ULUSAL BİLGİ SİSTEMLERİ GÜVENLİK PROGRAMI

Hayrettin Bahşi, Bilge Karabacak
TÜBİTAK-Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
bahsi@uekae.tubitak.gov.tr, bilge@uekae.tubitak.gov.tr

ABSTRACT
Information security failures are the prominent obstacles for being information society. In order to overcome these obstacles nationwide programs for increasing security awareness and security knowledge are needed. Also, proactive security controls for public services have to be established and a road map has to be formed for other services. Turkish Information Society strategy which is prepared by State Planning Organization of Turkish Prime Ministry has an action item called "National Information Security Program". This action item addresses several tasks for providing information security of public services and increasing nationwide information security awareness. The responsible organization of this item is National Research Institute of Electronics and Cryptology. This paper presents the studies done in this program.

Key words: Information Security, Information Society, System Security

1. Giriş

Günümüzde bilgi teknolojileri günlük yaşamın her aşamasında kurumsal ve bireysel olarak kullanılmaktadır. Kamu kurumları açısından da durum farklı değildir. Kamu kurumlarının, iş süreçlerini büyük oranda bilgi teknolojileri ile gerçeklemesi bu kurumların başarısının bilgi teknolojilerine doğrudan bağlı olması sonucunu doğurmaktadır. Geçmiş yılların aksine bilgi teknolojileri kamu kurumları için bir masraf kapısı değil, bir fırsat kapısı olarak değerlendirilmektedir. Kamu kurumları bilgi teknolojilerine ne kadar çok yatırım yaparlarsa, o kadar çok bilgi teknolojilerinin sunduğu imkânlardan faydalanmakta, vatandaşlar hizmetlerden hızlı ve sorunsuz olarak yararlanmakta ve bürokrasi hızlanmaktadır. Daha geniş açıdan bakıldığı zaman ise tüm bu faydalar ülke ekonomisine katkı yapmakta, yolsuzlukların önlenmesinde ve ortaya çıkartılmasında önemli rol oynamaktadır.

Ülkemizin bilgi toplumu olma yolunda ilerlemesi amacıyla 2003 yılında T.C Devlet Planlama Teşkilatı (DPT) Bilgi Toplumu Dairesi koordinatörlüğünde "e-Dönüşüm Türkiye Projesi" başlatılmıştır. Bu projenin amacı ülkemizin bilgi toplumu olması yolunda önemli mesafeler kaydetmek ve bilgi teknolojilerinden etkin olarak yararlanılmasını sağlamaktır. Projeyle amaçlanan hedefler doğrultusunda önemli gelişmeler sağlanmış bulunmaktadır. DPT tarafından 2005 yılında "Bilgi Toplumu Stratejisi" [1] başlıklı bir çalışma başlatılmış ve çalışmada bilgi toplumu olma yolunda yapılması gereken somut adımlar belirlenmiştir.

Bilgi toplumu olma yolunda ilerlerken önem verilmesi gereken konuların başında bilgi ve bilgi teknolojileri güvenliği gelmektedir. Bilgi teknolojileri kamu kurumlarının iş süreçlerinin hemen hemen hepsinin gerçekleşmesinde kullanıldığı için bu teknolojilerden kaynaklanan riskler de iş süreçlerini kötü yönde etkileyen etkenler olarak karşımıza çıkmaktadır. Öte taraftan, bilgi teknolojileri ise hem risk çeşidini artırmakta hem riskin gerçekleşmesini kolaylaştırmakta hem de riskin gerçekleşmesi durumundaki etki seviyesini artırmaktadır. Çünkü bilgi teknolojileri, bilgiye uzaktan erişime imkan verir, bilginin bir çok kopyasının kolaylıkla oluşmasını sağlar, merkezi olarak çok fazla sayıda bilginin tek noktada depolanmasına imkan verir, bilinçli ve bilinçsiz bir şekilde bilgiyi değiştirmek, silmek, kopyalamak gibi işlemlerin kolaylıkla yapılmasını sağlar. Bilgi teknolojileri bilgiye sadece kurum içinden değil, kurum dışından da erişimlere imkân verir.

