KAMU ALANINDA BİLGİNİN İNTERNET İLE SUNUMU VE ÖNÜNDEKİ TEHLİKELER: AMERİKAN ÖRNEĞİ

The Provision of Knowledge in Public Sector via the Internet and its Risks: USA Example

Güven ŞEKER*

Özet

Ağ (Network) iletişim sistemleri dünya çapında devletler ve iş alemi içerisinde iletişimde operasyonel kontrolde ve işbirlikçi yapıda gelişmektedir. Özellikle birincil araç olarak interneti içeren bu sistemlere güvenme artıştadır. Bu durum devletler ve onların özel teşebbüsleri için karmaşık teknikler ve siyasi görevleri içeren, tehlikeli çalışmalar devam ederken bir saldırı olsa bile, bilgi varlıklarını koruma ve garantisini sağlama görevi verir. Devletlerin kendi kritik araçları ve bilgilerini korunması ve yapılan saldırılara karşılık verebilmesi teknolojik meydan okumanın yanı sıra, yasal konularda siber dünyada birçok coğrafik ve yasal sınırlılıklar yüzünden mümkün görünmemektedir.

Bu yüzden ağdaki tehlikeleri (sistem kırıcılık, sosyal mühendislik, kuvvetli darbe, vb.) bilerek, devletin bilgi sistemi ile ilgili hukuk ve diğer alanlarda bilginin vatandaşlara bilinçli sunumuna yönelik çalışmalar yapılmalıdır.

Anahtar Kelimeler: Bilgi, Bilgi Sistemi, Ağ, Hukuk, Bilişim Suçu.

Abstract

Networked information systems are being rapidly adopted by governments and businesses worldwide to improve communications, operational control, and – ultimately – competitiveness. Reliance on these systems, especially where the Internet exists as the primary infrastructure, is likely to increase. It gives a complex technical and political task for nations and their commercial enterprises to protect information assets and ensure that critical operations continue even if attacked. Governments to give an answer to attacks for safeguarding information and critical infrastructures. Besides the technological challenges, the legal issues involved as they cross multiple geographical and legal boundaries.

For that as we know Networks risks (hacking, social engineering, whacking, etc), we have to make special work goverment knowledge system in law and other field about present knowledge consciously to citizen.

Key Words: Information, Knowledge System, Network, Law, Cyber Crime.

* Komiser, İzmir Emn. Md.lüğü, www.guvenseker.sayfasi.com, gseker@izmirpolis.gov.tr, gdseker@hotmail.com,

Giriş

Yüzyılımız artık internet ve bilgi üzerine yoğunlaşmış, insanların çalışma alanlarında sundukları yenilikler ile kapılarını yeni elektronik dünyaya açmaktadır. Bu durum kamu sektörünün çağdaş dünyada sürdürülebilirliği için bilgi ve bilginin sunumu noktasında araçlarını yeniden gözden geçirip bu yeni oluşuma ayak uydurma zorunluluğunu ortaya çıkarmaktadır. Çalışmamız bu alanda öncü ve en ileri sistemlere sahip Amerikan örneğini literatür taramasına dayalı olarak ortaya koymayı ve bir model sunmayı amaçlamaktadır.

Bilgi ve İnternet

Network (ağ) iletişim sistemleri, dolayısı ile internet dünya çapında devletler ve iş dünyası içinde, iletişimde operasyonel kontrolde ve işbirlikçi bir yapıda gelişmektedir. Ülkeler için önemli bilgilerin korunması can alıcı hayati bir işlemdir. Dünya pazarının büyümesi ve ülkeler arası ilişkilerin artması bu önemi arttırmaktadır (CERT Coordination Center, 1999).

İkinci olarak Amerika başta olmak üzere tüm dünyada internet ile hızlı ve coğrafik durumunuza bakılmaksızın sanki aynı odadaymışsınız gibi, kurumların içine girilebilir duruma gelmiştir (Widdison, 1997:144). 11 Eylül'den sonra içeriden gelen terör eylemi, Amerikan halkında, terörle mücadelede **e-devlet**'in (elektronik devlet uygulamaları) kritik bir rol alacağına olan inancını artmıştır. Devlet daireleri, federal devlet ile eyaletler arasındaki iletişimin ve koordinasyonun artması ile e-devlet teröristlerin yakalanmasında devlete daha fazla güç verecektir gibi bir kanı oluşmuştur. Tabi ki bu noktada Amerikan halkının çoğu kişisel bilgiler ve kimlikler ile ilgili bilgilerin devlet internet sistemlerinden çalınabileceği endişesini de taşımaktadırlar. Nitekim bu konu ile ilgili yapılan araştırmada; e-devletin başlangıcı değil de, e-devletin nereye kadar gideceği ile ilgili olan bilgiler ortaya çıkmış ve bunlar aşağıda belirtilmiştir (Hart, 2002: 1-2).

1. Halk e-devletin terörizm ile mücadelede yardımcı olacağına inanmaktadır. Halkın yüzde yetmişi federal ve yerel devlet kuruluşlarına koordinasyon ve eylem açısından e-devletin yardımcı olacağını düşünmektedir. Yine halkın yüzde doksanı e-devlet sisteminde bilginin değişimi ile devlet tarafından teröristlerin ve suçluların yakalanmasının kolaylaşacağına inanmaktadır. Yüzde elli ikisi ise herhangi bir büroya ya da hizmete bizzat gitmektense, on-line devlet servislerini tercih edeceklerini belirtmişlerdir. Amerikalıların yarıdan fazlası (yüzde elliyedisi) terörizme karşı mücadelede on-line gizliliklerini feda etmeye hazır olduğunu belirtmektedir.
2. Halk, e-devletin vatandaş devlet arasında kritik bir rol oynadığını belirtmektedir. Nitekim Amerika' da istatistiksel olarak internet kullanımı aynı düzeyde iken e-devlet uygulaması artmaktadır.

3. Halk devlet sistemlerine de izinsiz girme ve saldırılardan endişe duymaktadır. Halkın yüzde altmış dördü, sistem kırıcıların (hackers) devlet sistemine gireceğine dair bir endişe taşımaktadır.
4. Amerikan halkı e-devlet ile devletin vatandaşı kolaylıkla dinlediğini ve vatandaşa hesap verdiğini belirtmektedir. 2000 yılında yüzde ellidört olan bu görüş, 2001 yılında yüzde altmış iki olmuştur. E-devlet ile vatandaşlar yüzde altmış altı oranında seslerini ve fikirlerini kongreye ulaştırabildiklerini, ödedikleri vergilerin böylelikle takipçisi olabildiklerini belirtmektedirler (Hart, 2002:2).

Artık on–line olarak sistemlerin kurulması ve insanların bu doğrultuda hizmet yapısını devletten ister duruma geçirmesi devletlerin bu noktada daha çok çaba sarf etmesini gerektirmektedir. Sistemlere yönelik internette saldırılar yapılmakta ve bunlara karşı savunma çok zor olmakta, saldırganın kimliği belirlenememektedir. Dünyadaki bilgi teknolojisinin ve bilgisayar güvenliğinin genel durumunun gelişebilmesi için uluslar arası işbirliği gerekmektedir. Çünkü paylaşılan riskler, paylaşılan sorumlulukları beraberinde getirmektedir. Bu sorumluluğu taşıyan ulusların ortak çabaları ile bilginin ve teknolojinin depolanıp transfer edilebilmesi için uygun bir ortam meydana getirilebilir.

