standartlar belirli süzgeçlerden geçirilmiş ve uygulamalardan sonra genelleştirilmiş durumda. Bunun en yaygın olanı ISO 17799 olarak bilinen standart. Burada, kurumun güvenlik politikasına ilişkin belirlediği 11 tane madde var. Ulusal bilgi güvenliği yönetiminde bunların gerçekleştirilmesi esas alınıyor. Bir kere, kurumun güvenlik politikası olmalı, organizasyonun güvenliği sağlanmalı, varlıkların sınıflandırılması ve denetiminin yapılması, personelin güvenliği gibi hususlar, fiziksel güvenlik, iletişim ve operasyonel yönetimdeki güvenlik kavramı, erişimlerin kontrolü, sistemlerin geliştirilmesi ve sürekliliği; eğer sistem geliştiriyorsanız, bunların da güvenliği ve burada sürekliliğin sağlanması; olay yönetimi, güvenlikle ilgili birtakım olaylar olduğu zaman bunun yönetim sisteminin kurulması, iş sürekliliği yönetiminin sağlanması ve bunun standartlara, kurallara, kanunlara uygunluğunun sağlanması temel olarak esas alınıyor.

Tabii, bunun gerçekleştirilmesi için ilk adım, bilgi güvenliği politikasının oluşturulmasıdır. Ufuk hocam sormuştu "Bilgi güvenliği yönetim sistemi kimlerde var?" diye. Hakikaten, şu anda çok az kurumumuzda bilgi güvenliği yönetim sistemi var.

Tabii, en önemli konu risk değerlendirmesi ve risk yönetiminin gerçekleştirilmesi olmalı. Kurumsal bilgi güvenliğinin de daha önce bahsettiğimiz riskleri ve başka riskleri kurumun özelliğine göre değerlendirip, bunun yönetiminin yapılması; kontrol objelerinin seçilmesi ve bunların uygulanması, daha sonra da bunların uygunluğunun denetimi; yani bu yapılan işlemlerin standartlara uygunluğu ve gerçekten yapılıp yapılmadığının denetimi önemli hususlar.

Burada grafik olarak da, organizasyon ve teknik bakış olarak,

güvenlik politikası ve daha sonra da olay yönetimi şeklinde böyle bir piramit şeklinde bir yaklaşım söz konusu.

ISO'nun standartlarla belirlediği esaslarla birlikte, COBIT denilen ve açılımı Control Objectives for Information and Related Technologies olan kriterler ile bilgi güvenliği yönetiminde biraz daha farklı bir bakış açısı getiriyor. Daha çok finansal kurumlar COBIT'i benimsiyorlar. Burada kontrol nesneleri 4 tane ana başlık altında toplanmış. İlk başlık, planlama ve organize etme. Bu, politikanın oluşturulması, risk analizi vesaire hususları içeriyor. Diğerleri ise, veri güvenliği yönetim sisteminin edinilmesi ve gerçeklenmesi, kurumda uygulama dağıtımı ve desteği ile gözleme ve değerlendirme. Burada yapılan her olay gözleniyor, daha sonra değerlendirilmesi yapılıyor ve ne kadar gerçekleşiyor, bunun sonuçları elde ediliyor.

Burada, "Güvenli e-devlet için ne yapılmalı?" sorusu karşımıza çıkıyor. Devletin bu hizmetleri güvenli şekilde sağlaması için neler yapılmalı? Bilişim teknolojisi güvenliğinde bireysel ve kurumsal sorumluluklar söz konusu. Artık biz bilgi işlem yöneticilerine, "Senin sorumluluğun bu" diyemiyoruz veya genel müdüre bunu diyemiyoruz. Tamamen kurumun bütün çalışanlarını bu sorumluluğun belirli oranlarda içine almak durumundayız.

Bilinçlendirme çalışmaları bunun en önemli kısmı. Farkındalığın sağlanması, yani artık böyle bir konseptin önemli olduğunun anlaşılması. Diğeri, topyekûn savunma kavramının geliştirilmesi.

Biliyorsunuz, Atatürk'ün güzel bir sözü var; "Hattı müdafaa yoktur, sathı müdafaa vardır. Bu satıh bütün vatandır." Savunma söz konusu olunca da, "Kardeşim, kullanıcı olarak bana ne güvenlikten, sen sağla" diyemiyoruz. Kullanıcı, iletişim sağlayıcısı, kurumun en alt yöneticisinden, en üst yöneticisine kadar herkesin topyekûn savunma kavramını düşünmesi, anlaması gerekiyor.

Kurumların durum tespitinin yapılması önemli bir adımdır. Kurumların bilgi güvenlik politikalarının oluşturulması gerekiyor. Tabii, burada kurumsal bilgi güvenliğiyle ulusal bilgi güvenliğinin

birlikte ele alınması önemli bir husus. Kurumların koordinasyonu için bir organizasyon yapılması gerekiyor. Genelgeden anladığımız kadarıyla, bu, şu anda Devlet Planlama Teşkilatına verilmiş gibi gözüküyor; ama açıkçası, tam olarak onların sorumlu olduğundan emin değilim. Belki diğer panelistler cevap verebilirler.

Bilgi bakanlığı kurulması, ulusal bilgi güvenliği organizasyonu önemli bir gelişme olacaktır.

Belgelendirmenin teşvik edilmesi; yani güvenlik önlemlerinin belgelendirilmesi, üretilen güvenlik birimlerinin belgelendirilmesi. Bunun için, bahsettiğimiz ISO standartları, ortak kriterlerle test edilip belgelendirilmenin teşvik edilmesi. Diğeri, bilgi güvenliği denetim mekanizmasının kurulması ve bunun zorunlu hale getirilmesi. Dolayısıyla, nasıl hesaplar maliye tarafından denetleniyorsa, bilişim teknoloji güvenliğinin de kurumsal baz da denetlenmesi önemli bir husus. Tabii, bu tür organizasyonların belli bir takvime bağlanması önemli bir konu olmaktadır.

Sonuç olarak, güvenli e-devlette kurumsal bilgi güvenliği yönetim sisteminin mutlaka kurulması ve bunun işletilmesi önemli. Koordinasyonu bir yere verip, bunun belirleyici değil; kurumları düzgün çalışır şekilde formüle etmesi, çalışmaların birbirini desteklemesi, elde edilen bilgilerin paylaşımı çok önemli. Tabii, bilgi güvenliği konusunda, devlet ve hizmet veren firmalar aynı safta olacaklardır. Akademisyenler de yine benzer şekilde. Son olarak da, hattı müdafaa yerine sathı müdafaa kavramı; yani bütün kurumlar ve kişiler bilgi güvenliği sorumluluğu içerisinde olmalı. Herkesin az veya çok sorumluluğu olup, bunu yerine getirmesi kanımca iyi ilerlemeler olacaktır.

Teşekkür ediyorum. (Alkışlar)

PANEL YÖNETİCİSİ- Çok teşekkür ederiz.

Bir sonraki konuşmacı Eralp Curcioğlu'nu kürsüye davet ediyorum.

Eralp Curcioğlu, KKTC Başbakanlık Bilişim Danışmanı olarak görev yapmakta.

Eralp bey sunumunu hazırlarken, sorular hakkında bir öneri yapmak istiyorum. Hiç kuşkusuz, katılımcılar çok değerli bilgiler aktarıyor. Çok fazla müdahale etmek istemiyorum, ama süreyi de çok aştık. Sorular bölümünde süreyi biraz daha dikkatli kullanmak bağlamında, sorularınızı elinizdeki bloknotlara not alabilirseniz memnun olurum. İsminizi, sorduğunuz soruyu ve kime sorduğunuzu da yazarak bize aktarırsanız, hem konuşmacılar sorulara hazırlanır, hem de daha çok soruya cevap verme imkânı yakalayabilirler son bölümde.

Buyurun.

ERALP CURCİOĞLU (KKTC Başbakanlık Bilişim Danışmanı)- Başbakanlık Bilişim Danışmanı olarak görev yapıyorum. Kamunet Üst Kurulu Üyesiyim. EDP Projesinin bizim ülkemizde hayata geçirilmesi için yapılan çalışmalarda altyapı projeleri ve bu projelerin oluşumunda ilgili tarafların koordinasyonunu sağlamakla görevliyim. Biz, ülkemizde bu tür işleri özel firmalara yaptırıyoruz, çok az kısmı devlet tarafından yapılıyor. Bunların bir şekilde koordine edilmesi gerekiyor. Benim şu anda üstlendiğim görev bu.

Sayın hocam teorik olarak bizlere e-devlet konusunda ve güvenlik konusunda çok güzel bilgiler vermişti. Ben, daha çok gerçek yaşamda var olan bir uygulama üzerine bir sunum hazırladım.

Bizim ülkemizde uzun zamandan beridir E-Devlet Projesi için bir çalışma yapılıyor ve şu anda birinci aşama olan vatandaş portalı hizmete girmişti. Bugün biraz o hizmet sağlayan vatandaş portalının yapısı, altyapısı, güvenlik yapısı ve işleyişiyle ilgili, çok detaylı olmak üzere teknik bilgi vereceğim.

Kamunet, uzun zamandan beri çalışmalar yapıyor. Zamanımız kısıtlı olduğu için, burada çok kısa geçeceğim. 98'de başladı Kamunet ve uzun zamandan beridir, önceden var olan envanteri oraya çıkarmaya çalıştık, bir planlama hazırlandı, bütçeyle ilgili gerekli projelendirmeleri yaptı ve birtakım yasaların gerçekten

yararlı olduğunu görerek, 2006 yılının sonunda ve 2007 yılı içerisinde olmak üzere üç tane önemli yasayı Meclise sevk etti. Bunlardan birincisi Bilgi Edinme Hakkı, ikincisi Kişisel Verilerin Korunması, üçüncüsü de Elektronik İmza. Bu üç yasa olmadan elektronik devlet hizmeti verilmesinin çok mümkün olmadığını gördük ve bunun üzerine bu yasaları hazırlayıp Meclisten geçirilmesi için çalışmalar yapmıştık. Şu anda, Bilgi Edinme Hakkı ve Kişisel Verilerin Korunması Yasası yürürlüktedir. Bu yasaların uygulaması başlamış durumdadır. Kurumlar henüz daha kurulmadı; fakat biraz sonra bahsedeceğim yasamanın gereği olan birtakım hususlarda Kamunet Üst Kurulu görevlenerek, çözümlemeye başlamıştır.

Elektronik İmza Yasası da Meclisten geçti, fakat uygulama süreci 6 ay sonra başlayacak. Bu süreç henüz tamamlanmadı, haziran ayı sonu itibarıyla tamamlanacak ve haziran ayından sonra Elektronik İmza Yasası da yürürlüğe girmiş olacak.

Tabii, hedefleri var Kamunetin. Bunların belli bir kısmını oldukça iyi bir şekilde başardı, belli bir yere geldi. Biraz sonra detaylı bir şekilde bahsedeceğim.

Burada anlatmaya çalıştığımız şudur: Aslında insanların devlette kendilerine ait birçok bilgileri vardır. Bunlar farklı yerlerde, farklı şekillerde tutulmaktadırlar. Zaman zaman yanlış olabilirler, zaman zaman eksik olabilirler. Bilgi Edinme Hakkı Yasası çerçevesinde insanların bu bilgileri edinebilmesi imkânı sağlanmıştır. Sadece insanlar değil, kurumlar veya şirketler de birtakım bilgilere ihtiyaçlar duyuyorlar. Genel anlamda bu tür bilgileri de edinme hakları vardır. Bu Yasa çerçevesinde e-devletin ilk bacağı da oluşturulmuştur.