"Bilgi Toplumu Stratejisi"nin 88. maddesini "Ulusal Bilgi Sistemleri Güvenlik Programı" oluşturmaktadır. Sorumluluğu TÜBİTAK-UEKAE (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü)'ne verilmiştir. Programın en önemli hedefi başta kamu kurum ve kuruluşları olmak üzere ülkemizin bilgi sistem güvenliği ile ilgili bilgi ihtiyacını karşılamaktır. Diğer hedefi ise kamu bilgi sistemlerinin güvenliğinin sağlanması ile ilgili etkin önlemler alınmasına önayak olmaktır. Program 2007 Ocak ayı itibari ile başlamıştır ve 2009 yılı başında sona erecektir. Program başlıca altı alt projeden oluşmaktadır. 2. Bölüm'de projeler detaylı olarak incelenmiştir. Her bir proje başlığı altında, proje kapsamı, projenin hedefi ve şu ana kadar projeyle ilgili gerçekleştirilen çalışmalar ele alınmıştır.

2. Program Alt Projeleri

2.1 Bilgi Güvenliği Yönetim Sistemi Kurma Danışmanlık Projeleri

Bir kurumda bilgi güvenliğinin etkin olarak sağlanması ancak kurum yönetiminin, bilgi sistem kullanıcısının ve bilgi sistem işletmenlerinin rol ve sorumluluklarının belirlenmesi ve bu rol ve sorumluluklarının gereklerini yerine getirmeleri ile sağlanabilir. Bu amaçla, kurum bilgi güvenliği organizasyonunu, politika ve prosedürlerini belirlemelidir. Kurum, kullanılabilirlik – güvenlik dengesini etkin bir risk yönetimi süreci ortaya koyarak sağlamalıdır. Belirlenen risklerin, sahip olunan kaynaklar ve belirlenen risk düzeyleri çerçevesinde en aza indirilmesi amacıyla teknik ve yönetsel tedbirlerin uygulanması sağlanmalıdır. Günümüzde, uluslararası olarak genel kabul görmüş ISO 27001 standardı[2], yukarıda ifade edilen kapsamda bilgi güvenliği yönetim sisteminin oluşturulması ve sürdürülmesini hedefleyen en önemli standarttır.

Ulusal Bilgi Sistemleri Güvenlik Programı kapsamında pilot olarak seçilen kurumlara ISO 27001'e uygun bilgi güvenliği yönetim sistemi oluşturma konusunda danışmanlık verilmektedir. Pilot kurumlar, Başbakanlık, Adalet Bakanlığı Sayıştay Başkanlığı, ve Maliye Muhasebat Genel Müdürlüğüdür,. Bu kurumlarda, bilgi güvenliği yönetim sistemi kapsamı belirlenmiş, varlık envanteri oluşturulmuş, bilgi güvenliği koordinasyon kurulları oluşturulmuş ve kurullar işlerlik kazanmıştır. Risk analizi çalışmaları halen devam etmektedir. Çalışmaların hedefi, kurumların ISO 27001 sertifikası alabilecek seviyeye gelmesini sağlamaktır.

2.2 Ulusal Bilgi Sistemleri Tehdit Gözetleme Sistemi Kurma Projesi

Bilgisayar ağları, sistem bileşenleri ve uygulamalar, sistem açıklıklarını kullanarak sisteme zarar verecek çok sayıda tehditle karşı karşıyadır. Sistemlere ağ üzerinden erişim kolaylığı sayesinde erişim sınırları mantıksal olarak kalkmıştır. Bu sebeple saldırı ara yüzü çok genişlemiştir. Bilgi sistemleri, otomatik tarama yapan zararlı yazılımlar ve kasıtlı saldırganlar tarafından tehdit edilmektedir. Bilgi sistemlerini hedef alan tehditlerin tespit edilmesi ile ilgili saldırı tespit ve önleme sistemleri yaygın olarak kullanılmaktadır. Halen ağ ya da sunucu bazlı saldırı tespit edebilen sistemler kullanılmaktadır. Ama genelde bu tür sistemlerin "hatalı pozitif" (false positive) olarak tanımlanan yani gerçekte saldırı olmayıp da tespit sisteminin saldırı olarak belirlediği durumların oranı çok yüksek olmaktadır ya da gerçekte saldırı olup da algılanmayan durumlar sıkça gerçekleşebilmektedir. Son zamanlarda farklı bilgi kaynaklarından gelen bilgileri ilişkilendirerek saldırı tespiti yapan akademik çalışmalar ve pratik sistemler geliştirilmiştir [3, 4, 5, 6]. Bu sistemler hem saldırı tespitinin yanılma payını azaltmak hem de bir saldırının sisteme olmuş ya da olabilecek etkisini daha iyi belirlemeyi hedeflemektedir.