Yeni yüzyılda organizasyonlar bilgi yönetiminde insan zihnindeki bilgide hiçbir kayba uğramadan daha iyi örgütsel mekanizmaya ulaşmak için çaba sarf etmektedir. Alan Weber "Yeni ekonominin teknoloji içerisinde olmadığı, mikroyongaların ya da global telekomünikasyon ağında (network) bile olmadığını bunun insan zihninde olduğunu" belirtmiştir (Akt., Perton, 2000a). Bilgi yönetimi yaklaşımının adaptasyonunda üç büyük kuvvet etkilidir; globalleşme, rekabet ve yeni teknolojiler. Bu temel teorinin arkasındaki yapı elbette ki bilgidir. Bilgi yönetiminin temel amacı da; entelektüel kapasitenin etkin ve verimli olarak yapılandırılmasıdır. Bu noktada da bilgisayarlar bilginin düzenlenmesi, sınıflandırılması kolay erişilir olmasını sağlamaktadır. Bilgisayarın kolay erişilir olması ağ (network) ile birbirine ulaşması ve bunun maliyetinin düşük olması, bilginin daha kolay paylaşımına yol açmıştır. E- posta (e-mail), grup haberleşmeleri, kapalı ağlar (İntranet) ve internet, insanlara teknolojik araçları sunan bilgiyi mesafe sınırı tanımadan paylaştıran araçlardır. Şunu unutmamak lazımdır ki gizli kalmış bilgileri ileten bu yapılar, yeni teknolojiler ile bilgi değişimi için oluşturulmuş iletişim sistemlerdir (Akt., Perton, 2000a). Organizasyon değişimi ile gelen kültürel değişimde, bilgiyi sadece istifleyen değil, onun değerini bilerek paylaşan ve değer kazandıran organizasyonlar bilgi yönetiminde kritik başarıyı yakalayacaktır. Bilgi gerçekte eğer faydalı olamıyorsa hiçbir anlam taşımaz. Bu vizyona sahip kurum ve kuruluşlar bilgiyi güç olarak kullanabileceklerdir.

Devletlerin kendi ulusal güvenliği ve varlığını ilgilendiren araçların, bilgilerinin korunması ve yapılan saldırılara karşılık verebilmesi siber dünyada coğrafik ve yasal sınırlılıklar gibi birçok nedenden dolayı zor görünmektedir.

Örneğin Amerikan, 63 Nolu Başkanlık Emir Direktifinde (kritik altyapı ile ilgili beyaz kağıt[1]) "Hassas durumlarda eğer gerekiyorsa esnek davranarak devlet sisteminde oluşturulacak evrimsel yaklaşım ile resmi ve özel sektör arası işbirliği ile yerel ve ulusal güvenliğin korunabileceği… Federal Hükümetin global problemlerin çözümünde uluslar arası işbirliği için cesaretlendirmesi gerektiği" belirtilmektedir.

Polisler açısından ve diğer birçok açıdan internet ve siber dünyanın yeni bir karakol alanı olduğu mutlaktır. Yargılamanın milli ve politik sınırları olduğu gibi, fiziksel dünyada dijital bilgi altyapısının merkezi bir noktası da yoktur. Bu tip saldırılara sadece teknolojik açıdan cevap verme zor olduğu gibi, diğer kabul edilmiş metotlar ile pratikte polisin cevap vermesi zor olmaktadır ve bu durum polisi etkisizleştirebilecektir.

Uluslar arası bilişim suçu olayları ile ve bu olaylar ile ilgili koordinasyon için gerekli olan temel tekniğin ilk basamağı; kurbanın bulunduğu durumu ayrıntılı açıklayan rapor hazırlaması, o durumda uyarıların ve gösterilen hedefin tespit edilmeye çalışılarak toplumun bu konuda bilgilendirilmesi, teknik tehlike durumlarının belirlenmesi, açıkların önceden bilinmesi, siber saldırganların iz ve delillerinin takip edilmesi önemli noktalardır. Bu konu aşağıda detaylandırılacaktır.

Global altyapıda bir olay olduğunda bu olayı ele alabilmek için, global koordinasyon merkezi, uluslar arası zaman alanı koordinasyon merkezi, ulusal koordinasyon merkezleri gibi oluşumlara ihtiyaç bulunmaktadır (CERT Coordination Center, 1999). Günümüzde böyle örgütlenmelerin yapılabilmesi, bu örgütün mali açıdan desteklenmesi, kontrol ve yönetiminin kimlerde olacağı, organizasyonun yapısı, kültürel, coğrafik, engeller ortaya çıkabilecektir. Fakat yine de konunun önemi ortadadır. Bu durumda yapılabilecek en iyi şey bu konu ile ilgili ulusal örgütlerin bir koordinasyon içinde özel sektörün de konunun içine çekilmesi ile oluşturulacak birliktelikler ile mücadele etmektir (Perton, 2000:1-13).

İnternet ve Global Çalışma Alanı Yaklaşımı

İnternet ve bilgi güvenliği profesyonellerinin belirttiği ve yedi yıllık araştırmaların gösterdiği sonuçlara bakıldığında; teknolojinin sadece bilgisayar saldırıları ile mücadele etmek için yeterli olmadığı bunun yanında özel sektör ve kamu sektörü arasında bir ortaklığa ihtiyaç bulunduğu anlaşılmaktadır. Ayrıca geleneksel yaklaşımı bırakıp profesyonel bir yapı ortaya koymak gerekir. Örneğin; bir örgütün içinden gelen tehdit, dışarıdan gelen çoğunlukla bir oyun olarak oluşan tehditten daha ciddi ve önemlidir.

1 White Paper (Beyaz Kağıt): Bir kurumun durumunu, felsefesini, hizmetlerinde, ürünlerinde kullandığı yöntemleri, teknolojileri açıklayan makale türü düz yazılara verilen ad.

FBI'ın daha önceki operasyonlarını yöneten yönetici yardımcısı (EAD Executive Assistant Director) Bruce J. Gebhardt yılda bir kere yayınlanan FBI raporunda "devlet ve özel sektör arasında bilişim - teröristlerine yönelik öncelikli milli altyapı sağlayan yönetme ve işlem birimlerinin güvenliğini sağlamada ortaklığa ihtiyaç bulunmaktadır. Şimdi daha öncesine oranla devlet ve özel sektör, bilişim güvenliği kavramında milli hayati altyapı ile ilgili, bilişim teröristlerine karşı bilgiyi paylaşarak ve birlikte çalışarak koruma faaliyeti içine girmelidir" görüşlerini ortaya koymaktadır.

Nitekim Amerikan sistemi bu birlikte çalışma gerekliliğini çok önceden görerek gerekli kurumsal yapılanmaları oluşturmuştur. Bilgisayar Güvenlik Enstitüsü (CIS) 1974 yılında bilişim güvenliği profesyonelleri tarafından San Fransisko'da kurulmuş bulunan danışma birimidir. Dünya çapında binlerce üyesi olan değişik, geniş çaplı bilgi veren ve kanun adamlarına eğitim veren, kamu ve özel örgütlere bilginin korunması ile ilgili olarak yardım eden bir örgüttür. FBI'da suç olarak ekonomik altyapı sistemlerine ve büyük bilgi sistemlerine zarar verebilecek şahıs veya gruplara yönelik olarak FBI'ın merkezinde Milli Altyapı Koruma Merkezini (NIPC) ve Bölgesel Bilgisayar Sistemlerine Yönelik Saldırıyı Önleme Ekibi adında Amerika'nın tüm bölgelerinden seçilmiş memurlardan yapılanmış teşkilat oluşturulmuştur. NIPC Federal Devlet Daireleri ve Özel Endüstri ile birlikte milli altyapıya yönelik saldırılar ile mücadele etmek ve devletin yönetim mekanizmasının bu alanda etkinliğini sağlama amaçlı olarak düzenlenmiştir[2]. Bölgesel Bilgisayar Sistemlerine Yönelik Saldırıyı Önleme Ekibi, Bilgisayar Dolandırıcılığı ve Kötüye Kullanma Kanunu'na göre korsan bilgisayar yazılımı ve diğer suç vasıtaları ile halka açık ağ (network) sistemlerine izinsiz girenlere, özel alana müdahale edenlere, büyük bilgisayar ağlarına (network) izinsiz girenlere, endüstiriyel casusluk yapanlara yönelik soruşturmaları yapmaktadır (Computer Security Institute, 2002).

Bilgi ve Bilgiye Erişim Alanında Amerika Örneği

Amerika' da 04.09.1981 yılında Reno'nun Bilgi Özgürlüğü Kanunu (Freedom Of Information Act) ile ilgili yayınladığı genelgede sağlam kanuni dayanak bulunduğunda, bilginin vatandaşlar tarafından istenildiğinde verilmesi ile ilgili direktifi kurumları cesaretlendirmiştir. Bu değişimin etkisi ile federal servislerde halka açık bilginin toplamı bir anda artmıştır. Bu yeni Bilgi Özgürlüğü Kanunu (FOIA) standardı ile yaklaşık 800 milyon devlet dokümanı hazırlanmıştır (Gordon-Murnane, 2002:51).