Bilgi edinme hakkını bize sağlayacak olan veya bize en iyi şekilde verecek olan, tabii ki şu an için dünyada var olan ve herkesin de rahatlıkla kullanmaya başladığı elektronik ortamlardır. Bu elektronik ortamlardan bu bilgiye ulaşmak, bir daireye gidip bir form doldurarak yapacağınız bir müracaatla daha sonra yazılı olarak bilgi almaktan çok daha efektif, çok daha kısa zamanda

ve çok daha verimli yapılabilecek bir işlemdir.

Biz, E-Devlet Projesine başlarken, bunun güncel olması, sınırsız hizmet vermesi ve güvenilir olmasını her zaman sağlamaya çalıştık. Zaman sorunu dolayısıyla yine bu konu üstünde çok fazla durmayacağım burada. Ama bildiğiniz gibi, herkesin klasik konuşmalarında söylediği bir şeydir; zaman zaman, devletin yapısının hantal olduğunu, bu elektronik hizmetlerin, bu tür hizmetlerin devletleri bu hantal yapılarından kurtardığını ve bu hantal yapılardan kurtulan devletlerin daha iyi hizmet vererek, daha iyi liderlik kazanarak, daha küçük ve daha verimli olma yoluna gittiklerini görüyoruz. Bu şekilde, bu hizmeti sağlayarak kazançlarını gören birçok devlet bu konuya ciddi yatırım yapmakta ve her geçen gün elektronik hizmetlerin sayısı artmaktadır.

Bizde de E-Devlet Projesi başlarken, e-devleti 4 gruba ayırıyoruz; vatandaş, özel sektör, kamu ve yabancılar diye 4 ayrı grup. Bir ülkede yaşayan insanlara baktığımızda, ya o ülkenin vatandaşıdır, ya o ülkeye kısa süreli gelmiş, o ülkede çalışma izni veya kısa süreli oturma izni almış insanlar. Fakat o insanların da bu hizmetlerden yararlanacağını göz önünde bulundurursak, yabancılar diye bahsettiğimiz kısım odur.

Biliyorsunuz, dışarıda iş yapan bütün özel teşebbüs, bütün özel kuruluşlar özel sektör diye anılıyor. Kamu da, devletin yarı kamu veya tam kamu olarak belirlediği sektördür. Dolayısıyla, bu 4 sektör bizim hizmet alanlarımızın tümünü kapsayabilecek şekildedir. Biz de, vatandaş, özel sektör, kamu ve yabancılar diye 4 ayrı seçenekle bu hizmetleri vermek için çalışmalar başlattık.

Bu vatandaş kapısı için biz, KGK dediğimiz, kişisel güvenlik kartı diye bir kart hazırladık. Neydi bu kart? Sağ tarafta görülen, arkasını kazıdığınız zaman üzerinde uzun bir şifre olan bir kart. Kartın bir seri numarası vardır ayrıca. Bir de broşür var; nasıl kullanılacağını anlatıyor. Şu anda bunları KKTC vatandaşları kaymakamlıklardan 3 YTL'ye alıyor ve evine giderek, bilgisayarından adresine girerek kaydını yapıyor. Bu kaydını

yaptıktan sonra da kendisinin bileceği, kendine has, başkalarıyla paylaşmamasını önerdiğimiz bir şifreyle de değişiyor. "Neden böyle bir yöntem uyguladık veya niye böyle bir yöntem takip ettik?" diye sorulabilir. Elektronik İmza Yasası haziran ayından sonra yürürlüğe gireceği için, elektronik sertifika dağıtıldı. Bu sertifikaların insanlar tarafından alınması vesaire belli bir süreç gerektirecekti, belli bir zamana ihtiyaç duyulmaktaydı. Bu zaman aşamasında, yani bu süre tamamlanana kadar böyle bir kart hazırlayarak, bu arada vatandaşları bu portalla tanıştırarak, hem portalı daha iyi bir duruma getirerek... Bizim ilk müşterilerimiz aynı zamanda test yapan müşterilerimizdir de. Onlardan gelen feedback'lerle bu portalı çok daha iyi bir duruma getirmek için çalıştık.

Kişisel Verilerin Korunması Yasası çerçevesinde kişisel verilerin korunması zaten sağlanmıştır. Kişisel verilerin nasıl korunacağı, ne tür cezalar olduğu vesaire de aynı Yasa içerisinde belirlenmiştir. Onların detaylarına çok fazla girmek istemiyorum.

Konumuz ve bugünkü gündemi kapsayacak şekilde, bizim portalda ve bu hizmetleri veren kısmında güvenlikle ilgili bir yaklaşımımız var. Nedir bu yaklaşımımız? Biz, ağ güvenliğinden, sistem güvenliğinden ve veri güvenliğinden bahsediyoruz. Biz diyoruz ki, önce iletişim altyapısının güvenli olması gerekir, daha sonra bilginin içeriğinin sağlandığı yerlerin güvenli olması gerekir. Üçüncüsü de, bilgi ve verinin işlenirken ve işlendikten sonra paylaşılırken kendisinin güvenli olması gerekir. Yani kısacası, üç bacak var; biri tamamen altyapıyla ilgili, ikincisi sistem odalarıyla ilgili, üçüncüsü ise verilerin -şu anda biz henüz o aşamaya gelmedik, ama kısa bir süre sonra herhalde biz de o aşamaya geleceğiz- kriptolu ve şifrelenmiş bir şekilde tutulmasıdır; yani veri güvenliği derken, verinin kendisinin işlendiği şekilde sistemler üzerinde tutulurken kriptolu olarak tutulması.

Ağ güvenliği konusuna gelirsek, ATM, ADSL... 3.5 gigahertzle 5.5 gigahertz frekanslarında çalışan cihazlarla kurumlara bağlantı imkânı sağlanıyor. Biliyorsunuz, E-Devlet Projesi bütün kurumların zaten öncelikle birbirine bağlanmasını gerektiriyor. Bu altyapıyı

sağlarken, ağırlıklı olarak şu anda kurulmuş olan sistemlerde sağlanabilen bağlantı şekilleri bunlardır. Bu altyapı üzerinde ne tür güvenlik kullanılıyor? Bu altyapılar üzerinde VPN, VLAN, Put-Fibering kullanılarak, her kuruma kendi ihtiyaçları çerçevesinde, her kurumun ihtiyaçlarına cevap verebilecek şekilde bir veya birden fazla farklı güvenlik servisleri kullanılarak güvenlik sağlanmaktadır. Örneğin, bir kurum eğer kendi şubelerinin kamuoyu tarafından kendi bakanlığından direkt gitmesini istiyorsa, o kurum için oluşturulan bir VPN üzerinden, aynı zamanda metro sisteminde de oluşturulan VLAN'a bağlanarak, kendine bağlı bütün kurumlarını kendi girişlerinde var olan ... indirerek, bunların kurum içerisinde açılmasını ve kurumun kendi istekleri doğrultusunda, onlara ister Internet, isterse sadece veri alışverişi sağlanmıştır.

Şu anda çalışan sistem bu şekilde. Şu anda bizim Telekomünikasyon Dairesinde bir tane metro ... var şu anda, yaklaşık 880 gigabayt olan. Kıbrıs küçük bir ülkedir. Yurtdışından gelen misafirlerimiz var burada. Belki bu, Türkiye Cumhuriyeti için, İstanbul'un bir semtine yetmeyebilir; ama bizim için oldukça büyük bir orandır. Bağlı kurumlar ise demin bahsettiğim şekilde 6 megabayt, 22 megabayt ve 2 megabayt gibi farklı hızlarda, kurumların taleplerine ve ihtiyaçlarına göre, bu yapı üzerinden ADSL şebekesine entegre edilmiştir sistem. Şu anda ADSL şebekesi üzerinden, telefondan alınan ADSL sistemiyle de direkt kurumların bağlantıları verilebiliyor. Bir de kurumlar arzu ederse, Internet servisi sağlayabiliyor bakanlık şu anda. Aslında bunu kısa bir süre sonra kaldıracağız. Bizim amacımız, tek yerde, tek merkezde, tek bir yapıyla, tek bir kapıdan her şeyi sunabilmektir. Neden; çünkü bütün e-devlet projelerinin en büyük sorunu, dağınık ve birbirinden bağımsız olmaları. Aslında bunların hepsini bir merkezden yaparsanız, her şey çok daha mükemmel olur. Tabii ki, bunu yapmak belki bizim için büyük bir avantajdır; çünkü biz çok küçük bir ülkeyiz. Nüfus sayımıza da baktığımızda, bunu merkezi bir yapıdan sağlamamız mümkündür. Şu anda burada gördüğünüz yapıda, herhangi bir kurum web servisi vermek

isterse, mail servisi verme isterse, hosting hizmetleri, mail hizmetleri... Demin gördüğünüz prezantasyon onu gösteriyordu.

Sistem güvenliğinden bahsedelim biraz. Şu anda bizim sistemlerimizin olduğu yerden bir-iki fotoğraf var burada. Ulusal bilgi sistemi diyoruz esas merkezde tuttuğumuz yere. Bu merkezde tutulan bütün verilen öncelikle fiziksel güvenlik ihtiyacı duymaktadır. Yani nedir bunlar? Orada 24 saat polis vardır. Yangın, deprem vesaire gibi muhtelif birtakım şeylere karşı, doğal afetlere karşı oranın korunması vardır. Bunların yanında da, bunun üzerinde yazılım olarak sağlanan hizmetlerin güvenliği vardır ki, içerik filtrelemesi vesaire yapılmaktadır ve bunların takibi yapılmaktadır. En önemli şey zaten sistemin güncel olarak takip edilmesidir.

Burada e-devlet hizmetleri sağlanırken ne tür bir yapıda sağlanmalıdır? En sağa baktığımızda, 4 farklı sektöre hizmet vereceğini kabul ediyoruz. Bunu çağrı merkezi ve e-devlet portalıyla sağlıyoruz. Şu anda bir çağrı merkezimiz de var, çalışır durumda. Orada operatörlerimiz var; onların eğitimleri devam ediyor. Her geçen gün daha fazla hizmet vermeleri için, var olan çağrı merkezi daha da geliştirilerek, yeni hizmetler eklemek mümkün.

Burada, tasarım, geliştirme, veri zamanları ekibi ve destek ekibi, bunun arkasında birçok ekip, birçok arkadaş vardır. Onlar da sürekli bu sistemde olan olası hataları gerek operatörlerden, gerekse müşterilerimizden alarak, daha iyiyi bulmak için sürekli onları yenileştirmek durumunda.

Tabii ki, biz burada veri entegrasyonu yaparak, birçok kurum ve kuruluşun veritabanlarını birleştirerek, bu veritabanlarının tümünü bir tek kapıdan vermek için çalışıyoruz. En solda, farklı kurumların data base'leri yer alıyor. Demin resmini görmüş olduğumuz, Başbakanlığın altında oluşturduğumuz bilgi sistemi ve onun yanında yine Başbakanlıkta e-devlet portalı vardı.