Kurulması düşünülen Ulusal Bilgi Sistemleri Tehdit Gözetleme Sistemi, kamu kurumlarına ait kritik bilgi sistemlerini hedef alan tehditleri tespit etmeyi amaçlamaktadır. Bu sistem, birden fazla kamu kurumunu hedef alan koordineli tehditleri tespit edebileceği gibi bir kamu kurumunu hedef alan çok ciddi saldırıları da fark edebilecek yapıda olacaktır. Farklı bilgi kaynakları ilişkilendirerek saldırı tespiti yapabilen teknoloji sistemin temelini oluşturacaktır. Ayrıca bu sisteme ilave olarak dağıtık yapıda bir balküpü (honeypot) sistemi kurularak, saldırganların kamu kurumlarına ne şekilde saldırabildikleri ile ilgili tespitler yapılacaktır. Kurulacak sistemle elde edilecek tehdit bulguları, tehdide uğrayan kurumlarla paylaşılacaktır. Ayrıca periyodik olarak tehditlerin genel analizi yapılarak kamu kurumları için genel tehdit gözlem raporları oluşturulacaktır. Bu raporlarda kamu sistemlerini hedef alan tehditlerin türlerini, dağılımlarını, kurumlara olan veya olabilecek etkileri ortaya konacaktır. Alınabilecek genel tedbirler belirlenerek uygulanması koordine edilecektir.

Ulusal Bilgi Sistemleri Tehdit Gözetleme Sistemi Kurma Projesi kapsamında ilgili teknolojiler incelenmiş, geliştirilebilirlik ve maliyet etkinlik sebepleri ile açık kaynak kodlu tespit sistemlerinin kullanılması kararı alınmıştır. Sistemin tasarımı yapılmış, test laboratuarı ortamında örnek bir sistem kurulmuş ve değerlendirme çalışmaları yapılmıştır. Söz konusu sistemin gerçek ortamda kurulması planlanmıştır. Gerçek ortam çalışmalarının tamamlanmasını takiben, pilot seçilecek kurumlar sisteme dahil edilecektir.

2.3 Bilgisayar Olayları Müdahale Koordinasyon Merkezi Kurma Projesi

Bilgisayar güvenlik olaylarına müdahale edebilmek, günümüzde bilgi sistemlerini kullanan kurumlar için önemli hale gelmiştir. Güvenlik ile ilgili tehditler sadece sayısal olarak artmamış, aynı zamanda daha fazla zarar verici ve sistemleri daha uzun süreli kesintiye uğratıcı olmuştur. Güvenlikle ilgili olayların çeşidi de her geçen gün artmaktadır.

Korunma mekanizmaları ve güvenlik önlemlerinin alınması, güvenlik olaylarının sayısını azaltabilir; fakat sistemlerde güvenlik açıklıklarının bulunması ve bu açıklıkların güvenlik olaylarına sebep olması daima olasıdır. Her kurum ve kuruluş, ne kadar

güvenli sistemlere sahip olurlarsa olsunlar bilgi güvenliği olayı yaşama riski ile karşı karşıyadır. Bilgi güvenliği ile ilgili bir olay yaşamamak için önceden gerekli tedbirlerin alınması yanında bir olay olduğunda söz konusu olayın tespit edilmesi ve olayın verebileceği zararın en aza indirgenmesi amacıyla gerekli çalışmaların gerçekleştirilmesi de çok önemlidir.

Bilgi güvenliği olaylarına hazırlık, kurum organizasyonu içerisinde olaylara müdahale edecek bir ekibin oluşturulması veya hâlihazırda bulunan bir ekibe olay müdahale görevi verilmesi ile başlamaktadır. Olayın tespit edilmesi, olaya müdahale edilmesi, olayın yaşandığı sistemin minimum zararla eski haline dönmesi ile ilgili politika ve prosedürlerin oluşturulması ve uygulanması gerekmektedir. Olay müdahale ekibinin gerekli teknik yeterliliğe sahip olması bilgisayar olaylarına müdahalenin başarıya ulaşması için önemli koşullardan birisidir. Dolayısıyla bir kurumda olay müdahale süreci oluşturmak için yönetsel bir yapı kurmak ve yönetsel yapı içerisindeki personelin teknik yeterliliğe sahip olması olay müdahale sürecinin temelini oluşturmaktadır. Çoğunlukla bu tür süreçlerin oluşturulması aşamasında, danışmanlık desteğine ihtiyaç duyulabilmektedir.