Amerikan devlet bilgi politikasının ve bilgiye erişim sisteminin değişiminde birkaç kanuni yapılanma etkili olmuştur. Federal devletin yaptığı işlerde fazla kağıt harcanmasını engellemek için yapılan amacı baştan sona kadar yukarıdaki di-

2 Bu altyapı telekominikasyon, enerji, ulaşım, bankacılık, finans, ilkyardım servisleri ve işletimsel devlet kuruluşlarıdır.

rektife hizmet eden Kağıtla Yapılan İşlerin Azaltılması Kanunu (Paperwork Reduction Act of 1995) hazırlanmıştır. Böylelikle federal anlamda milli bilgi altyapısı (National Information Infrastructure) gelişmiştir. Federal servisler bu kanun ile kağıtsız ve mikro filmsiz elektronik sunum avantajı ile tanışmışlardır. Bu kanun iki yönlü bir avantaj sağlamıştır; birincisi kağıt ve yazım maliyetinin ortadan kalkması; ikincisi; elektronik ortamda her türlü sunulabilen bilgiye erişme. Bu kanun (Paperwork Reduction Act of 1995) bizim bu günkü e-devlet diye adlandırdığımız yapıyı ortaya çıkarmıştır. Günümüzde artık e-devlet kavramı[3] Amerikan halkı için vazgeçilmezliği ifade etmektedir (Hart, 2002:1-2).

Devlet bilgilerine genişçe erişimi sağlayan bir diğer kanun ise Kanuni Bölüm Ayırmadır (Legislative Branch Appropriations Act, 1996). Bu kanun ile Devlet Basım Dairesi (GPO) diğer dairelere oranla en fazla şekilde resmi dokümanları elektronik formata dönüştürmüştür. Seksen müracaat formu altında 2200 veri tabanı (özellikle kongre kayıtları federal kayıtlar ve federal kanunlar) 2001 Kasım itibari ile 130.000 başlık altında erişime sunulmuştur. Ayrıca Devlet Basım Dairesi altında sunulan 94.000 başlık altındaki köprü ile diğer federal servislere erişim bulunmaktadır. Her ay Devlet Basım Dairesi tarafından otuz bir milyon doküman hazırlanmaktadır ve 2001 yılında hemen hemen üçyüz elli beş milyondan fazla doküman hazırlanmıştır.

Amerikan Federal Elektronik Bilgi Özgürlüğü Kanunu (E-FOIA, 1996) kendinden önceki Bilgi Özgürlüğü Kanununda bulunmayan elektronik dokümanlar ile ilgili olarak, devletin kamuya bilgi sunma politikasını ortaya koymuştur. Bu kanunun önemini Genel Muhasebe Dairesinin (General Accounting Office) 2001 Mart ayında sunduğu "Bilgi Yönetimi: Elektronik Bilgi Özgürlüğü Kanunu Düzenlemesi (1996 yılından beri yürürlüktedir)" başlıklı raporunda görebiliriz. Raporda "Yirmi beş servis işleminde yaklaşık 1.9 milyon Elektronik Bilgi Özgürlüğü Kanunu'ndan kaynaklanan müracaat olduğu, önceden var olan kayıtların yüzde seksen ikisinin doldurulduğunu; Yirmi üç servis raporunda 1.6 milyon müracaatın ortalama yirmi gün veya daha az günde sonuçlandırıldığını 140.000 işlemin ortalama yirmi günden fazla bir zamanda sonuçlandığını" belirtmektedir. Vatandaşlara e-devletin devlet sorumluluğunu geliştirip geliştirmediği ile ilgili fikirleri sorulduğunda; yüzde yirmi dokuzu önemli konularda fikirlerini sunabilmek için devlet memurları ile hızlı ve kolay iletişime geçilebildiği, yüzde yirmi biri ihtiyaç duydukları ya da problem olan konularda devlet kurumlarına erişebildiklerini, yüzde yirmi biri halka devlet politikaları ve kararları ile ilgili fazlası ile bilgi verdiklerini belirtmiştir (Gordon-Murnane, 2002: 53); görülüyor ki Amerika'da vatandaşlar e-devletin devleti daha işler hale getirdiğine inanmaktadır.

11 Eylül 2001 tarihinden beri Bilgi Özgürlüğü Kanunu'nun uygulamasında bilgilerin özelliği başlıklı yönerge yayınlanarak federal dairelerce sunulan bilginin yeniden sınıflandırılması gerekliliği belirtilmiştir. Böylece teröristler tarafın-

3 Amerika' da Yönetimde Mükemmeli Yakalama Komisyonu Şubat 2002, raporuna göre yapılan değerlendirme (Aktaran Gordon-Murnane, 2002: 52).

dan potansiyel olarak kullanılabilecek "hassas ve sınıflandırılmamış" bilgiler, federal dairelerce federal internet sitelerinden kaldırılmıştır. Eğer bilginin sunulmasında federal açıdan bir zarar doğacaksa bilginin sunulmaması kararlaştırılmıştır.

Devletin kullandığı bilgiler ile ilgili olarak yapılan çalışmalarda bilimsel bilgilerin kullanılması, yüksek kalite standartlarına erişmenin gerekliliği belirtilmektedir. Bu konu ile ilgili olarak yapılan çalışmalarda kamuya açık bilgilerin istatistiksel açıdan risklerinin hesaplanması gerekmektedir. Bu konuda Dr. Graham[4] "Bütün devlet daireleri -her türlü görevde- kullandıkları ve belirttikleri bilgileri sadece kalitesi ile değil, aynı zamanda kendi analizlerinin kalitesi ile sunmaktadırlar. Uzun sürede bu durumda devlet problemlere odaklanacaktır. Oysa bilim problemlerden uzaklaşarak daha ciddi yaklaşımda bulunmayı önermektedir" şeklinde bir değerlendirme ortaya koymuştur (Gordon-Murnane, 2002: 55). Bu yaklaşım ışığında kendi ülkemize dönük bir değerlendirme yaptığımızda; bizler de sadece bilgileri kendi anlayış düzeyimizde ortaya koymaktayız, subjektif değerlendirmeler toplumsal veya kişisel problemlere, ne kadar çözüm sunabilir? Tabi bu noktada bilgi sunumu ile ilgili atlanılmaması gereken bir nokta bulunmaktadır: "risk değerlendirmesi". Unutulmamalıdır ki; risk değerlendirilmesi bilimsel yaklaşım ve profesyonel çalışma ile yapılabilecek bir iştir.

11 Eylül saldırısından sonra Amerikan Federal Daireleri halka açık bilgileri tekrar gözden geçirmişler ve bunun sonucunda, Nükleer Düzenleme Komisyonu (NRC), "Biz halk sağlığını ve güvenliğini sağlamak ve korumak amacı ile internet sitemizden bu konudaki tüm araçları sunmaktaydık, 11 Eylül saldırısından sonra sunduğumuz bilgiler artık sınırlı olacaktır. Sizin şu yaşadığımız zor anlarda anlayışınıza sığınarak bu kararı almış bulunuyoruz" şeklinde internet sitelerinden açıklama yapmıştır. Daha sonra internet sitelerini tekrar gözden geçirilmiş ve seçilmiş bilgilerden oluşturulmuş hali ile 11 Ekim'de kullanıma açmışlardır. Enerji Dairesi, Çevre Koruma Dairesi, Boru Hattı Güvenliği Dairesi, Coğrafik Bilgi Servisleri gibi federal daireler internet sitelerindeki bilgilerin çoğunu kaldırmışlardır (Gordon-Murnane, 2002:58-59). 11 Eylül öncesi bütün bu sitelerde olan bilgilerin teröristler tarafından kullanımı tahmin edilemeyecek zararlara yol açabilecektir.