Bizim burada yaptığımız şudur: Birçok kurumun verileri yeniden düzenlenmişti ve her şey kimliğe bağlı olarak çalışıyordu. Birtakım datalar merkezde tutulmaktadır. Eğer güncel, 24 saat servis verecek kurumlar varsa, ki şu anda örneğin Nüfus Kayıt Dairesi, Muhaceret Dairesi gibi daireler sistemlerini sürekli ayakta tuttukları için, ihtiyaç duydukları zaman ihtiyaç duydukları bilgileri alarak vatandaşa vermektedir.

Sağ taraftaki grafik, o kimlik bilgilerini gösteriyor. Bu, direkt Nüfus Dairesinden alınıyor.

Vatandaş giriş işlemlerinin yapıldığı ekran buradadır. Verilerin güvenliğiyle ilgili, şu anda E-Devlet Projesinde bizim verdiğimiz hizmetlerde, demin bahsetmiş olduğum kişisel güvenlik kartı yer almaktadır. İkincisi, güvenlik sertifikası vardır ilgili portalın. Güvenlik sertifikası olarak alınmış bir sertifikamız var. İleride elektronik imza ve elektronik imzayla birlikte bilgiyi de taşıyabileceğimiz bir ortam olursa, belki de çok daha farklı hizmetler de verilebilecektir.

Bir tek devlet vardır, e-devlet portalları da veya bütün böyle bir portalda da tek bir yerden olmalıdır. Bizim inancımız budur. Burada, ilk denemeye başladığımız bir yapıyı görüyorsunuz. Şu anda çalışmaları devam ediyor. Bilgilerin kurumlar arasında paylaşılırken kriptolu paylaşılması gerekiyor. Bunun yanında, bu paylaşılacak olan bilgilerin arasında video, ses, görüntü gibi birtakım şeyler de olacaktır. Bu, bu sene sonunda devreye girecek. Parmak iziyle çalışacak bir cihazdır.

Kripto merkezi ileride daha da büyütülerek, verilerin tümünün kriptolanmış hareket etmesi de sağlanabilecektir bütün bu altyapılarda. Şu anda var olan ve çalışan bir de sesli sistem vardır. Burada ise ... tabanlı cihazlar kullanılmaktadır. Dediğim gibi, daha uzun yolumuz vardır. Her gün gelişen yeni teknolojiyle daha yeni hizmetler sağlamak için, daha da iyi içerik sağlamak için de bu çabalar devam edecektir.

Beni dinlediğiniz için teşekkür ediyorum. (Alkışlar)

PANEL YÖNETİCİSİ- Eralp arkadaşa teşekkür ediyoruz.

Konuşmasını yapmak üzere, Sayın Ersin Gülaçtı'yı kürsüye davet ediyorum.

Ersin Gülaçtı, TÜBİTAK'ta Kamu Sertifikasyon Merkezi Yöneticisi olarak görev yapmaktadır.

Buyurun Sayın Gülaçtı.

ERSİN GÜLAÇTI (TUBİTAK UEKAE Kamu Sertifikasyon Merkezi Yöneticisi)- Teşekkür ederim.

Değerli konuklar; hepinizi saygıyla selamlıyorum.

Bugünkü sunumda, asıl çalışma konum olan e-imza odaklı bir bilgi aktarımında bulunmaya çalışacağım. Fakat buna başlamadan önce, enstitüyü tanımayan kişiler olabileceğini düşünerek, kısa bir bilgi vermek istiyorum.

TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü bilgi güvenliği konusunda her türlü çalışmayı yürüten bir kuruluş. Bu konuda çok sayıda uzmanı barındırıyor. Teorik ve pratik olarak geliştirdiği ürünler, verdiği hizmetler, danışmanlıkla, özellikle askeri ve sivil kamu kurumlarının, bunun yanı sıra özel sektörün bilgi güvenliği ihtiyaçlarını çözmeye çalışıyor.

Enstitümüzde şu anda yaklaşık 700 kişi çalışmakta. Esasında bu panelde benden önce konuşan değerli konuşmacıların bahsettiği bilgi güvenliği konularında faaliyet gösteren ağ güvenliği grubumuz bulunmakta. Bu gruptan değerli arkadaşlar da sempozyuma katıldılar. Bilgi güvenliğini sağlamaya çalışan yazılımları üreten ve bu yazılımları kullanarak da kamu kurumlarına hizmet veren bir konumdayım. Nasıl oluyor bu? Şöyle oluyor: Enstitümüzde, Milli Açık Alanlar Altyapısı adını verdiğimiz bir projemiz var. Tüm çalışmalar proje sistemiyle yürütülüyor bizde. Bu proje, adı proje olmakla beraber, bir bölüm sayılabilir. PKI dediğimiz teknolojiyi her boyutuyla üreten bir proje çalışması. Buna neler dahil; elektronik sertifikalar, bu sertifikaları kullanarak şifreleme,

elektronik imza yapılmasını sağlayan yazılımlar diyebilirim.

Bu proje grubunun yöneticiliğinin yanı sıra, Kamu Sertifikasyon Merkezi olarak adlandırılan ve bütün Türkiye'deki kamu kurumlarına nitelikli elektronik sertifika üreten bir merkezin de yöneticiliğini yapıyorum. Kamu Sertifikasyon Merkezi de yine bizim kendi geliştirdiğimiz bir altyapıyla faaliyetlerini sürdürüyor.

Bilgi güvenliğiyle ilgili elektronik imza bağlantısını nasıl kuracağımızı anlatacağım. Zaman zaman sunum dışında da çeşitli noktalara temas edeceğim. Önemli bir bilgi vermek lazım burada. Enstitümüz tarafından faaliyete sokulan bir web sitesi var; www.bilgigüvenliği.gov.tr. sitesinde hizmet veriyor. Biz, bilgi güvenliği konusunda bu web sitesinin tüm ihtiyaç sahiplerine kaynak olabilecek bir hale gelmesi için çalışıyoruz. Burada çok değişik konularda makaleler bulmak, çeşitli uygulama örnekleri, pratik hayatta işimize yarayacak bilgiler bulmak mümkün.

Az önce de KKTC'deki durumdan bahsedildi. Haziran ayında Elektronik İmza Yasası yürürlüğe girecek. Elektronik İmza Yasası, 5070 sayılı Elektronik İmza Kanunuyla Türkiye'de 2004 yılında yürürlüğe girdi. Elektronik İmza Kanunuyla, Türkiye'deki Kanunla KKTC'deki Kanun birbirine çok benziyor. KKTC'nin Kanunu biraz daha kurumsal elektronik imza konusuna dikkat edecek şekilde yazılmış. Dolayısıyla, şu anda Türkiye'de gündemde olan Elektronik İmza Kanununun kurumsal elektronik imzayı da destekleyecek şekilde değiştirilmesine gerek yok.

Elektronik imza, elektronik verileri birtakım tehditlere karşı korumamızı sağlıyor. Elektronik verinin kimden çıktığını, kim tarafından üretildiğini ve değiştirip değiştirilmediğini belirleyici oluyor özellikle. Bize sağladığı faydalar nedir? Bilgilerimizin bütünlüğünü koruyabiliyoruz, kimlik doğrulama yapabiliyoruz - bu verilerin kimin tarafından hazırlandığını bize gösteriyor- verileri hazırlayanların bu işlemi inkar etmesini engelliyor.

Elektronik imza niçin çok önemli; çünkü insanların resmi işlemleri tamamıyla imzaya dayanıyor. İmza olmadan yürüyen

hiçbir işlem yok. Bu işlemleri elektronik ortama taşıyabilmek için de, aynı fonksiyonları tekrar edecek bir çözüme ihtiyaç var. Elektronik imza bunu sağlamayı hedefliyor.

Elektronik imza, ıslak imza dediğimiz imzaya göre çok daha güvenli bir imza. Bunu şimdi size anlatmaya çalışacağım. Islak imzada, biz her türlü dokümanın altına her zaman aynı şekilde imza atıyoruz. Dolayısıyla, bir dokümandan diğerine değişiklik göstermiyor ve kopyalanması çok kolay oluyor. Elektronik imza ise, imzanın uygulandığı dokümanın içeriğiyle ilişkili ve bizim kimliğimizle ilişkili. Bu nedenle, bir dokümandan diğerine kopyalanması mümkün değil; yani kopyalansa bile sahte olduğu ortaya çıkıyor.

Elektronik imza için, açık anahtarlı teknoloji dediğimiz bir teknoloji kullanılıyor. Sempozyumu takip eden herkesin bu konuda hemen hemen bilgisi olduğunu düşünüyorum. Burada asimetrik kripto algoritmaları kullanılıyor ve özet algoritması kullanılıyor. Saati de düşünerek, bunların detayına fazlaca girmemem gerekir.

Bu kriptografik algoritmalar sertifika adını verdiğimiz bir elektronik veri formatını imzalamak için kullanılıyor.

Sertifika kullanılarak elektronik imza nasıl oluşuyor, burada bunu kısaca görebiliyoruz. İmzalanması istenilen belge özetleme işleminden geçiyor. Belge özetlenerek, kişiye ait anahtarla elektronik imza bilgisine dönüştürülüyor. Bu elektronik imza bilgisi de orijinal belgenin altına eklenerek, elektronik imzalı belge ortaya çıkarılıyor.

Elektronik imzalı belgelerin doğrulanması da yine elektronik ortamda gerçekleştiriliyor. Bu işlemleri yapabilmek için, sertifikanın doğruluk kontrolleri yapılıyor, iptal olup olmadığı yine gözden geçiriliyor.

"Elektronik imza gerekli, elektronik imzaya geçmeliyiz" deniliyor hep. Bu neden böyle? İlk başta söylediğim gibi, hayatımız hep imza üzerine inşa edilmiş. Bunları elektronik olarak yaparken,

ıslak imzaya göre çok daha güvenli hale getiriyoruz, taklidi çok zor hale geliyor, değiştirilmediğini ispat edebiliyoruz, veriyi kimin imzaladığı anlaşılıyor ve veriyi imzalayan kişinin kimlik doğrulaması çok güvenli bir şekilde yapılıyor. Çünkü sertifika hizmet sağlayıcıları sıkı bir yönetim altında sertifikaları gerçek sahiplerine teslim ediyorlar. İmza sistematiğinde, imza süreçlerindeki sübjektif değerlendirme yöntemlerini ortadan kaldırıyor, tamamıyla matematiksel ve ölçülebilir bir hale getiriyor imza süreçlerini. Çünkü bir bankada imza atarken, eğer siz bir sahtekârsanız ve çok iyi çalışmışsanız imzayı taklit etmek için, çok rahatlıkla oradan parayı çekebilirisiniz. Eğer orada bu doküman doğrulanamıyorsa, imzası doğrulanamıyor, doküman içeriği görülemiyorsa, elektronik imzadan bir yarar sağlamak mümkün olmayacaktır. Bunun için, Telekomünikasyon Kurumunun da bir kurul kararıyla önerdiği bir standardı var Avrupa Birliğinin. Bu standarda uygun yazılımlar üretiyoruz ve kamu kurumlarının da nereden yazılım tedarik ederlerse etsinler, bu standarda uygun yazılım alması gerekiyor. Bu standart, çok sayıda uzmanın yıllarca çalışarak ortaya çıkardığı bir standart. Dolayısıyla, elektronik imzayla ilgili ihtiyaç duyulan birçok konuyu çözüme kavuşturmuş. Özellikle uzun vadeli olarak elektronik imzanın kullanılması için, arşiv imzası dediğimiz imza formatının desteklenmesi gerekiyor. Bununla ilgili zaman damgası olması gerekiyor imzanın üzerinde. Sanırım, uzun vadeli imzalarla ilgili konuyu tamamlayacak şekilde Zafer beyin bir sunumu olacak.