Bilgisayar güvenlik olayları çoğunlukla birden çok kurumu etkilemektedir. Bu nedenle güvenlik olayının etkisinin en aza indirilmesi için birden çok kurumun yardımına ihtiyaç duyulabilmektedir. İlgili kurumların bir olay anında koordineli ve etkin olarak çalışması gereklidir. Yurt dışı kaynaklı güvenlik olaylarının önlenmesi amacıyla diğer ülkelerle de koordineli çalışmaya ihtiyaç olabilmektedir. Gerekli koordinasyon ülkelerin Bilgisayar Olaylarına Müdahale Koordinasyon Merkezleri (Computer Emergency Response Team-Coordination Centre) tarafından gerçekleştirilmektedir [7, 8].

Ulusal Bilgi Sistemleri Güvenlik Programı kapsamında TÜBİTAK-UEKAE bünyesinde Bilgisayar Olaylarına Müdahale Koordinasyon Merkezi kurulmuştur. Bu merkez hem bilgisayar olay müdahale ekibi kurma konusunda kamu kurumlarına danışmanlık vermekte, hem de güvenlik olayları ile ilgili koordinasyon görevini yürütmektedir. Merkez, halihazırda Başbakanlık, Adalet Bakanlığı, Sayıştay Başkanlığı, Maliye-Muhasebat Genel Müdürlüğü ve Sermaye Piyasası Kurulu'na bilgisayar olay müdahale ekibi kurma danışmanlığı vermektedir. Hazine Müsteşarlığı, Merkez Bankası, Dış Ticaret Müsteşarlığı ve Tapu ve Kadastro Genel Müdürlüğü ile de aynı tür çalışmaların planlaması yapılmıştır. Mart 2008 tarihi itibari ile söz konusu kurumlarla ilgili çalışmalar başlayacaktır. Merkez, uluslararası tanınırlığını da sağlamıştır ve yurt içi-yurt dışı olay ihbarlarını kabul ederek gerekli koordinasyon çalışmalarını sürdürmektedir.

TÜBİTAK-Ulusal Akademik Ağ ve Bilgi Merkezi bünyesinde akademik kuruluşlarına hizmet veren Ulak-Net ağı için Ulak-CSIRT adıyla bir güvenlik birimi kurulmuştur [9]. Bu birim, Ulak-Net'e yapılabilecek güvenlik ihlallerini önleme, ihlalin kaynağını tespit etme aynı şekilde Ulak-Net'ten yapılabilecek saldırıları önleme hizmetleri vermektedir.

2.4 Bilgi Sistemleri Güvenliği Dokümantasyon Projesi

Bilgi sistem unsurlarını oluşturan işletim sistemleri, uygulamalar, ağ cihazları, donanımlar vs zaman ilerledikçe çeşitlenmektedir. Bilgi sistem unsurlarının güvenlik açısından en zayıf halkası aslında sistemin çoğu zaman bütününün güvenlik seviyesini belirler. Sistem güvenliğinin sağlanması, tüm bu unsurların yeterince güvenliğinin sağlanmasına bağlıdır. Çoğu kurum, sınırlı sistem işletmeni veya yöneticisi ile birçok sistemi yönetmek zorunda kalmaktadır. Bu kısıtlı sayıdaki teknik personelin bilgi sistem unsurlarının tamamının problemsiz işletmek adına yeterli bilgi birikimi ya da imkânı olamamaktadır. Dolayısıyla unsurların güvenliği ile ilgili teknik bilgi edinme ihtiyacı en üst düzeydedir. Ayrıca, sistem güvenliği ile ilgili Türkçe doküman bulmak da hayli zordur. Ülkemizde yabancı kaynakları yeterli düzeyde anlayabilecek yabancı dil bilgi seviyesine sahip teknik personel sayısı da çok fazla değildir. Bu durum bilgi sistem güvenliği alanında Türkçe doküman ihtiyacını had safhaya ulaştırmaktadır.