İnternet üzerinden bilgilerin bir anda kaldırılması, ihtiyaç duyulan bilgilere erişememe gibi bir sonucu da ortaya çıkartmıştır. Bu noktada Amerikan devletinin bilgi politikası ile ilgili halka aydınlatıcı bilgi verme gerekliliği bulunmaktadır (Gordon Murnane, 2002:60). Sonuçta genel politikası belli olmayan bilgi sunumu bir olay ile (11 Eylül saldırısı) anında değişmiş ve bir gün önce halka açık olan internet sitesi, ertesi gün şifreli kullanıma açılmıştır. Genel bir değerlendirme açısı ile yaklaşıldığında, Amerikan sisteminde belki de baştan öngörülmesi gereken bilgi sistemi ve bilginin sunumu konularında daha önceden oluşturulan sistemin iflası ile güven bunalımı yaşandığı görülecektir. Ülkemiz açısından ko-

4 Dr. Graham Amerikan Federal Bilgi Ve Düzenleme İşleri Bütçe ve Yönetim Dairesinin Yöneticisidir. Kendisi Harward' da Risk Yönetimi konusunda uzmanlık yapmıştır.

nu değerlendirildiğinde; bugün daha yeni yeni tartışılmaya başlayan e-devlet çalışmalarında bilgi sistemimiz ile ilgili köklü ve her bakış açısının süzgecinden geçmiş yaklaşımlar geliştirilmelidir. Yapılacak çalışmalar adım adım ve sabırla yürütülmelidir. Nitekim bu konu ile ilgili olarak Patrice McDermott "11 Eylül 2001 tarihinden sonra "açık devletin tekrar sürdürülmesi" başlığı ile sunduğu tebliğinde halka açık sunumların potansiyel olarak değerlendirilmesindeki kriterleri şöyle sıralamıştır:

1. Bilgi herhangi bir yerde, on-line sunulmaya uygun mudur?
2. Sadece sizin sitenizde bulunabilecek, halka faydalı olacak şeyler midir?
3. Bilginin on-line sunumunun riskleri nelerdir? On-line sunulmamanın riskleri nelerdir?
4. Bilgiyi veri tabanına ya da girilebilen dokümanlara çevirmeden değerlendirebilmenin yolu var mıdır?
5. Sizin servisinizin internet bağlantısına gelecekte, kimlerin bağlanmasına ihtiyaç duyacaksınız?

Bu soruların internet hizmeti verecek devlet organlarınca cevaplanarak internet hizmet alanı oluşturulması, bilgi politikasının geliştirilmesi için iyi bir başlangıç noktası olacaktır" diye belirtmiştir (Gordon Murnane, 2002:60-61). Bu kriterlerin ülkemizdeki internet çalışmalarında da kullanılması sağlam tabanlı bilgi sunumu çalışmalarını gösterecektir.

İnternette Kanunsuz Şekilde Bilgiyi Elde Etmede Kullanılan Yöntemler

Amerika'da CSI ve FBI tarafından yapılan 2002 bilgisayar suçları ve güvenliği araştırmasında; ankete katılanların, yüzde doksanı (Büyük şirketler ve devlet kuruluşlarından oluşmaktadır), 2001 yılı içinde bilgisayar güvenlik açığı tespit etmiştirler, yüzde sekseni güvenlik açığından kaynaklanan mali kayıpları olduğunu kabul etmektedir, yüzde kırk dördü (223 katılımcı) mali kayıplarının belirtilmesinde sakınca görmeden kayıplarını ortaya koymuşlar ve 455,848,000 dolar mali kayıp rapor etmiştirler. Önceki yıllarda yapılan araştırmalarda olduğu gibi, oldukça önemli mali kayıplar özel bilgilerin hırsızlığından (26 katılımcının belirttiği 170,827,000 dolar) ve mali sahtekarlıklardan (25 katılımcının belirttiği 115,753,000 dolar) kaynaklanmaktadır.

Yapılan beş yıllık çalışma sürecine bakıldığında, katılımcıların çoğu (yüzde yetmiş dördü) iç sistemlerinden, yüzde otuz üçü ise internetten saldırı tespit ettiklerini belirtmişlerdir. Yüzde otuz dördü bu izinsiz girişleri yetkili makamlara bildirmiştir (1996 yılında yetkili makamlara, bilinen sadece yüzde on altılık bildirim bulunmaktadır). Katılımcılar geniş çapta saldırı ve izinsiz müdahale tespit ettiklerini belirtmişlerdir; yüzde kırkı sistem içine dışarıdan sızma tespit etmiş,

yüzde kırkı servis saldırılarının ret edilişini tespit etmiş, yüzde yetmiş sekizi çalışanlarının internet erişimini kötüye kullandığını (Örneğin; pornografik içerikli nesneler, korsan programlar indirmek veya e- mailin (e- posta) uygunsuz olarak kullanılması) tespit etmiş, yüzde seksen beşi bilgisayar virüsleri tespit etmiştir (Power, 2002:1-5).

Özellikle Amerika'da çalışanların internetten takibi bilinen bir gerçektir. Amerikan Yönetim Birliğine göre Amerika'da 2001 yılında işverenlerin yüzde yetmiş üçü çalışanlarının internet üzerindeki hareketlerini izlemektedir (Power, 2002:16).

Art niyetli sistemler (ülke veya işletmeler) veya kişiler, hedeflenen sistemlerin bulunduğu iç yapıdan yada dışarıdan bilgi elde etme konusunda, güncel teknoloji ve tekniği artık çok kolay şekilde internetten elde etmektedirler. Rekabet ortamında ticari gizlilikteki bilginin çalınması iyi niyet esaslarının ihlali ve ticari kayıp anlamına gelir. Tabi ki bu bilgilerin sadece şirketin ticari alandaki rakipleri tarafından değil de yabancı milletlerce de elde edilmesi mümkündür (Robinson, 2002).

Rusya kaynaklı banka sistemlerine yönelik saldırılardan birinde Nikolai isimli 21 yaşındaki üniversite öğrencisi bir bankayı on bin dolar dolandırmıştır. Bankaya bu dolandırma eyleminin maliyeti ikiyüz elli bin dolar olmuştur. Bunun sonunda Rusya bilgisayar dolandırıcılığı birimi Nikolai isimli şahısı internet protokol (Ip) adresinden takip ederek yakalamıştır. Nikolai şu an on beş sene hapis cezası almış biri olarak hapiste yatmaktadır (Power, 2002: 13).

Mart 2002'de Federal ajanlar Newyork elektronik suç görev gücü ile birlikte çalışarak McNeese isimli Prudential Insurance Co. isimli şirketin bilgisayar sistemine internetten girip altmış bin çalışanının kimlik ve kişisel kayıtlarını çalan ve bu bilgileri internetten satmak isteyen şahsı yakalamıştır. Ayrıca bu şahıs bunun yanında kredi kartı bilgileri ile internetten kredi kartı dolandırıcılığı suçlarına karışmıştır. Bu suçlardan dolayı McNeese tutuklanarak ceza evine gönderilmiştir (Power, 2002:14).

E-ticaret yapan birçok internet sitesi, saldırganlar tarafından daha sonradan yapacakları bilgisayar sistemlerinin geliştirilmesinde mali araç olarak nitelendirilmekte çok iyi ve hazır bir lokma olarak görülmektedir. Özellikle internet sunucularda tutulan ve basit kodlar ile hazırlanmış sistemlere yönelik (Oracle veya SQL veri tabanlı) yönetilecek SQL zehirleme saldırısı (SQL poisoning)[5] ile değerli ve internette kolaylıkla paraya çevrilebilecek bilgiler kötü niyetli kişilerce elde edilmektedir (Power, 2002:14).

Değişik konularda bilginin artık çok zor elde edilmesinden ve belli konularda çok fazla şekilde özelleşmiş olarak elde edilen teknik ve teknolojilerin değerli bil-

5 Sql zehirleme tekniği (SQL poisoning); internet sunucusuna yönelik, en sondaki sunucuda bulunan Sql veya Oracle gibi veri tabanının elde edilmesi tekniğidir. Bu teknik yardımı ile, bilginin kendi başına internet sunucuda saklanmadığı ya da internet sunucusunun basit kodlama ile yazılmış olduğu veri tabanlarından değerli bilgiler elde edilir.

giler olarak oluşması bilginin önemini arttırmıştır. Fakat son yıllarda özellikle iki faktör bilginin öneminde etkin olmaktadır:

1. Bilginin bir değere sahip olduğunun farkına varılmasındaki artış,
2. Bilginin değerini algılamaktaki artış (Power, 2002:7). Bu öneme sahip bir değere yönelik saldırılarda aynı oranda artmaktadır.

İnternette sosyal, siyasal, ekonomik, teknolojik v.s. alanlar başta olmak üzere birçok alanda ulusal hedefler yanında, değişik uluslar arası yerler de hedef alınarak bilişim suçları işlenilmektedir.