Beni dinlediğiniz için teşekkür ediyorum.

PANEL YÖNETİCİSİ- Bir sonraki sunumu yapmak üzere Zafer Babür beyi davet ediyorum.

Buyurun Zafer bey.

ZAFER BABÜR (Eczacıbaşı Bilişim A.Ş. İş Geliştirme Müdürü)- ZAFER BABÜR (Eczacıbaşı Bilişim A.Ş. İş Geliştirme Müdürü)- Panelin son panelisti olarak fazla vaktinizi almayacağım.

E-devletten bahsetmeden önce, sizi biraz daha öncesine almak

istiyorum. Çok önceleri bu iki büyük nehir arasında site devletleri kuruldu. O günden bugüne neler değişti, kısaca bir yazılı beleglere bakalım. Önce duvarlara sonra kil tabletlere yaziliyor, sonra papirüse, parşömene, kağıda... Hep vatandaşı izliyor devlet baba kontratlari izliyor. Hep devletle bir ilişkimiz var, ama hepsinde de kapı kapı dolaşıyoruz. Ticaret yapıyorsunuz, vergi ödemek için gidiyorsunuz; mülk alıyorsunuz, tapudan işleminizi yapıyorsunuz; ama hep bu arada biz vatandaşı götürüyoruz, bu kamu kurumlarının önüne koyuyoruz. Oysa e-devlet sayesinde kamu kurumları vatandaşın önünee geliyor.

Sonrasında devlet arşivleri oluşuyor. Bu arada Osmanlı'ya ait bir örnek vermek istiyorum Kıbrıs Osmanlı'nin eğemenliği altında iken tüm tapular kayıt altında. 74'senesinde apar topar bırakılmış bir çok şey bu arada Magosa'nın kayıtları Maraş'ta bir otelin altında bulunuyor.. Vakfın olan toprakları İngilizler tarafından buradaki Rumlara işletmeleri karşılığında verilmiş oysa verilebilecek olan kullanım hakkı, toprağın mülkiyeti değil. Zira toprak Lala Mustafa Paşa vakfının. Her ne kadar kimi kayıtlarda değişiklik yapılsa da kayıtların orjinalleri olması lazım bir yerlerde nerede? Bu kayıtların orijinalleri nerede; orijinalleri İstanbul'da. Elektronik imzaya bağlayacağım bu işi. Böyle bir uygulama olmuş olsaydı, yapılabilir miydi? Bu noktada çok dikkat etmek gerektiğini düşünüyorum. Biz elektronik imzaya geçerken, birkaç nesil sonrasını da düşünmemiz lazım. Kayıtların bozulmaması lazım, kayıtların ileride başka amaçlar için kullanılması gerektiğinde kullanılması lazım. Bu kayıtlara saldırılar oluyor. Bu, iç tehditler olacak, dış tehditler olacak. Bizim bunlara karşı çok güvenli bir yapıda olmamız lazım; yani sadece vatandaşın işini kolaylaştırıyor olmamamız lazım, elimizdeki kayıtları da iç ve dış düşmanlara karşı korumamız lazım.

Tabii, "Kimin kayıtları muteberdir?" sorusu geliyor bu arada.

O yüzden, eğer ben devletsem, insanların kayıtlarını alıyorsam, bunları dışarıya vermemem lazım. Yine İbrahim hocam bahsetti; bu kayıtların peşinde olacaklar. Çünkü ona göre bize fiyat verecekler. Bu, ilaç olabilir, hastalık olabilir, bambaşka şeyler olabilir.

Bu, ilk imza formatı. "O günden bugüne neler değişti?" diye bir bakalım.

Bu da bir kontrat örneği, MÖ 2300 yılında Mezopotamya'da yazılmış bir kontrat. Bu kontratı hızlıca bir okuyayım müsaadenizle. "Ilı-Eribu'nun oğlu Sini İştar ve kardeşi Apil-li, Sini İştar ile Minani'nin evine komşu, sokağa cepheli, Migrat-Sin oğlu Minani'ye ait olup içinde hali hazırda evi olan 1/3'şar araziyi anlaştıkları fiyat olan 4.5 sekel gümüşten almışlardır. Minani'nin bu satıştan dolayı hiç bir hakkı kalmamıştır. Kralın huzurunda yemin ettiler. Tebet ayı, Büyük Karra-Şarma duvarı yılı" diye devam ediyor. Ne farkı var? Konu mevcut, koşullar mevcut, taraflar mevcut, tarih mevcut, tanımlar var, bir de üstüne üstlük mühür var. Bu sözleşme nerede yapılmış, Burgul'da yapılmış.

O günden bugüne pek bir şey değişmedi. Çivi yazısı vardı, Sümerce vardı, kil tabletler vardı. Mezopotamya'da MÖ 2300'de bunlar vardı. Bilahare ne oldu; papirüs, mürekkep geldi. Sonrasında, Anadolu'da başka ortamlar geliştirilmeye başlandı. Ceylan derisi veya keçi derisinin üzerine yazı yazmaya başladılar daha sonra. Sonrasında sıcak mühür geldi, soğuk mühür geldi, sayısal sertifika geldi, mobil imza geldi. Sadece ortam değişiyor, ama kontratlar değişmedi. Dolayısıyla biz burada elektronik devlet derken, elektronik ortam derken, sadece araçları değiştiriyoruz. Çok çok farklı bir şey yapmıyoruz, sadece araçlar değişiyor.

Bir de imza atmaktan bahsettik. Neden imza atıyoruz? Birkaç tane işlevi var aslında imzanın. Törensel işlevi. Sonra, delil işlevi kişiye özgü bir iz bırakıyoruz. Onay işlevi; içerik ve hukuksal

yaptırımların kabulünü gerektiriyor. Lojistik işlevi ; paranın, malın yer değiştirmesi silsilesi işlemlerini başlatıyor..

Ayrıca noter kayıtları dediğimiz bir mekanizma var. Ersin arkadaşımızın dediği gibi, bu sayede bir imzanın bir sahtekarın imzası olup olmadığını anlayabiliyorsunuz. Noterin Doğrulama ve onaylama mekanizması var. Peki, bunları sayısal imza sağlayabiliyor mu; gerçekten sağlıyor. Ersin'in de sunumunda da söylediği gibi, siz, sayısal sertifikanızın bileşenlerini almak için gerçek kimliğinizi götürüyorsunuz, onun karşılığında size bir sayısal sertifika veriyorlar. Sonra belgenin kimliği var. Güvenlik mekanizması var; imzalayan ya da imzalanın değiştirilmesi mümkün olmamalı.

Sizi yine tekrar Mezopotamya uygarlıklarına götüreceğim. Mühür basılı tablet oluşturmak zor, çünkü mühür sizin elinizde. Mühür basılan kil tablet asırlarca yaşayabiliyor. Kil, bugüne kadar geldi. Peki, elektronik imzadan farkı ne? Eğer o dönemki insanlar hash oluşturmasını bilselerdi, buraya da özetini çıkartıp bunun altına özütünü koysalardı, elektronik imza gibi bir şey yapmış olacaklardı.

Peki, elektronik imza her yerde kullanılabiliyor mu; hayır. Belli yerlerde kullanılıyor da, bazı yerlerde kullanılmıyor. "Şahit gerektiren olaylarda kullanılmaz" demiştik. Şahit gerektiren yerler neresi; nikah, tapu vb. Malum, bizim ülkemizde, Türkiye'de çok yaygın bir uygulama var; boş kağıda imza atmak. Elektronik imzada böyle bir şey olmayacak, çünkü boş kağıda imza atamayacaksınız.

Yine bir başka konu daha var. Siz, eğer kurumda birine görev verdiğiniz zaman, onaylama veya bir başka yere geçirme yetkisi verdiğiniz zaman, başka mekanizmaları da devreye sokuyorsunuz. Elektronik ortamda, o önemli kişiler ortadan kalkmış oluyor. Bu açıdan da çok büyük yarar var.

Elektronik imza elle atılan imzanın kesinlikle uzantısı değildir; çünkü kısa bir imza neyse, elektronik imza da o.

Kontratlar elektronik ortamda tutulabilir, her ne kadar kontratlar elektronik ortamda oluşturlmasa da.

Ticari defterler konusunda Maliye Bakanlığında çalışmalar var. Elektronik fatura üzerinde çalışmalar var ki, Türkiye'de şu anda elektronik fatura üreten bir projemiz var. Bu proje yaygınlaşacak.

Türkiye'de elektronik imzanın hukuksal yapısına baktığımız zaman, 5070 sayılı Kanuna istinaden Telekomünikasyon Kurumu var. Anlaşmalar bireylerle gerçekleşiyor; bir kamu şirketi veya bir özel şirket, tüzelkişilik olarak elektronik imza alamıyor. Şu ana kadar herhangi bir hukuksal vaka olmadı.

Peki, toptan sürece baktığımız zaman ne var? Aslında süreçte, vatandaş önce kimliğini ibraz ediyor. Kendisine kimlik teyidinden sonra sizin adınıza elektronik imza üretiliyor, tıpkı eskinin mühürcüsü gibi Bu kart ve elektronik imza oluşturma yazılımı sayesinde dokumanları elektronik olarak imzalayabiliyorsunuz. .Biz, özellikle uygulamaların XML standartlarında yazılmasını talep ediyoruz ki, bunun asıl standart olacağını düşünüyoruz. Sonra karşı tarafa imzalı dokumanı gönderince alan tarafta çalışan doğrulama yazılımı doğrulamaları yapılıyor.

5070 sayılı Kanundan bahsettik. Bu kanun “Elektronik imza ıslak imzayla eşdeğerdir” diyor. Tabii, sertifikaların da bir hayat çevrimi var. Sertifikayı talep ettiniz, size verdiler, bir yıl ya da üç yıl ömrü var. Bu arada kaybedebilirsiniz sertifikanızı veya iptal ettiniz; yenisi çıkar sertifika ömrünün sonunda arşive gider. Ölen sertifikanız ondan sonra hep orada bulunuyor. Herhangi bir problem olduğu zaman, oradan bunu inceletebiliyorsunuz.

Asıl burada önemli olan, elektronik imzanın atılış biçimi. Piyasada birtakım şirketler türedi. Hiç kimse kalkıp da, bunun ileriye dönük olarak saklanması gerektiğini düşünmedi ve BES olarak üretmeye başladılar. Oysa, atılan imzanın doğrulanmasının yapıldığı anda, zaman damgasının da içine konulması lazım. Oysa, atılan imzanın içindeki sertifikanın geçerli olup olmadığı ve zaman damgası bilgisinin de içinde olması lazım. Son olarak

Türkiye'de bir de yeni Ticaret Kanunu çıktı. Yeni Ticaret Kanununda diyor ki, "Elektronik imzaya tebliğ ve tebellüğ edebilirsiniz." Ki, sanırım sizde de benzeri bir kanun çıkacak.

Hepinize tekrar teşekkür ediyorum.

PANEL YÖNETİCİSİ- Teşekkür ediyoruz.

Sayın Ömer Yurdagül'ü konuşmasını yapmak üzere davet ediyorum.