Bilgi sistem güvenliğinin sağlanması için etkin bir bilgi güvenliği yönetim sistemi kurulması gerekmektedir. Söz konusu konuda da önemli ölçüde Türkçe kaynak dokümana ihtiyaç vardır. Örneğin bir kurumun nasıl bilgi güvenliği politikası dokümanı yazması gerektiği, iş sürekliliğini nasıl sağlaması gerektiği ile ilgili somut örneklerin de yer aldığı dokümanlara ihtiyaç bulunmaktadır.

Diğer ülkelerde bazı kurumlar, bilgi sistem unsurlarının güvenliğinin sağlanması ve bilgi güvenliği yönetim sisteminin çeşitli konularında rehberlik edecek dokümanlar hazırlamaktadır. ABD'deki NIST (National Institute of Standards and Technology) [10] ve NSA (National Security Agency) [11] bu kurumlara örnektir.

Bilgi sistemleri güvenliği dokümantasyon projesi, ülkemizin bilgi sistem güvenliği ile ilgili bilgi birikimini artıracak dokümanların oluşturulmasını hedeflemektedir. Bu proje iki alt kategoride ele

alınmıştır. Birinci kategori bilgi sistem güvenliği teknik dokümanlarıdır diğer kategori ise bilgi güvenliği yönetim sistemi ile ilgili konuları ele alan dokümanlardan oluşmaktadır. Şu ana kadar belirli bir sayıda doküman hazırlanmış, bazılarının da hazırlanma çalışmaları devam etmektedir. Birinci kategori için hazırlanması tamamlanan dokümanların bazıları şunlardır:
"Zararlı Yazılımlara Karşı Korunma Kılavuzu", "Kablosuz Ağ Güvenliği Kılavuzu", "Yönlendirici Güvenliği Kılavuzu", "VPN Güvenliği Kılavuzu" ve "Web Uygulama Güvenliği Kılavuzu".
İkinci kategori kapsamında ise "Bilgi Güvenliği Risk Yönetim Süreci Oluşturma Rehberi", "Erişim Kontrol Politikası Oluşturma Rehberi" ve "Bilgi Güvenliği Bilinçlendirme Süreci Oluşturma Rehberi" hazırlanması tamamlanan dokümanlara örneklerdir. Tamamlanan dokümanlar, Bölüm 2.5'de hakkında daha detaylı olarak bilgi verilen "Ulusal Bilgi Güvenliği Kapısı"nda yayınlanacaktır.

Hazırlanan dokümanlar, teknoloji gelişmeleri, yeni ihtiyaçların ortaya çıkması gibi sebeplerle zamanla güncellenecektir.

2.5 Ulusal Bilgi Güvenliği Kapısı Projesi

Ulusal Bilgi Sistemleri Güvenlik Programı'nın en önemli unsurlarından birisi de hazırlanma çalışmaları devam eden ve ürün olarak bir web kapısı (portalı)'nın çıkacağı Ulusal Bilgi Güvenliği Kapısı Projesidir. Web kapısının önemli bir kısmı, tüm ülkemize hizmet verecektir. Belirli bir kısmı ise sadece kamu kurumlarının erişimine açık olacaktır. Kapının ana hedefi ülkemiz için bir bilgi birikimi havuzu oluşturmak ve bunu sunmaktır. Bilgi birikimine katkının sadece TÜBİTAK-UEKAE tarafından yapılması planlanmamaktadır. Ülkemizde bilgi güvenliği alanında bilgi sahibi her türlü kurum veya kişinin katkıda bulunmasına imkân sağlanacaktır. Kişilerin, bilgi güvenliği konularında oluşturduğu rehber doküman veya makale oluşturulacak değerlendirme komitesinin gözden geçirmesini takiben web kapısında yayınlanacaktır.

Kapıda, bilgi sistemleri güvenliği ile dokümanlar yayınlanacaktır (Bkz: Bölüm 2.4). Ayrıca, bilgi sistem güvenlik açıklıkları ile ilgili güncel uyarılar ve bilgi güvenliği ile ilgili ülkemizde yapılacak etkinlik, toplantı, sempozyum vs gibi organizasyonların duyuruları yapılacaktır.

Bilgi güvenliğinin belirli konuları hakkında, kamu kurumlarının personelinin üye olabileceği e-posta listeleri oluşturulacaktır. Bu listelerde ilgili konular hakkında bilgi alışverişi yapılması planlanmaktadır.