Mi2g[6] sitesinde 09 Kasım 2001 sonrası yayınlanan yazıya göre 2001 yılında meydana gelen zararlarda bir artma olmuştur. Özellikle Mayıs ayında görülen artma (3,853 site), Ağustos ayında ise en düşük seviyesini yaşamıştır (812 site). Mi2g' nin raporuna göre 2001 yılında ".com" uzantılı isim alanına yönelik bütün siteler içindeki genel yapıda (30,388 zarar gören sitede) verilen zarar yüzde otuza (8,736) çıkmıştır. İkinci en çok zarar gören siteler ise Çin devletinin ".cn" ve Tayvan devletinin ".tw" uzantılı isim alanlarıdır. Bu zararlar genel zarar içinde yüzde dokuzu (2,653) ifade etmektedir. Dünyadaki yerel, bölgesel, ulusal ve uluslar arası çatışmalar internet üzerinde işlenen suçlar ile doğru orantılı olarak değişmektedir. Nitekim; 2001 yılında ".gov" uzantılı isim alanlarındaki zarar yüzde otuz yedi, olmuş önceki yıla göre yüz seksen birden, ikiyüz kırk sekize yükselmiştir. Aynı dönemde ".mil" uzantılı isim alanlarına yönelik zarar yüzde yüz yirmi sekiz artmıştır. İsrail' in ".il" uzantılı isim alanlarına yönelik zarar 2001 yılında yüzde ikiyüz yirmi oranında (413) artmıştır. Yıl içinde Hindistan'ın ".in" uzantılı isim alanlarına yönelik zarar yüzde ikiyüz beş oranında (250) artmış, yine aynı yıl Pakistan' ın ".pk" uzantılı isim alanlarına yönelik zarar da ise yüzde üçyüz (82) artma olmuştur. İngiltere'de "gov.uk" uzantılı isim alanlarına yönelik 2000 yılında dokuz olan zarar 2001 yılında yüzde üçyüz yetmiş sekize (43) yükselmiştir (Power, 2002: 1–5). Görülüyor ki siyasi, ekonomik, teknolojik v.s. savaş artık internette meydana gelmektedir.

Ayrıca gelişmiş ülkelerin bilgisayar sistemlerine bilgi hırsızlığı için yöneltilen saldırılarda da artma olmuştur. Nitekim iki Çinli bilim adamı ve bir Amerikalı vatandaş Lucent Teknolojinin kaynak kodlarını çalmaktan dolayı hapse atılmışlardır. Bu konu ile ilgili olarak çalışan The NCIX[7] değişik metotlar ile yabancı oluşumlar ve devletlerce ekonomik casusluk için Amerikan hedeflerine yönelik saldırılar düzenlendiğini belirtmektedir. Ayrıca bu saldırılar sabırla ve her türlü bilginin toplandığı, bu bilgilere göre saldırı metodolojisinin geliştirildiği yöntemler ile yapılmaktadır diye belirtmişlerdir (Power, 2002: 7-8). Kısaca işlenilen suçlar ile ilgili istatistiksel ve boyutsal örnekler verdikten sonra kullanılan teknikleri ortaya koyma gerekliliğine inanıyoruz.

6 www.mi2g.com, isimli internet sitesi.

7 www.nicx.com isimli internet sitesi.

Ortak Casusluk

Ortak casusluk bilgiye dayalı olarak çalışan şirketlere yönelik bir tehdittir. Bu bilgiler müşteri listeleri, önem arz eden sözleşmeler, personel kayıtları, araştırma dokümanları, yeni hizmet ya da ürün ile ilgili prototip planları olabilir. Bu bilgiler bir şirket üzerinde yıkıcı etkisi olabilecek mali düşünce ve inançlar olabilecektir. Şirketten toplanılan bu bilgiler ile kredi kartı hileleri, şantaj, zorla ve farklı isim tanımlama ile menfaat temin etme gibi şirkete yönelik her türlü kötülük türünü içine almaktadır. Endüstri analistlerine göre şirketler "Big Brother" tarzında kendilerine yönelik bir izleme yapmalıdırlar, yoksa bunun sonunda birçok problem ile karşılaşılabilecektir. Dünya şirketlerinin yüzde sakseni kendi personelinin bilgilerini korumak ve rakipleri hakkında bilgi toplamak için resmi bilgi programlarına bir milyar dolar para yatırmaktadır (Cliff, 2000). Altyapıları karmaşık olan, uzak müşteri ve kullanıcıları olan, uzak ofis ve iletişimleri olan sistemlere sahip büyük şirketler sistemlerine gizli girişlere karşı daha uygun durumdadırlar. Fakat şirketler bu durum sanki hiç önemli değilmişçesine sistemlerini geliştirebilmek için para harcamayı istemezler. Şirketler sahip olmadıkları bir problem için para harcamayı sevmediklerinden, çok az şirket bu konuda personel eğitmeyi, donanım ya da yazılım yatırımı yapmayı kendi sistem ve ağlarının (network) koruma ve takibi için kaynak ayırmayı düşünür.

1999 yılında Fortune dergisinde yayınlanan araştırma sonucuna göre bin şirket, kırk beş milyar dolar değerinde ticari sırların çalınmasından dolayı kayba uğramıştır. Tabi bu konudaki gerçek rakamlara ulaşmak çok zordur, bunun bir nedeni; hiçbir şirketin ticari gizli hırsızlığın kurbanı olarak kendisini ortaya koymak istememesidir. Bankalar güvenlik açıklarını ortaya koymayı, Amerikan federal hükümetinin, uyguladığı sistem ya da güvenlik politika ve uygulamaları ile ilgili olarak sorgulamaya girmek istemezler. Küçük şirketler uğradıkları zararlar ile ilgili olarak ortaklarını korkutmama ve sistemlerinin güvensiz olduğunu düşündürmeme adına bilgi vermek istemezler (Eisenberg, 1999). Aynı durumda bizim ülkemizde de aynı tepkilerin verilebileceği açıkça görülecektir.

Ortak casusluk, süzgeççilik, sistem kırıcılık (hack) olarak iki temel kategoriye ayrılır, bunlarıda içerdekiler ve dışarıdakiler olarak adlandırabiliriz. İçeridekiler genellikle, çalışanlar, yöneticiler, Bilişim Teknolojisi (IT) çalışanları, yükleniciler (programcılar, ağ (network) giriş hakkı olanlar, bilgisayar denetçileri), mühendisler, veri tabanına, bilgisayara yada ağa (network) erişim hakkı olan kişilerdir. Sık sık yapılan istatistiklerde çalışanların yüzde seksen beşinin ortak casusluğu yaptıkları tespit edilmiştir. Şirket içindekilerin yüksek erişebilme ayrıcalığı bir trojan atı programları yardımı ile bilgileri kolay erişebilir duruma sokabilmektedir. Kurum çalışanlarının bunu yapma nedenleri olarak da sadakat eksikliği, aksi huyluluk, sıkıntılı olma, zarar verme isteği, şantaj yapma, en önemlisi para nedenleri sayılabilmektedir.

Dışarıdakiler, şirket dışından gelen casuslar, saldırıcılar (attackers) ve sistem kırıcılardır (hackers). Soğuk savaşın sonundan beri birkaç ülke kendi bilgi toplama yeteneklerini birçok büyük tescilli Amerikan şirketlerinden elde etmektedir. Dışarıdakiler İnternetten, çevirmeli-ağ (Dial-up) hatlarından, fiziksel girişler ya da ağ (network) ortaklarından (satıcı, müşteri ya da tedarikçi) bir bağlantı ile diğer şirketin ağına (network) geçerler.

Kite dışarıdakilerin genişleyebilen bir yapıdaki özel çeşididir. Kite müşterisine öyle bir yaklaşır ki karşıdaki anlamadan hangi tür bilgi işine lazımsa onları elde eder. Kite akla yatkın ikna edici nedenler sunabilen birisidir. Gizli operasyon açığa çıktığında, bir dava yada kriminal itham ortaya çıktığında, kiralanan şirket kite' in hareketlerinin sorumluluğunu inkar edebilir, ilişkiyi keserek, kite' nin uçup gitmesine izin verir.

Soğuk savaşın sonlanması ve işsiz istihbarat uzmanlarının artması ile ileri teknoloji ürünleri, ileri hayat uyumu (proliferasyon) ile ortak casusluğu kolay hale getirmiştir. Karşı istihbarat uygulamalarına anında uydurulan teknolojiler (Improvised Technology In Counter-Intelligence Applications) dergisinin yazarı Dr. Robert Ing, "Artık yerden atılabilen füze kodları yerine, flat panel tv' ler ile ilgili olarak teknolojik ve bilimsel datalar, elektrikli arabalar, yeni bilgisayarlar, rekabete dayalı stratejiler ve yenilikçi üretim/dağıtım süreçleri üzerine yeni hedeflere yönelik saldırılar ortaya konmaktadır." (aktaran, Eisenberg, 1999) demiştir.