Ömer Yurdagül, Kamu Yönetimi Araştırma Derneği Başkanı.

Ömer bey sunumunu yapmak üzere hazırlığını yaparken,

ÖMER YURDAGÜL (Kamu Yönetimi Araştırma Derneği Başkanı)- Derneğimiz, akademisyenlerden, bürokratlardan, müfettişlerden oluşan bir dernektir. Amacımız, kamu yönetiminin sorunların; gerek Türkiye'nin, gerekse Türk dünyasındaki sorunların araştırılması ve çözümlerine katkının sağlanmasıdır.

Tabii, son konuşmacı olduğum için, bunun nimetlerinden de istifa etmek istiyorum açıkçası. Çok saygıdeğer hocalarım benim sunumumun içeriğindeki birçok konuya değindikleri için, o kısımları daha hızlı geçeceğim. Böylece, sizin çok fazla zamanınızı almamış olacağım.

Birçok kamu kurumu nezdinde, "Acaba son durum nedir?" şeklinde bir bilgi aldık. Özellikle Türksat'a gittiğimizde, e-devletle âlâkalı kısımlar geliştirmişler.

Mustafa Kemal Atatürk, "Zamanın gereklerine göre bilim ve teknik ve her türlü buluşlardan azami derecede yararlanmak zorunludur" demektedir.

Bir sürü teknolojik ürünler, bir sürü farklı şeyler, mevzuat yapıyoruz, kanun yapıyoruz. Aslında bunun bir temel amacı var; güven. Yani vatandaş kamu yönetimine güveniyor, kamu yönetimi de vatandaşa güveniyor. Eskiden en çok şikayet ettiğimi konu neydi? Biz gittiğimiz zaman, bir işlem için yüzlerce belge

isteniliyordu. Yani çok basit bir sağlık karnesinin çıkarılmasında, nüfus kaydından diğer kayıtların olup olmadığına kadar bir sürü şeyler istenilirdi. Fakat biz bunların devletin bilgi sistemleri içerisinde var olduğuna inanıyoruz, bizim adımıza kayıtların tutulduğuna inanıyoruz. Fakat burada şöyle bir şey var: Bu güven gerçekten kontrol edilmezse ya da bizim devletimize karşı güvenliğimizde bir sıkıntı olur mu? Geçen gün bir kamu kurumunda -öğrencilerle ilgili bir kamu kurumu bu- bir liste yayınlandı, daha sonra da o listenin bir yazılım hatası nedeniyle yanlış yazıldığı belirtildi ve komple sıralar değişti. Bu, insanların hakkına şiddetli şüpheler getirdi. E-devlet dediğimiz kavramla, bu güvenin karşılıklı kontrollerle beslenmesi ve güvence altına alınması gerekiyor.

Güvenlik politikasıyla ilgili kısımları geçiyorum. Sayın hocalarımız bu konuları işlediler. Ama özellikle burada fiziksel güvenlikten bahsetmek istiyorum. Malum, şu anda Çin'de bir deprem oldu. Kocaeli de benzeri bir deprem yaşamıştı. Ben de görevim nedeniyle 17 Ağustosta Kocaeli'nde olan insanlardan bir tanesiydim.

Güvenlik derken, sadece teknolojik güvenlik anlamında güvenliğin ötesinde bir güvenlik kavramı algılamamız gerekiyor. Yani binaların tasarımından, depreme dayanıklılıklarından, orayı kullanan insanlardan, girip çıkanlara kadar daha geniş bir güvenlik kavramını kurumların bir politika haline getirmesi gerekiyor. Yani kurumların da ihtiyaçlarına göre güvenlik daireleri geliştirmeleri gerekiyor.

17 Şubat 2003 tarih ve 2003/10 sayılı Başbakanlık Genelgesiyle, ülkemizin üye olduğu OECD'nin bilgi ve iletişim teknolojileriyle yapılan haberleşme ve bilgi alışverişlerinde güvenliği ve kişisel mahremiyeti sağlamak amacıyla bir rehber yayınlandı. Burada, "Dünya çapında bilgi ve iletişim ağlarını kullanan hükümetler, iş çevreleri ve bireyler arasında haberleşme özgürlüğü ve mahremiyet gibi demokratik toplum değerleri ile bağdaşık güvenlik kültürünü oluşturmayı amaçlamaktadır. OECD üyesi ülkelerin

ortak tutumunu yansıtan söz konusu rehber ilke, iş dünyası ve sivil toplum kurumlarının da desteğini taşımaktadır" denilmektedir.

Bununla amaçlanan şey nedir? Bilgi sistem ve ağlarının koruma aracı olarak tüm kullanıcılar arasında güvenlik kültürünü teşvik etmeyi; bilgi sistemleri ve ağlarının karşı karşıya olduğu riskler ve bu risklere karşı mevcut politikalar, uygulamalar, önlemler ve prosedürlerle ilgili bilinci arttırmak ve bu yöntemlerin uygulanmasının gerekliliğini vurgulamayı; bilgi sistemleri ve ağları ile bunların sunum ve kullanım yöntemleri konusunda tüm kullanıcıların güvenini artırmayı; bilgi sistemlerinin ve ağlarının güvenliğine yönelik uyumlu politika, uygulama, önlem ve prosedürlerin geliştirilmesi ve uygulanması ile ilgili etik değerlere kullanıcılar tarafından saygı gösterilmesi ve güvenlik konularının iyi anlaşılmasına yardımcı olacak genel bir referans çerçevesi oluşturulmasını; güvenlik politikalarının, uygulamalarının, tedbir ve prosedürlerinin geliştirilmesi ve uygulanması açısından tüm kullanıcılar arasında işbirliği ve bilgi paylaşımını teşvik etmeyi; standartların geliştirilmesi ve uygulanmasında rol alan tüm kullanıcıların güvenlik konusunu önemli bir hedef olarak belirlemelerini teşvik etmeyi amaçlamaktadır. Burada en temel olan şey, bu sistemi kullanacak olan insanların bundan bir değer üreteceğini bilerek, etik değerlere yani bilişim etiği dediğimiz Internet etiğine; yani bu etik değerlere saygı göstermesi gerekiyor, karşı taraftaki insanların haklarını ihlal edebilecek uygulamalardan kaçınması gerekiyor.

Kullanılacak güvenlik yönetimiyle ilgili kapsamlı bir yaklaşım benimsenmelidir. Kullanıcılar, bilgi sistem ve ağlarına yönelik güvenlikleri incelemeli, değerlendirmeli.

Sonuç ne olmuş? Mevzuatı çıkarıyorsunuz; fakat tüm kullanıcılarda ideal bir kültür anlamında bunun yerleşmediğini görüyoruz. Bunun nihayetinde yasal birtakım haklar ihlali olduğu zaman da yasal birtakım uygulamalara maruz kalıyorlar insanlar. Fakat kamu yönetiminde, özellikle bu bilişim kültürü alanında

bir zafiyet olduğunu d düşünüyorum bir sivil toplum kuruluşu olarak.

Türkiye Bilgi Toplumu Strateji Belgesinden bahsetmek istiyorum. Toplam 203 farklı proje yürütülmüş ve bu projelerden farklı farklı kurumlar kendi alanlarına ilişkin projeler geliştirmişler. Daha sonrasında ise, 2006 ve 2010 yılını kapsayan bir strateji geliştirilmiştir. Bir Danışma Kurulu şeklinde, e-ticaret tabanlı bir anlayış benimsendi. Fakat daha sonrasında bu dönüşüm stratejisiyle birlikte bu tüm kamu kurumlarının; yani hem merkezi kamu kurumlarının, hem yerel yönetimlerin bir ortak sorunu oldu ve bu alana yönelik olarak da yeni bir yapı benimsendi; yani bilgi toplumunun temel stratejisinin hedefleri, kamu yönetiminin işleyişi ve modernizasyonunu sağlayan hedefler, hizmetlerin erişilebilir olması. Fakat ben, "Bizim bu kurtulduğumuzu sandığımız bürokrasi acaba bu bilişim sistemlerinin işlememesi, birtakım sıkıntılar nedeniyle ofline olur mu, bundan bir sıkıntı yaşar mıyız?" diye de endişe ediyorum açıkçası.

Bu bilgi toplumu eksenli uygulama stratejisinde amaçlar belirlenmiş. Bu bir sosyal dönüşüm modeli, bilgi toplumuna sosyal dönüşüm modeli. Bilgi teknolojilerinin iş dünyasını etkilemesi bekleniyor. Kamu yönetiminde teknolojilerin bir kaldıraç olabilmesi için, kamu yönetiminin bilgi teknolojileri süreçlerini de göz önüne alıp yeniden yapılanması gerekiyor. Rekabetçi, yaygın ve ucuz bilişim altyapı hizmetlerine değindik. Şu ana kadar daha tamamı gerçekleşen olmadı. İnşallah, 2030'da bu eylemlerin hayata geçmesini ve bir fayda sağlayacağımızı umuyorum.

Bu, şu andaki Strateji Belgesindeki konu. Strateji ve politika belirlenmesi, E-Devlet Türkiye İcra Kurulu, kaynak tahsisi, stratejik formülasyon, uygulama formülasyonu... Kamu Yönetimini Geliştirme Genel Müdürlüğü, İçişleri Bakanlığı Mahalli İdareler Genel Müdürlüğü uygulamada dönüşüm liderleri. Yine kamu kuruşlarında bir sorumlu kuruluş Türksat A.Ş. oldu. Telekom özel bir şirket oldu. Dolayısıyla, görevi yürütemeyeceği anlaşıldığından,

bu, şu anda Türksat A.Ş.'ye verildi. Performans değerlendirmesi için E-Dönüşüm Türkiye İcra Kurulu, dış denetim için Sayıştay, iletişim için DPT görevlendirildi.

Bu, biraz öncekinin farklı bir yorumu.

Güvenlik kısmına geldiğimiz zaman, Strateji Belgesinde güvenlik kısmı acaba ne içeriyordu? Ben kısaca, güvenlikle âlâkalı gördüğüm şeyleri aldım. Birlikte çalışabilirliği sağlamak çok zor. Dolayısıyla, ortak bir bilgi güvenliği ağı geliştirilmesi için bir çalışma yapılması öngörülüyor. Yine bilgi güvenliğiyle ilgili yasal düzenleme yapılması için, Kişisel Verilerin Korunması Hakkında Kanun Tasarısı, verilerin elektronik ortamda korunmasına ilişkin bilgi güvenliği sistemlerinin geliştirilmesi amacına uygun yasal çalışmalar ve en önemlisi, 88. Eylem dediğimiz, yine TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsünün de görevli olduğu bir çalışma var. Bu çalışmada, bir ulusal bilgi güvenliği kapısının kurulması öngörülüyordu ve bu kapı kuruldu. Bunun önemi şu bence: Kamu yönetiminde, özellikle bilgi güvenliğinin arttırılmasına yönelik olarak birçok rehber yayınlandı. Yani şurada görmüş olduğunuz birçok rehberi birçok kamu kurumu para vererek dışarıdan satın alıyor. Gerçekten değerli bir çalışma, kendilerine de ayrıca teşekkür ediyoruz kamu kurumları olarak. Şu anda görev yaptığım kurumda denetim birimindeyim ben. Bu çalışmalardan, özellikle bilgi teknolojileri denetimi alanında istifade ettik. Çok teşekküre ediyorum.