Web kapısının teknik altyapısı hazırlanmıştır. İçerik belirleme çalışmaları devam etmektedir. Nisan 2008 tarihinden itibaren başlayacak test yayınının ardından kısa bir süre sonra tamamen hizmete girecektir.

2.6 Bilgi Sistemleri Güvenlik Eğitimleri

Kamu kurum ve kuruluşlarında çalışan bilgi sistem uzmanlarının bilgi sistem güvenliğinin değişik alanları ile ilgili bilgi eksikliğini gidermek amacıyla program kapsamında eğitimler düzenlenmektedir. Bu eğitimler, 20 kişilik laboratuar ortamına sahip sınıflarda uygulamalı olarak gerçekleştirilmektedir. Eğitimlere katılanlar, öğrendikleri konuların pratiklerini sınıfta gerçekleştirmektedirler.

Bilgi sistem güvenliği, 13 farklı eğitim alanında ele alınmaktadır. Her bir eğitim iki ile altı gün arasında değişen sürelere sahiptir. "Linux/Unix Güvenliği", "Microsoft Sistemler Güvenliği", "Veritabanı Güvenliği", "Web Uygulamaları Güvenliği", "Kablosuz Ağ Güvenliği", "Bilgi Güvenliği Yönetim Sistemi", "İş Sürekliliği/Felaket Kurtarım" verilen eğitimlere örneklerdir. Tüm eğitimler yaklaşık olarak 40 gün sürmektedir. Şu ana kadar eğitimlerin her birisi program kapsamında üçer kez verilmiştir. Yaklaşık olarak 100 kamu kurum personeli eğitimlere katılmıştır.

SONUÇLAR

Ulusal Bilgi Sistemleri Güvenlik Programı, ülkemizdeki bilgi güvenliği ile ilgili bilgi eksikliğini gidermek adına önemli bir işlevi yerine getirmektedir. Program kapsamında kurulacak ulusal bilgisayar olaylarına müdahale merkezi ve ulusal bilgi sistemleri tehdit gözetleme sistemi ülkemiz için önemli katkılar sağlayacaktır. Bu program özellikle bilgi toplumu olma hedefine ulaşmaya çabalayan ülkemizin önünde en büyük engellerden birisi olarak sayılabilecek bilgi güvenliği problemlerini azaltma konusunda çok büyük katkı sağlayacaktır.

Ülkemizin bilgi güvenliği ile ilgili eğitim, bilgilendirme, araştırma ihtiyacı sürekli olacaktır. İki senelik bir program ihtiyacı gidermek adına önemli bir altyapıyı oluşturacaktır. Fakat söz konusu ihtiyacın sürekliliği göz önüne alınırsa Ulusal Bilgi Sistemleri Güvenlik Programı'nın da bu paralelde sürekliliğinin sağlanması çok önemlidir.

KAYNAKLAR

[1] Bilgi Toplumu Stratejisi Eylem Planı (2006-2010), Temmuz 2006, http://www.bilgitoplumu.gov.tr/btstrateji/Eylem_Plani.pdf

[2] International Standard ISO/IEC 27001 2005, Information Technology – Security Techniques

– Information Security Management Systems – Requirements
[3] A. Valdes and K. Skinner, “Probabilistic alert correlation”, In Proc. of the 4th Int. Symposium on Recent Advances in Intrusion Detection (RAID 2001) pages 54-68, 2001.
[4] O. Dain and R. Cuningham, “Fusing heteregenous alert stream into scenario”, In Proc. of the 2001 ACM Workshop on Data Mining for Security Applications, pages 1-13, Nov 2001.
[5] P. Ning, Y. Chui, and D.S. Reeves, “Constructing attack scenarios through correlation of intrusion alerts”, In Proceedings of the 9th ACM Conference on Computer and Communications Security, pages 245-254, Washington, D.C., November 2002.
[6] Open Source Security Information Management, www.ossim.net
[7] United States Computer Emergency Readiness Team, US-CERT, http://www.us-cert.gov/
[8] Australian Computer Emergency Response Team, AusCERT, http://www.auscert.org.au/
[9] ULAK-CSIRT, http://csirt.ulakbim.gov.tr/
[10] Computer Security Division / Computer Security Resource Center – NIST, http://csrc.nist.gov/index.html
[11] National Security Agency – Central Security Service, http://www.nsa.gov/snac/