İnsanlar gerçekten okuduklarına inanan tembel yaratıklardır, artık sahte diploma ile seçilen bir şirkette çalışan olarak işe girmek çok kolaydır. Herhangi bir sertifika programına yeniden başlamış gibi, istenilen bir derecede internette satın alınmış uydurma bir yüksek okul ismine oluşturulan bir kimlikle yapılabilmektedir. Her hangi biri Saint Regis Üniversitesinden değişik seviyelerden isteğine göre seçtiği diplomayı bedelini ödeyerek alabilir. Örneğin;

Hazırlık Sınıfı:450$

Yüksek Okul:550$

Yüksek Lisans:655$

Doktora: 995$

Yüksek okul ve master Kombinasyonu:1100$

Master ve fen fakültesi diploması: 1600$

Hazırlık master ve fen fakültesi diploması:1895 $

Seçtiği her bir alandan bir kişi; üniversite ya da lisenin ismini düzenleyebilir, diploma üzerinde mezuniyet tarihini düzenleyebilir.

Her bir düzeyde transkript verilebilmektedir, ayrıca istenilen şekilde kurs tarihleri, dereceler ve ortalama dereceleri. Diplomalar profesyonel parşömen kağıt üzerine basılı, altın mühürlü ve diploma başlıklı basılmaktadır. "Gerçekten mü-

kemmel şeklide sunum için hazırlanmıştır". Ayrıca transkript doğrulama servisi bulunmaktadır (Eisenberg, 1999).

Bilginin yerel ağlardan, internetten, bilgisayarlardan alınması bir diğer yere aktarılması o kadar kolaydır ki sadece bir diskete veya isimsiz bir hotmail e- postasına yollanabilir ve bu işi yapacak metotlar sayfalar dolusu yazı ile internette bulunmaktadır.

Şirketlere en az direnç gösteren yerlere saldırı mümkündür. Birçok şirkette güvenlik önlemleri alınmamış olarak, ofis kapıları kapatılmadan çıkılır, bilgisayarlar güvenlik korumaları olmadan terk edilmektedir. Güvenlik ve eğitim eksikliği ve saldırganların değişik taktikleri ile şirketlerin hayati bilgilerine erişim imkanı sağlar.

Ortak casuslukta kullanılacak bilgiye erişmek için kullanılan bazı metodlar; Fiziksel olarak hard diskin ayrılması ve bilgilerin başka bir makineye aktarılması, sistem kırma (hack etme), çöpleri boşaltma (dumpster diving), sosyal mühendislik, rüşvetçilik, anahtar çalışanları kiralama (Hiring away key employees) ve farklı bir çok taktik ile. Anahtar çalışanları kiralama ile ilgili Time Dergisindeki örnek, işin boyutları açısından ilgi çekicidir; Motorola İntelin kilit elamanlarını kiralama yolu ile (hiring away key employee), microyonga ticari sırlarını aldığını iddia etmişti. Minneapolis tarımsal alan ticaret devi Cargill, hilekar çalışanlarının rakiplerden genetik materyallerin çalınmış olabileceğini ve bununla Kuzey Amerika yem bölümünden Alman Bio teknoloji girişimine altı yüz elli milyon dolarlık sözleşme ile etkili şekilde giriş işlemi yapıldığını ve bunun ile karşı tarafa zarar verdirilmiş olabileceğini kabul etmiştir (Eisenberg, 1999).

Ortak Casusluk İle İlgili Örnekler

Yukarıda verilen ilk örneğimizde; iki şirket bir konu ile ilgili olarak bir açık arttırmada dokuz yüz milyon dolar üzerinde teklifte bulunmuştur. Şirketlerden birisi diğer şirketin e-postalarının açık arttırma ile ilgili olan e-postayı almış ve böylelikle e-postayı ele geçiren şirket diğer şirketin teklifinden daha az teklif ile açık arttırmayı kazanmıştır. Sistemi kırılan (hack) şirket içine yapılan bu sızmayı haftalar sonra tespit etmiş ve aslında işin acı tarafı şirket sisteminin bu hareketi anında kayıt altına almış olmasıdır.

İkinci örneğimizde; bir ilaç şirketinin çalışan sistem kırıcıları MS-DOS saldırıları ile rakip şirketin hizmet sunucusunu (server) çökertmeye çalışmıştır. Hizmet sunucusu (server), çöktüğünde sistem kırıcı (hacker) sisteme bir trojan atı programı yerleştirmiştir. Trojan ağda pusuda parolaları toplayıp bir gizli dosya içinde saklamıştır. Bu gizli dosyada biriken bilgiler ile rakip firmanın e- posta sistemine girmek, veri tabanı parolasını elde etmek, ücretlendirme tarifelerine erişmek için kullanmıştır. Nitekim rakip şirket ücretlendirme tarifelerini rakipleri ile ilişkilerini kesmek için kullanmıştır.

Üçüncü örnekte ise; Fransız savunma sanayine ait bir çalışma içine sızan sistem kırıcıları takımın üyesi gibi çalışır ve savunma şirketi içinde bir görev alır, stenegrofik metotları kullanarak resimler arkasına gömülü (Camuflage)[8] ticari sırları şirketin ticari sitesinin altında yayınlanmıştır. İkinci tim üyeleri ticari sırları şirketin internet sayfasından indirmiştir (Robinson, 2002).

İnternette Bilişim Suçlarında Kullanılan Metotlar

Sistem Kırıcılık (Hacking)

Tabi ki popüler olanları içinde ticari sırları çalmada sistem kırıcılık (hacking) üç metottan birisidir. E- posta sistem kırıcılığın (hacking) en önde olmasının iki nedeni vardır; 1) Sistem kırıcı (hacker) araçlarının büyük şekilde yararlanılabilir alanda olması. Şu anda yüz bin internet sitesi düzenlenebilir ücretsiz indirilebilen sistem kırıcı (hack) araçları ile doludur. 2) Sistem kırıcılık (hacking) göreceli olarak çok kolay işlemektedir. Derin bilgiye gerek olmadan, basitçe portokol veya internet protokol (Ip) adres bilgisi olmadan bir klik ve tuş ile kullanabilme kolaylığı vardır. Sistem kırıcılık (hacking) üç kategoride yapıyı kırıp içeri girer: Sistem, uzak erişim ve fiziksel erişim.

Sosyal Mühendislik

Temel amacı sistemlere izinsiz girmek yada dolandırma yolu ile bağlantı kurmak, izinsiz ağa (network) girmek, endistüriyel casusluk, kimlik hırsızlığı, sistem ya da ağın (network) bozulmasına yol açmaktır. Sosyal mühendislik iki ana kategoride tarif edilebilir; hem insan kaynaklı, hem de bilgisayar kaynaklı saldırı metodudur (Wendy, 2001).

Sosyal mühendislik kişileri kandırarak değerli bilgi ve parolalarını ellerinden almayı amaçlamaktadır. Bu amaçla örneğin e- posta (e-mail) atarak şifre elde etmeye çalışırlar, "shoulder surfing" sörf metodu ile basitçe kişisel bilgileri toplanan kişiye uygun parola tahminleri yapılır. Bu noktada sosyal mühendislerin çalışma metodolojisini anlayabilmek için bir örnek çalışmaya bakmak gerekir:

Bilgi erişimi amaçlı klasik bir saldırı metodolojisi için neler gereklidir? Hedef ile ilgili ne kadar çok bilgi toplanabilirse o kadar çok hedefin durumuna yönelik hedefleri, planları, hareketleri, stratejileri hakkında değerlendirme yapılabilir.

- Hedef ile ilgili alınabilecek bilgiler aşağıda belirtilmiştir:
- Pazar ve yeni ürün planları
- Kaynak kodları
- Şirket stratejileri
- Üretim, teknolojik çalışmalar

8 Belirtilen programın benzerleri ücretsiz olarak internette kolaylıkla bulunmaktadır. Örneğin; http://www.camouflage.freeserve.co.uk/Download.html, [online], 14.08.2003.