Hocalarımız 27001 Standardından bahsetti. Ben merak ettim, "Acaba kaç kamu kurumu almıştır?" diye. Bunu burada açıklıyorum; iki tane kamu kumu almış. Fakat bize bu bilgiyi veren görevli şunu da söyledi: "Ben tanık oldum ki, Türk Standartları Enstitüsü dışında 27001 belgesi veren kurumlar var." Dolayısıyla, bu bilgi ne kadar doğrudur, bilemiyorum; yani bunun bir istatistiği yok.

Bu eylem şeyinde şunu söylemişler: "Korsanları küçümsemeyin. Internet'e daha çok önem verin. Güvenliğinden emin olmadığınız sistemleri kullanmayınız. Bilgisayar korsanlarını küçümsemeyin.

Ne yapıyorsak Türkiye için. Amacımız, Internet'te Türk'ün gücünü dünyaya göstermektir" mesajını bıraktılar, tavsiye olarak da site kodlarının gözden geçirilmesini, resim uzantılarının denetlenmesini, şifrelerin günlük olarak değiştirilmesini tavsiye ettiler." Özellikle Bilgi Edinme Kanunundan sonra bütün kamu kurumlarından Internet sayfası artık resmi bir standart haline geldi. Yani merkezi idare örgütleri, 3628 belediyenin tamamı Internet sitesi kurmak ve oradan bilgi edinme müracaatlarını ve sonuçlarını Internet üzerinden almak konusunda bir yasal zorunluluk vardır. Bu nedenle kamu kurumları, gerek yeterli bilgiye sahip olmayan kendi personeli, gerekse özel şirketlerden yardım alarak bu çalışmayı yaptılar. Yani bu, sadece bizde de değil; İngiltere'de de birçok laptop çalınmış.

Bu kısımları geçiyorum; fakat burada önemli gördüğüm, e-devletin sürekli, ulaşılabilir, şeffaf ve çift yönlü bir iletişim ağı olduğunu, karşılıklı bir etkileşim alanı olduğunu ve geliştirilmesi gerektiğini ifade etmek istiyorum.

E-kurum olgunlaşma modeli var. Dört tane süreç var bu süreçlere bağlı olarak, e-dönüşüm stratejisi, kurumsal altyapı, vatandaş servisleri anlamında; başlangıç, bilgilendirme, etkileşimli düzey ve geçişken güzey olarak.

Başlangıç düzeyinde, özellikle bilgi güvenliği anlamında, güvenlik düzeyi düşüktür diyoruz birinci düzeyde. Yani birçok kamu kurumunun altyapı açısından düşük düzeyde olduğunu görüyoruz. Yine ikinci düzeyde de kurumun işlevleri birim seviyesinde yürütülmektedir, yani üst yönetimin de desteği yoktur. Yine güvenlik politikaları yoktur burada. Üçüncü düzeyden sonra ise üst yönetimce benimsenmiş bir e-dönüşüm projesi vardır, kurumsal bilgi güvenlik politikası vardır ve sistemler birleşiktir. En son düzeyde ise kurumsal girişim güvenliği politikaları vardır. BİT uygulamaları, üst düzey güvenlik teknoloji uygulamaları vardır. BİT kullanımında yüksek düzeyde güvenlik önlemleri uygulanmaktadır. Biraz önce bahsettiğim yasal zorunluluktan

dolayı ülkemizde bu sistemler kurulmuştur. Dolayısıyla, güvenlik açısından altyapı hazır olmadan, kamu kurumlarının çoğu bütün bilgilerini, kamuya ait bilgilerini Internet'e açmak zorunda kalmıştır.

Bu alanla âlâkalı olarak iki tane denetimden bahsetmek istiyorum. Bir tanesi, şu anda var olan Sayıştay'ın denetimi. İkincisi ise, 5018 sayılı Yasayla oluşturulan Kamu Mali Kurumlar Yasasında birçok hüküm getirildi bu konuyla âlâkalı olarak. Üç tane mekanizma geldi; iç kontrol, dış kontrol müessesesi ve risk yönetimi. Bunlar yeni konular. Standartlar yeni yeni yayınlanmaya başlıyor. Biraz önce bahsettiğim gibi, birçok yasal uygulama çıkıyor, ama bunları kontrol eden sistemlerimiz yok. Bir standardın benimsenmesi gerekiyor. Bu konuda da Bankacılık Düzenleme Denetleme Kurulunun COBIT anlayışını benimsediğini ifade etmek isterim.

Sayıştay'ın üç tane raporu var bu alanda, yine bilgi güvenlik anlamında. Bunlardan bir tanesi Hazine Bilişim Sistemleri Raporu. Internet Sistemlerinin Performans Raporu 2006, E-Dönüşüm Türkiye Projesi çerçevesinde yürütülen faaliyetler yine aynı tarihte yayınlandı. Hazine'nin özellikle bütçesinde o yıl bazı tutarsızlıklar oldu, kurumlar arasında kayıp kaldı, borç rakamları tespit edilemiyordu. Sonuçta ne oldu, onu vurgulamak isterim. Birçok riskleri var; iç denetim riski, belgeleme politikaları riski görülmüş; girdi kontrolleri, değişim yönetimi, yazılım geliştirme, fiziksel kontroller, mantıksal erişim kontrolü ve güvenlik denetimi. Yani bu siyahla gördüğünüz alan, özellikle risk alanını gösteriyor.

Sonuçta ne oldu? Hazine Müsteşarlığının o yılki bütçesi Sayıştay Genel Kurulunca reddedildi. "Hazine bilişim sistemlerini yeniden yapılandırma çalışması tamamlamalıdır" denildi. "Yeni sistemde, Hazine Bilişim Sistemleri Raporunda değinilen ve sistemin güvenliğini etkileyen kontrol zaafları giderilmelidir" denildi.

Türk kamu yönetimi olarak yaklaşık 6 yıl kadar bir zaman geçirmişiz. Kamu kurumlarından iki tanesi bilgi güvenliğine önem

vermiş. Bir de İGDAŞ örneği verildi, İGDAŞ'ın bilgi güvenlik sistemini kurduğunu söylediler. Yani bu kadar zaman geçmiş; ama nedense, biz her şeyi sona bırakıyoruz ve riskleri gittikçe katlıyoruz.

Sivil toplum örgütü olarak bizim bu konuda önerilerimiz neler? Kamu kurumlarında, görev, yetki ve sorumluluklar tanımlanmalı, güvenlikle ilgili düzenlemeler mutlaka yapılmalı. Kamu yönetiminde, sevil savunma planlarına bilgi teknolojileri güvenliğiyle ilgili bilinçlendirme konuları ilave edilerek güncellenmelidir. Kamu kurumları için, gerek merkezi, gerek yerel yönetimler için bir kamusal standarda dönüşmesi gerekiyor. Kamu kurumları ve çalışanları güvenlik konusunda bilinçlendirilmeli, güvenlik konusu herkes tarafından paylaşılmalıdır. Sorumluluklar paylaşılmalı, sorunun önemi anlaşılarak sahip çıkılmalıdır. Kamu kurumlarında güvenlik politikaları yazılı olmalı, çalışanlarla paylaşılmalı, kontrol süreçleri geliştirilmelidir. Kamu bilgi sistemlerini kuracak, uygulayacak, denetleyecek personele yatırım yapılmalı. Bilişim alanında çalışan personelin teşvikini sağlayacak özel işe alma süreçleri yeniden gözden geçirilmeli. Mali destekleyici ücret sistemleri geliştirilmelidir. Kamu kurumlarının bilişim alanındaki projeleri desteklenmeli. Bu tür projeler bir yatırım olarak düşünülerek, fayda-maliyet analizleri daha ciddi yapılmalı. Bilgi teknolojileri alanında yapılacak her türlü yatırımın ülke bazında data takibini sağlayacak bir bilişim istatistik ve izleme sisteminin geliştirilmesi sağlanmalıdır. Kamu kurumlarında bilişim etiği uygulamaları ve kontrol süreçleri oluşturulmalı. Kamu kurumlarının bilgi teknolojileri konusunda uluslararası standartlara uygun bilgi teknolojileri kontrol süreçleri oluşturulması ve risk yönetim sistemlerinin kurulması ve geliştirilmesi sağlanmalıdır. Kamu kurumlarında iç denetimin işlev ve önemi anlaşılmalıdır. Uluslararası standartlara uygun bilgi teknoloji denetimi ve bilgi güvenliği konusunda rolüne uygun olarak kaynak tahsisi yapılmalıdır.

Bu hizmetleri yaparken, kamu hizmetlerinin sunulmasında da

sayısal uçurum var. TÜİK tarafından yayınlanan bir araştırmada şöyle bir şey var: Şehirde yaşayanlar köyde yaşayanlara göre hizmetlerden daha fazla yararlanma hakkı elde ediyorlar. Beylerimiz, bayanlara göre daha fazla yararlanıyor Internet'ten. Özürlü vatandaşlarımız var özellikle. Bu performans raporlarında da özellikle belirtilmiş. Yani kamu kurumlarında herkesin yararlanabileceği şekilde, özürlü-özürsüz bütün vatandaşların anlayabileceği şekilde siteler dizayn edilmeli. Tam bilemiyorum; yani teknik biri değilim ben, denetim elemanıyım. Yani uluslararası standartlarda varsa, ona uygun olarak yapılmalı. Yine aynı şekilde, öğrencilerin bilişim alanındaki eğitimleri alması sağlanmalı. Bu alanda çalışanları teşvik etmek için bir tazminat gibi bir şey konulmalıdır. İletişimin üzerindeki vergiler düşürülmelidir teşvik açısından. Bilgi toplumu stratejisi kurumsal yapılanma modeline 5018 sayılı Yasayla ihdas edilen iç denetim de ilave edilmelidir.

Sabırla dinlediğiniz için teşekkür ediyorum. (Alkışlar)

PANEL YÖNETİCİSİ- Teşekkür ediyoruz.

Soru-cevap bölümüne geçiyoruz.

Buyurun.

Doç. Dr. İBRAHİM SOĞUKPINAR- Bir arkadaşımız, "Türkiye Cumhuriyetinin Kasım 2001'de Avrupa Birliğine e-devletle ilgili olarak verdiği raporda, e-devletten sorumlu bakan olarak Sayın Ekrem'e değinilmişti" deniliyor. DPT'den Recep Çakmak, Halil İbrahim Haksever'in E-Devlet Projesinden sorumlu oldukları belirtilmiş" demiş. Teşekkür ediyoruz kendisine.

Diğer soru, Sayın Doç. Dr. Kadri Büründcük tarafından yönlendirilmiş. Soru şöyle: "Türkiye'nin e-devlet hazırlığı 0.48. E-devlete katılım 0.1364. Hazır olmanın katılımdan yüksek olmasının, gelişmekte olan devletlerde normal olduğunu düşünüyorum. Ancak, bu kadar fazla olmasının sebebi sizce nedir?" E-devlette hazırlık oranı yüksek, katılım düşük. Ben şöyle düşünüyorum: Birincisi, kullanıcı olan vatandaş yeterince bilgili

değil ve şu anda tam olarak yeterli güvene sahip değil. Yani bizim Türk vatandaşının bir özelliği var; tam güvenmediği işi yüz yüze yapmak ister. Örneğin, cebinde banka kartı vardır, gidip bankada kasiyerden parayı çeker veya elektronik bankacılığı kullanmaz. Sanırım, vatandaşın bilgilendirilmesi ve bu güvenin artmasıyla e-devlete katılım oranı artacaktır.

Diğer soru Sayın Gölay Şakiroğulları tarafından sorulmuş. İki soru var. Birinci sorusu, "E-devlet çalışmalarında, çalışan bilişim elemanlarının yeteneği, eğitimi, bilgi ve tecrübe açısından gerekli şartları konusunda bir yönetmelik var mı?" şeklinde. Bildiğim kadarıyla şu anda yok.

Bir devletin bu çalışma için kendi elemanları, bir de özel sektörden bu hizmeti sağlayan elemanları var. Dolayısıyla, devlet sektörü kendi yapmıyor bu çalışmaları, ihaleyle şartnamesini hazırlıyor. Şartnamede, personelle ilgili nitelikleri de bazen belirtiliyor. Genellikle böyle uygulamalar yapılıyor. Dolayısıyla, kişiler hakkında özel bir yönetmelik yok.

Diğer soru, "Bilgisayar Mühendisliği Bölüm Başkanı olarak, bilişim projelerinde bilgisayar mühendislerinin imza yetkisi olması gerektiğine inanıyor musunuz?" şeklinde. Bu soruyu tam olarak anlamadım. Şöyle değerlendiriyorum: Biliyorsunuz, Türkiye'deki projelerde imza yetkisi ve imza prosedürü daha ağırlıklı olarak bayındırlık ve yapı esaslı düzenlenmiş durumda mevzuat gereği. Örneğin, bir binanın inşaatında inşaat mühendisi projeyi hazırlayıp imzalıyor, elektrik projesini elektrik mühendisi imzalıyor, makine tesisatıyla ilgili projeyi makine mühendisi imzalıyor; ama bilişim projelerinde böyle bir mevzuat yok şu anda. Örneğin, bir yazılım projesi hazırlıyorsunuz veya yazılım geliştireceksiniz; projeyi hazırlayıp ... gerekmiyor. Gerekiyor mu? Yazılım projesini siz hazırlayıp, götürüp elektrik mühendisine mi imzalatıyorsunuz? Yani bir yerde özellikle bilgisayar mühendisliği kavramı meslek odaları açısından biraz yeni olduğu için, mevzuatta bazı eksiklikler var kanaatimce. İletişim ağı projelerinde bir eksiklik var. Örneğin,

bilgisayar ağı projesi hazırlayıp, binanın bilgisayar ağı dağıtımını genellikle elektrik mühendisleri hazırlıyor. Yani biraz tesisat kapsamına giriyor; ama bilişim projelerinde, projeyi hazırlayıp, gidip Elektrik Mühendisleri Odasından onay alınıyor mu, tam olarak bilmiyorum. Gerçi, çoğu zaman yazılım projeleri dört başı mamur projeler olarak hazırlanmıyor, analizler yapılıyor. Yani burada bir mevzuat eksikliği var kanaatimce.

SALONDAN- Yazılım mühendisliğinde proje sözcüğünü kullanmanızla inşaatta proje sözcüğünü kullanmak arasında çok fark var.

İBRAHİM SOĞUKPINAR- Bunu kastediyorum. Yapı mevzuatında bu düzenlenmiş, ama bilişim projelerinde...

SALONDAN- Mevzuatta yazılım var mı?

Doç. Dr. İBRAHİM SOĞUKPINAR- Onu belirtmek istiyorum. Yani bu mevzuat yok şu anda. Dolayısıyla, öyle olmayınca da önce bu konuya el atmak gerekir diye düşünüyorum.

SALONDAN- Hocam, oldum olası derttir bu. Yıllar önce de bu tür tartışmalar yapıldı. Biliyorsunuz, bilgisayar mühendislerinin ayrı bir odası yok, Elektrik Mühendisleri Odasına üye olabiliyorlar. Aslında olması lazım.

Doç. Dr. İBRAHİM SOĞUKPINAR- Mutlaka olması lazım.

SALONDAN- Çünkü bilişim ağları, bilgisayar ağları son derece önemli bir hale geldi. Neredeyse bir binanın kendisi kadar önemli hale geliyor, bir mimarın yaptığı iş kadar önemli. Mutlaka bunun üzerine düşünülmeli, gerekli mevzuatların çıkarılması için girişimlerde bulunulmalı bence.

Doç. Dr. İBRAHİM SOĞUKPINAR- Katılıyorum. Buyurun.

GÖLAY ŞAKİROĞULLARI- Hocam, sorunun sahibi benim. Bölüm Başkanısınız. "Ne yapabilir yetiştirdiğim çocuk" diye

düşündüğünüzde, bu soruya "Olmalı" mı demelisiniz? Çünkü bir işi iyi bilen, eğitilmiş bir adam yaparsa, o iş o kadar iyi, o kadar kalitelidir ve o kadar da güvenilirdir. Siz, çocuklarınıza bu donanımı veriyor musunuz? Bu tür dersler veriyorsanız, çıktığı zaman, çocuk ne gibi ehliyetlere sahip olmalı, ne gibi yerlerde kullanılmalıdır? Yani biri yerde, e-devlet uygulamalarında eleman politikaları içinde yer ne olmalıdır? Esas olarak sorumun püf noktası buydu. Herhalde ben yanlış ifade ettim. Bir işi ne kadar ehli yaparsa, ne kadar liyakat sahibi yaparsa, bu iş o kadar güvenilirdir.

Doç. Dr. İBRAHİM SOĞUKPINAR- Türkiye'de şöyle bir realite var: Üniversitedeki akademisyenler öğrenciyi yetiştiriyor, ama mevzuatın değişmesinde etkileri o kadar fazla değil. Bir defa, doğrudan siyasi otoritenin bunu kal'e almasıyla orantılı bir olay. Siyasi otorite bunları kısa sürede kal'e almıyor çoğu zaman. Dolayısıyla, Türkiye'de böyle kötü bir durum var. Hatta bazen, "Siz oturduğunuz yerde oturun, konuşmayın" gibi şeyler söyleniyor üniversitedeki akademisyenlere. Dolayısıyla, böyle kötü bir durum var. Bunu çözmek hakikaten şu anda biraz siyasi tartışmalara girer.

Teşekkür ederim.

PANEL YÖNETİCİSİ- Buyurun.

ERALP CURCİOĞLU- Tabii ki, burada zaman kısıtlı olduğu için, çok fazla ayrıntılara giremedik; ama biz, e-devlet projelerini yaparken, Lizbon'da alınan bütün kararları... Çünkü bizde olup da orada tanımlanmamış hizmetler vardır. Bunun içerisinde, bizde hazır olan polisteki sicil kayıtları ... gibi bir sistem var. Başbakanlık, bu bilgileri 24 saat kullanabilecek kurumların ulusal bilgi sistemine entegrasyonuyla ilgili bir genelge yayınlamıştı. Bu bilgileri ulusal bilgi sistemine aktarmalarıyla ilgili genelgeyi yayınlamıştır. Bunlar içerisinde birçok bilgi vardır; bu bilgiler elektronik ortamdadır şu anda. Biz, bunların çalışmalarını yaptık.

Bizim yaptığımız sadece şu: Şahıs geliyor, kimliğini gösteriyor,

o şahsın kimliğini sisteme işliyoruz ve diyoruz ki, "Şu kimliği kullanan şahıs, bu seri numaralı kartı almıştır."

SALONDAN- Kredi kartı kullanabiliyorsa zaten Internet'ten satış almak için, sizin pek yapacağınız bir şey yok. Kredi kartıyla satışta zaten banka benim kimliğimi onaylıyor, ismim geliyor zaten, kimlik bilgilerim de geliyor, onun üzerinden bilgilerim zaten geliyor.

ERALP CURCİOĞLU- Bu yaklaşım doğru. Başka farklı çözümlere yönelen arkadaşlar var kurumda.

Yalnız, çok ilginç bir şey var. Kartı kazıdığınızda karşınıza çıkan numara kredi kartı numarasıdır.

Mustafa bey, "Tüm devlet kurumlarının kendi aralarında online servisi var mı?" diye sormuş. Şu anda E-Devlet Projesinin ana bacağını oluşturan kurumların hemen hemen hepsinin online bağlantıları vardır. Olmasa, bu verileri alma ve güncelleme imkânı olmazdı zaten. Önümüzdeki 1-1,5 ay içerisinde, bağlantısı olmayan kurum, daire, okul ve benzeri bir devlet kuruluşu kalmayacaktır. Şu anda kendi aralarında bilgi paylaşımı yapabiliyorlar. Evet, bu tür projeler vardır. Yollarda hız tespit radarları vardır bizde. Yol boyunca gördünüz mü, bilmiyorum. O radarlar sizi çektiğinde, o aracın kimliği tespit edilir, araç kaydı sorgulanır, sorgulandıktan sonra aracın kime ait olduğu bulunur, daha sonra o kimlik ulusal bilgi sisteminde bulunan adresle birleştirilerek, adınıza bir zarf yazılır ve evinize gelir. Bu yapı tamamen e-devlet sisteminin üzerindedir ve otomatik olarak yapılıyor. Burada e-devlet uygulamasının ilginç bir örneği vardır. Bu, veri paylaşımının canlı bir örneğidir.

Bir arkadaşımız, "Felaket Kurtarma Merkeziniz var mı?" diye sormuş. Felaket Kurtarma Merkezi kurulması için bir çalışmamız var. Tamamen farklı bir yerde, farklı bir bina içerisinde, hatta şimdiki sistemi yedek yapacağız. Oraya yeni bir sistem kurarak, daha sağlıklı bir sistem kuracağız. Bununla ilgili bir çalışma var şu anda.

Normal koşullarda ulusal bilgi sisteminde bu veriler korunuyor. O yönden kesinlikle güvenmeniz lazım. Ama özellikle sırf kendilerinin verilerini saklamamız için bize veren kurum şu anda yok. Bu konuda herhangi bir mevzuat da yok. Ama önümüzdeki süreç içerisinde bunlar da olacaktır.

"Güvenlik açısından saldırılar oluyor mu?" diye sorulmuş. Evet, zaman zaman bu tür saldırılar oluyor. Bu saldırıları tespit ederek, mümkün olduğu kadar tümünü kapatma yoluna gidiyoruz. Bu tür saldırılar kesinlikle ve kesinlikle teknolojiyi kullanarak engelleyebileceğimiz saldırılardır. Bence en büyük sorun, kurumların iç yapılanmalarıdır. İç güvenliklerin arttırılması lazım.

SALONDAN- Bu soruları soran bendim. Kıbrıs'ın e-devlet konusunda çok gelişmiş olduğunu gördüm, sevindim de; ama bir Estonya örneği var. Kıbrıs da kritik bir ülke. Siber ataklara karşı herhangi bir önlem var mı? Bazı atakların çok da önlemi yok. Örneğin, sizin bant genişliğiniz kısıtlıdır, sınırlı sayıda çıkışınız vardır. Buna karşı bir önleminiz var mı?

ERALP CURCİOĞLU- İleride bunlar sağlanacaktır. Bu tür şeylere karşı, bildiğimiz, iyi kaliteli diyebileceğimiz, yani iyi seviyedeki donanımlar var. Bugüne kadar böyle bir sorun yaşamadık. Zaten Türkiye'deki bir firmayla anlaşmamız var.