-Olağan ticaret metotları

-Ürün tasarımı, araştırma ve maliyetler

-Anlaşmalar ve akit tedbirleri; teslim, fiyatlandırma, bilimsel terimler

-Şirket internet sitesi

-Müşteri ve destekleyici bilgileri

-Birleşme ve elde etme planları

-Mali bütçeler, gelirler, vergiler

-Pazar, reklam giderleri

-Kaynakların fiyatları, stratejiler, listeler

-Sorumlular, operasyonlar, organizasyon şeması, isim/aylık cetvelleri

-Ayrıca tescilli bir hedef çalışması için sıcak hedefe yönelik, personel kayıtları

Aşağıdaki bilgilerden herhangi biri değerli olabilir:

-Ev adresleri

-Ev telefon numarası

-Karı koca ve çocuk adları

-Sosyal Güvenlik numarası

-Hasta kayıtları

-Kredi kartı kayıtları

-Performans değerlendirmeleri

Tüm bu veriler toplanarak elde bulunan veya internetten kolaylıkla bulunabilecek yardımcı program veya metotlar ile hedefe kolaylıkla varılabilecektir.

Sosyal Mühendislere Karşı Savunmayı Artırma

Davetsiz misafirler yani sistem kırıcılar (hackers) sürekli olarak değişik taktikler kullanarak bilgisayar sistemlerine yönelik yasal olmayan yollar ile sistemlere erişmeye çalışırlar. Kurumlarda bu tehlikeye karşı ağlarını (network) korumak için daha fazla zaman ve para harcarlar. Daha çok yapılan harcamalar teknolojik güvenlik önlemleridir, sistem yükseltmeleri, güvenlik sistem paketleri, en son teknoloji kripto sistemleri gibi. Fakat yeni bir yol olan sosyal mühendislik bu önlemleri önemsemeden, yasal olmayan uygulamalarına devam etmektedir. Bu tip saldırılara karşı kurumların savunmaları için iyi politikalara sahip olmaları gerekmektedir. Tabi ki bu durumda en iyi savunma eğitimdir.

Günümüzün güvenlik uzmanları sürekli bir değişmez mücadele içerisinde, son teknolojik değişimlere ayak uyduran ama bunu her zaman sistem kırıcıların (hacker) ve script şakacılarının (script kiddes) bir adım önünde yapan kişilerdir. Yayınlanan güvenlik bültenlerinde güvenlik açıkları, yeni zayıf noktalara yönelik bilgilendirmeleri, yeni yamaları, onarımları, yeni güvenlik ürünlerini, güvenlik uzmanları takip etse de yeni standart, ürünlerin standardını sağlama açısından takip etme çok fazla zaman ve imkan gerektirmektedir.

Sosyal mühendisler, güvenlik zincirinin en zayıf yerindeki, karmaşık güvenlik araçlarının bir yere toplanarak kullanımı ile çalışan insan aracına farklı yollardan giderler.

Dünyada hiçbir bilgisayar sistemi yoktur ki; insanı merkeze almasın. Bunun anlamı güvenlik zayıflıkları programların, platformun, ağın (network) ya da donanımların bağımsızlığı ile ilgili olmayan evrensel bir şeydir. Bütün bilgisayar güvenlik sistemleri fonksiyonlarında insani aracılık sistemleri gerektirir. İnsan aracı üzerine odaklanan bir sistem içinde hiçbir bilgisayar güvenlik sisteminin sosyal mühendisliğe karşı bağışıklığı temin edilemez.

Sosyal mühendislerin hangi sömürü metotlarını kullandıkları, nasıl çeşitli şekilde kişilik özelliklerini değiştirerek başarılı bir sosyal mühendislik yaptıkları aşağıda belirtilecektir, nitekim bu metotlar kullanılarak kişisel özellikleri de artırmak mümkündür, böylelikle daha başka yeni metotlarda geliştirilebilecektir (Wendy, 2001).

Sorumluluğun Yayılımı: Eğer hedefe onların kendi hareketlerinden sadece sorumlu olmadıklarına inandırılırsa, sosyal mühendisin ricasına uygun hareket ederler. Sosyal mühendisler çeşitli faktörlerin de yardımı ile oluşturdukları durumda, kişisel sorumluluk konusunu şaşırtma ile o kadar sulandırırlar ki bir karar vermeye zorlarlar. Sosyal mühendisler karar verme sürecinde diğer çalışanların isimlerini kullanırlar, ya da yüksek seviyeden yetkilendirilmiş bir eylem olduğunu; diğer bir çalışanın ağzı ile bunu iddia ederler.

Göze Girme Şansı: Hedef eğer bir rica ile razı olan birisi ise, başarılı olma şansı yüksektir. Bir rakip olarak onu yönlendirmede bu çok büyük bir avantaj sağlar, yada bilinmeyene göre yardım verir, sıcak bayan sesini kullanarak telefon aracılığı ile iletişime girerler.

Sistem kırıcılara (hackers) teknoloji ile içli dışlı insanlar olarak toplumsal ilişkilerde çoğu zaman beceriksiz insanlar topluluğu olarak bakılır. Nitekim bu kanı da doğrudur. Sosyal mühendisler etkilemenin yüksek hiçbir formunu kullanmadan bilgi elde ederler.

İlişkilere Güvenmek: Çoğu zaman, sosyal mühendisler belirledikleri kurban ile, iyi güvenilir bir ilişki için beklerler ve o zaman bu güveni sömürürler. Bunu takip eden zamanlarda ufak küçük etkileşimlerle ilişkiye girer ve doğal seyir içinde problem ortaya çıkar ve sosyal mühendis büyük hamlesini yapar. Böylece karşı taraftan şans verilmiş olur.

Ahlaki Görev: Hedefi dışarıdan ahlaksal olarak davranmaya cesaretlendirmek ya da başarı şansı için ahlaki hareket arttırmayı sağlamak. Bu durum için hedef olan kişi ya da organizasyondan bilgilerin sömürülerek alınmasını gerektiren bir iştir, hedef eğer karşıdakine uymanın yanlış olduğuna inanırsa, karşıdakini sorgulamanın hoş olmadığını hissederse, başarı şansı artmış demektir.

Suçluluk: Eğer mümkünse çoğu insan suçluluk hissinde olmaktan sakınır. Sosyal mühendisler çoğu zaman, psikodrama üstatlarıdır, öyle bir mizansen hazırlarlar ki insanın yüreği cız eder, empati ve duygudaşlık meydana getirirler. Hedef ile aralarında suçluluk duygusunu ortadan kaldıracak bir bağışta bulunurlarsa, hedef bundan çok fazla memnun olacaktır.

Künye: Sosyal mühendisin hüneri ile daha çok hedef tanımlanır ve bilgiye erişilir. Sosyal mühendisler iletişim anında daha çok zekice bir araya getirilmiş öncelikli temelli girişimlerle bağlantı kurmaya çalışırlar.

Faydalı Olmaya İstekli Olmak: Sosyal mühendisler diğer insanlara yardım etmeden zevk alanlara güvenerek eylemlerini yürütürler. Kahramanımız karşı kişiden ya bir giriş hakkı ister ya da bir hesaba giriş için yardım etmesini ister. Sosyal mühendisler ayrıca birçok bireyin zayıf red etme düzeyini bilerek ve işin uzmanına danışmanın dayanılmaz cazibesine sırtlarını dayayarak işlerini yaparlar.

Birbirine Göre Ayarlama: Hedef ile en az çatışma en iyisidir. Sosyal mühendisler genellikle ortamın gerektirdiği ses tonu ile zekice ve sabırlı sunuş yaparlar. Emir gibi, bir şey sipariş eder gibi, sinirli ve baş belası gibi kazanmak adına nadiren çalışırlar.

Sosyal mühendis kahramanları genellikle direkt rica edenler, uydurma durum, kişisel ikna gibi kategorileri kullanırlar.

Direkt Rica Edenler: Muhtemelen en basit metottur ve başarı için en son olan yoldur. Bir işe basitçe girişildiğinde sorulan bilgidir. Direkt rica genellikle meydan okumadır ve genellikle reddedilir. Başarı şansı düşük olduğundan nadiren tercih edilir.