SALONDAN- Estonya örneğini biliyor musunuz, hiç duydunuz mu? Ruslar tarafından büyük oranda kullanılmaz hale getirildi, sitenin altyapısı kullanılamaz hale getirildi.

ERALP CURCİOĞLU- Estonya iyi bir örnek bizim açımızdan. Biz, Estonyalılarla çok görüştük. Hatta Estonya'nın bir E-Devlet Akademisi vardır; oradaki hocalarla çok görüştük, konuştuk. Hangi türden bir saldırı olduğunu bilmiyorum; ama Estonya'nın geliştirdiği her şeyi ... altındaki yazılımlarla geliştirdiğini ve açık kaynak kodlu olduğunu çok iyi biliyorum. Söz konusu saldırının

ne olduğunu hiç incelemedim.

SALONDAN- Kusura bakmayın, vaktinizi alıyorum; ama önemli bir konu olduğu için söyleyeyim. Ruslar sürekli bant genişliğini tüketerek, içeride bulunan devlet kurumlarına saldırarak, e-devleti çalışmaz bir hale getirdiler.

PANEL YÖNETİCİSİ- Buyurun.

ERSİN GÜLAÇTI- Gelen sorulara cevap vermeye çalışayım.

Sayın Kadri Büründük'ün, Panel Yöneticisinin bir sorusu var. "Vermiş olduğunuz sertifika sayısının 20 bin civarında olduğunu söylediniz. Müracaat ... nedir acaba?" diye sormuş. Biz şöyle bir yöntem uyguluyoruz: Eğer gerçekten çok sayıda sertifika almak isteyen kurumlar varsa ve bunların sistemleri müsait değilse, zaten ilk yaptığımız toplantılarda kendilerine bu durumu bildiriyoruz. Resmi olarak bir yazıyla başvurmalarını ertelemelerini istiyoruz. Fakat daha küçük çaplı olan başvurularla ilgili başka bir politika izliyoruz. Burada da bununla bağlantılı bir soru var. Yüksek Teknoloji Enstitüsünden Furkan bey sormuş. Az önceki soruyla bağlantılı alarak, 2006 yılında çıkartılan bir Başbakanlık genelgesi var. Elektronik imza altyapısı uygun olan kurumlara sertifika verilmesi konusunda bize yetki verdi. Bunları denetleyip, Eğer elektronik imza kullanmaya müsaitlerse sertifika verilmesi söylendi. Aksi takdirde, bizim için sorun yok. Ama o sertifikalar alındıktan sonra üç yıl ömrü var. Eğer üç yıl boyunca kullanılmayacaksa, devletin parası harcanmış oluyor.

Eğer çok yüksek miktarlarda sertifika almayacaksanız... Yani hiçbir uygulamanız olmasa dahi... Örneğin, belediyelerde bu durumla karşılaşıyoruz. Örneğin, bankalara ödeme talimatı imzalayıp göndermeleri gerekiyor. Bu durumlarda çok fazla incelemiyoruz.

SALONDAN- Sizin bu yazılımınız hazır olarak Internet'te yoktu, sadece kütüphaneler vardı. Kütüphaneleri kullanarak yazılım geliştirebilirsiniz" şeklinde bir ibare yer alıyordu. Yani bu imzayı belki yeni koydunuz ya da biz bulamadık. Alınması istenilen sertifika sayısı sadece iki. Ama şunu sorduk: Sizin onayladığınız, özel sektörün ürettiği yazılımlar var mı? "Bize yol gösterin, bir liste verin mesela. Biz, o firmalarla konuşalım" dediğimizde de, böyle bir listenin olmadığı söylendi. Dolayısıyla, yazılım yok ve biz sertifikayı alamıyoruz gibi bir noktaya geldik.

ERSİN GÜLAÇTI- Paket yazılım olarak, onayladığımız ve web sitemizden yayınladığımız yazılım yok. Kanunlar, yönetmelikler çıkıyor; ama bir görev verilmediği zaman, örneğin, "Kamu kurumlarının bütün bankacılık işlemleri elektronik imzayla yapılacaktır" diye bir hedef konulmuyor. Bu durumda işlemler gerçekleşmiyor.

Yazılımların onaylanmasıyla ilgili olarak da Telekomünikasyon Kurumu sertifika servis sağlayıcılara sorumluluk verdi. CWA standardı var. "O standarda uygun yazılımlar kullanılmalıdır" dedi. Bunlardan da sertifika hizmet sağlayıcılar sorumludur. Sertifika hizmet sağlayıcıları Türkiye'de yazılım geliştiren tek yer değil. Fiilen biz şöyle bir uygulama yapıyoruz: Bize başvuran firmalar olursa, onların yazılımlarını inceliyoruz; standarda uygunsa, bunların uygun olduğunu web sitemizde yayınlıyoruz. Fakat henüz yayınlanmış yazılım yok, elektronik imzayla üretilmiş olarak yok; ama özel sektörün yazılımları var. Demek ki, orada da tanıtım eksikliği var.

Bir bilgi eksikliğimiz var, onu tamamlamak istiyorum; kamu kurumları arasında, ISO 27001 sahibi olan kurumların sayısı. Sanırım, TSE'den aldığınız bilgi o. TSE kendi sertifikalandırdığı yerleri size bildirmiş. Zaten sertifika hizmet sağlayıcı kurumların ISO 27001 sertifikasına sahip olması gerekiyor. Ben, yöneticiliğini

yaptığım birimin ISO 27001 denetiminden geçtiğini ve sertifikası olduğunu biliyorum. Onu listenize ekleyebilirsiniz.

Gölay Şakiroğulları, "E-devlet uygulamalarında en önemli konu, çokuluslu tekellere, markalara bağımlı olmayan ulusal yazılımların, işletim sistemlerinin kullanılmasıdır. Bu konuda Türkiye ne kadar hassastır?" diye sormuş. Türkiye'nin bu işlerin hepsini organize eden, düzenleyen tek bir yetkili yer yok; herkesin belli bir alanlarda belli sorumlulukları ve güçleri var. Bir teknoloji bakanlığı olsaydı Türkiye'de, bu söylediğiniz nokta, tek bir politika yapılabilirdi; ama burada böyle tek bir yerden politika yapılması söz konusu değil. Örneğin, bizim Enstitümüzün bu konuda sizin görüşlerinize benzer bir politikası var. Biliyorsunuz, Pardus işletim sistemi var. Ayrıca, bilgi güvenliği için kullanılacak türde bilgi olması gerekiyor.

Tabii, bir bilinçlendirme de gerekiyor. "Sadece açık kaynak kodlu yazılım kullanılır. X firması, y firması bu sistemlere giremez" gibi bir sınırlandırma da konulabilir; ama rekabete açık olması lazım. En son, Türkiye'nin de açık standartlara veyahut da tekellere bağlı olmayan standartlara uygun şekilde oy vermesi ya da çekimser hale gelmesi için etkide bulunduk, bilgilendirdik, bilinçlendirdik.

Yüzüncüyıl Üniversitesinden Sayın Pala, yazılım güvenliğiyle ilgili bir soru sormuş. İmza işlemi akıllı kartın içindeki özel anahtarla gerçekleştiğinden, akıllı kartı kırabiliyorsa bir kişi, bu yazılımın da güvenliğini kırabilir demektir.

Onun dışında, bir yazılımı yayınlandıktan sonra, Internet'te sürekli arama motorlarından takip ediyoruz. O yüzden, indir.com vesaire belirli yazılım indirme sitelerine konuldu. Buna karşılık, kullanıcıları bilgilendirecek özellikler eklemeye çalışıyoruz. Tabii, burada kullanıcının bilinçli olması lazım; yani bilmediği bir yerden yazılım alırsa, ekranda gördüğü şeyi değil, o yazılımda yer alan

saldırganın istediği şeyi alır. Dediğim gibi, buradaki güvenlik, doğru yazılımı kullanmak.

PANEL YÖNETİCİSİ- Buyurun.

ZAFER BABÜR- Bana iki soru yöneltilmiş.

(... ...)

Teşekkür ederim.

ÖMER YURDAGÜL- Biraz öncesi sunumumda, Telekom'un özelleştirilmesi nedeniyle ... görevlerinin Türksat'a verildiğinden bahsetmiştim. Buna ilişkin bir soru geldi. "Telekom'un yabancıların kontrolünde olması, ulusal bilgi sistemi güvenliği açısından nasıl bir tehdit oluşturur?" diye sorulmuş. Telekom gibi bir kurumun özelleştirilmesinin, ulusal bilgi güvenliği açısından mutlaka sakıncaları vardır. Ancak, artık dünyada bütün ülkeler bir şekilde birbiriyle ekonomik olsun, sosyal olsun ilişki içerisine giriyorlar. Bu soruyu soran arkadaşımız acaba kredi kartı kullanıyor mu? Burada yine aynı şekilde bir risk olabilir. Bence bu, bakış açısına bağlı olarak değişir. Ancak, şu konuda bir şey söylemek isterim: Biz, ülke olarak, özelleştirmeler konusunda bazen ipin ucunu kaçırıyoruz. Mesela, karşılıklılık, ekonomik ilişkilerde çok önemli bence.

Teşekkür ederim.

PANEL YÖNETİCİSİ- Teşekkürler.

Sanıyorum, çok kısa bir katkı koymak istiyor Hasan bey.

HASAN ...- Katkı değil de, bir soru sormak istiyorum. Bir bakanlık bir yönetmelik yayınlıyor. Bunun yaşama geçmesiyle ilgili olarak bir yazılım yapıyor, fakat bu yazılımı yaşama geçiremiyor ve iki-üç ay süreyle sistemin önünü tıkıyor. Burada

çok büyük mağduriyetler söz konusu. Burada devletin bu mağduriyetleri karşılama anlamında ne tür önlemleri söz konusu? Kimin cevap vereceğini bilemiyorum, ama böyle bir uygulama ar şu anda. Üç-dört aydan beri sektörün önünü tıkamış durumda, binlerce insanın mağduriyeti var.

ÖMER YURDAGÜL- Eğer bu tarz mağduriyetler söz konusu olursa, hukuk mahkemelerinde feshedilebilir.

İBRAHİM SOĞUKPINAR- Bir şey eklemek istiyorum.

Değerli katılımcılar; sorulan sorulardan, yapılan tartışmalardan şu ortaya çıkıyor ki: Türkiye'de bir bilişim teknolojileri bakanlığının kurulması ve aktif olarak faaliyete geçmesinin ne kadar önemli ve elzem olduğunu değerlendiriyorsunuz sanırım. Bu problemlerin büyük bir çoğunluğunun böyle bir organizasyonla, en azından hantal devlet yapısından ayrılmış bir organizasyonla çözülebileceğini düşünüyorum. Sunumumda da böyle önerilerde bulunmuştum. Yani fikir olarak herkesin böyle bir konuyu desteklemesinde fayda var. Hakikaten hayati bir öneme sahip gözüküyor.

Teşekkür ederim.

PANEL YÖNETİCİSİ- Sağ olun.

Efendim, öncelikle gecikmeden dolayı hepinizden özür dilerim; ama katkılarınızdan dolayı da teşekkür ederim. Çok değerli panelistlerimiz çok değerli bilgilerini bizlerle paylaştılar. Sunumlarından dolayı kendilerine ayrı ayrı teşekkür ederim. Sizlere de ilginizden dolayı teşekkür ediyorum. (Alkışlar)