Uydurma Durum: Bir şey veya bir organizasyonun özelliğine göre elde edilen bilgilerle yapılan üretilen bir durum, bir kriz veya özel bir an ile ilgili olarak bu durumdan faydalanmadır. Kriz durumları anlık yardım içerir, sosyal mühendisler hedefin güvenini arttırıcı durumun gerekliliği ve yardım edilme ile ilgili ortam oluştururlar. Sosyal mühendislerin taktikleri gerçek üzerine kurulu olsa da şunu unutmamak gerekir ki, kahramanlar gerçek tabanlı şeylere ihtiyaç duymaz, sadece ortalama gerekli şeylerle çalışırlar.

Kişisel İkna: Kişisel olarak yardım yapmayı isteyen bununla ilgili istekli insan gibi davranırlar. Amaçları kuvvetli uyum değildir, gönüllü-uyumlu insan anlayışına ulaşmaya çalışmaktır (Wendy, 2001).

Birçok bilişim teknolojisi (IT) güvenliğinde çalışan insan, gerekli bilgilerden yoksun bulunmaktadır. Bu işle uğraşanlara yönelik bilgi güvenliği farkındalığı programı uygulanmalıdır. Son kullanıcı kılavuzu, güvenlik öngörüleri ve güvenlik bilgileri olmalıdır.

Çalışanların, sosyal mühendis riski ile ilgili eğitimi bu saldırılara karşı kurumların savunma aracıdır. Sosyal mühendisler psikoloji üzerine kurulu ve sosyal hainliklere dayalı yeni hileler ile bizimle paylaşımda bulunurlar (Stevens, 2001). Bu çok özel saldırı metodunun farkındalığında özel süreçlerde eğitim ve çalışma gerektirir.

Dumpster Diving (Çöpleri Boşaltma)

Çöpleri karıştırma, oradan birşeyler bulabilmek için faaliyet içine girme, hem görüntü, hem koku, hemde insanın böyle bir şeye dayanabilmesi açısından tahammül edilebilecek bir iş değildir. Fakat ticari ve değerli bilgileri elde etme açısından çok önemli ve başarılı bir tekniktir. Çöpleri karıştırma kulağa iğrenç gelse de, Amerika'da kanunlara uygun bir iştir. Çöp umuma açık yer üzerinde sokaklarda, geçitlerde bulunuyorsa, kolaylıkla erişilebilecek yer olarak göz önüne alınır. Amerikan mahkemelerine göre; "ticari şirketlerce erişilebilecek alanlardaki çöpler, özel mülkiyetten çıkar. Bunlar sadece "izinsiz girilmez" levhası olan yerlerde bulunuyorsa ve siz eğer izinsiz boşaltım işlemi için girmişseniz, suç işlemiş olursunuz" şeklinde hüküm vermektedir.

Paylaşılan çöpler ile ilgili potansiyel güvenlik zayıflıkları olarak; şirket telefon rehberleri, organizasyon şekilleri, kısa notlar, şirketin siyaset tarzı, toplantı zamanları, sosyal olay ve tatiller, elle yapılan sistemler, bağlantı isim ve parolalarını içeren hassas yazıcı çıktıları, diskler ve kayıt üniteleri, şirket mektup başlıkları ve kısa not formları, zamanı geçmiş donanımlar belirlenmiştir. Çöpler, zengin bir bilgi kaynağı olarak ortak casusluk imkanını sunmaktadır. Yukarıda sayılan her bir araç uzman birinin elinde birçok işe yarayabilir.

Konunun önemine uygun olarak, Amerika'da, çöpleri boşaltma ile ilgili kanun maddeleri hazırlanmıştır "An Act Concerning Dumpester Diving". Kanun tasarısına konan bu ilke bilgisayar sistem kırma (hack) ve kanunsuz dinleme v.b. ile aynı sayılarak, Ticari Gizliliği Koruma Kanunu adı altında başlıklandırılmıştır. Çöp boşaltma kurbanı olan şirketin kendine karşı bu bilgilerin kullanılması durumunda yüksek mahkeme yolu ile bunu bozma gibi bir hakkı vardır. Bu şirketler ayrıca cezayı gerektiren tazminat hakkı için dava açma hakkı elde ederler. Fakat bu konu ile ilgili olarak mahkemenin verdiği karara dayanarak insanların çöpe attıkları çöpler ile ilgili bir hakkı olmaz iken; "Neden iş alemi korunuyor ve sen, ben, hemen yanı başımızdakiler korunmuyor?" şeklinde eleştiriler vardır (Scarponi, 1997). Nitekim bu konu ile ilgili olarak yüksek mahkeme kararında polisin dahi yaptığı aramada bir haklı gerekçeye işaret edilmiştir; "Greenwood is-

minde birisi hakkında narkotik trafiğini yönlendiriyor olabileceği ile ilgili bilgi alınmıştır, polis iki kere olağan olarak toplanan evinin önüne koyduğu çöplerini karıştırmış ve narkotik maddelerin kullanıldığını gösteren emareler bulunması üzerine polis bu maddelere dayanarak evi araştırmak istemiştir. Araştırmada gerçekten böyle maddeler bulmuş ve buna dayanarak narkotik maddeleri bulundurma suçlaması ile şahıs göz altına almıştır. Narkotik maddenin evin içinde bulunabileceğini gösteren emarelerin çöp içinde bulunması evin aranması için yeterli delil olduğu ile ilgili ithamın geri alınmasını jüriden Krivda isimli şahıs sebepsiz yere çöplerin karıştırılmasının Kaliforniya Anayasası ve dördüncü kanun değişimine uymadığını belirtmiştir, fakat federal kanun için bir şey belirtmemiştir. Devlet mahkemesi de Krivda' nın görüşü üzerine karar almış, ayrıca federal ve devlet kanunlarını da göz önünde bulundurmuştur. Kararda; "a) Çöp toplama alanına atılan çöpler ile ilgili objektif değerlendirmede, bu yapılan eylemin açık alanda yapılan bir eylem olduğu, kişisel gizlilik alanına müdahale olmadığı görülmüştür. Halkın kullanım alanında uygun olan yerlere atılan plastik çöp torbalarına, çocuklar, hayvanlar, çöpçüler, gizlice bir şey arayanlar, kısaca herkes rahatça erişebilir. Çöp toplayıcılardan topladıkları çöpleri ayrı ayrı düzenleyenler olduğu gibi polis de çöpleri suç hareketinin takibi için ayrı ayrı düzenleyebilir. Polis diğer insanlar gibi istediği zaman araştırma yapmaz ancak **suça yönelik aydınlatma amacı** ile araştırma yapabilir. b) Greenwood'un çöp ile ilgili olan alternatif görüşünde ise; kişinin özel alanına yönelik yapılan sebepsiz arama Kaliforniya Kanununa göre izinsiz yapılmış olur. Sebepsiz arama, Anayasa'nın ve devletin vatandaşlara tanımış olduğu özgürlük alanına müdahaleyi ifade eder" (U.S. Supreme Court California v. Greenwood, 1988) şeklinde yargı kararı bulunmaktadır.

Kuvvetli Darbe (Whacking)

Temel olarak kuvvetli darbe kablosuz sistem kırma (hacking) dır. Kablosuz ağı (network) gizli dinleyen sistemlerin hepsi doğru bir radyo kanalını bulmayı ve kablosuz iletimin içinde bulunabilmeyi gerektirir. Gerekli donanım ile ofis binalarının dışından sinyallerin toplanabilmesi mümkündür. Bir defa yüklenen bir kablosuz şebeke sistemi ile davetsiz misafir genelde şifrelenmemiş (kriptolanmamış) olarak ağdan (network) gönderilen bilgiyi toplarlar.

Kolay Telefon Düşmesi

Ortak bilgide (corporate espionage) telefon düşmesi başka bir yol olarak kullanılmaktadır. Dijital kayıt yapan alet ile faks cihazını iletim ve kabulünü izleyen bir sistemi oluşturmak, faks cihazına bir bilgi gelmeden önce kimsenin bilgisi olmadan bir kopyasının alınması, telefon ile görüşmede bir kişinin sesleri toplanarak, banka hesabına erişmesi mümkündür.

Amerikan Örneğinde Bilişim Suçlarını Takip

Amerika'da bilgisayar ve bilgisayar sistemlerine yönelik olay meydana geldiğinde yerel polis otoritelerine müracaat edilmekle birlikte internet üzerinden bu müracaatların yapılması mümkündür. Özellikle bilişim güvenliği konusunda FBI ile birlikte çalışmalarını devam ettiren CERT/cc'nin bu konu ile ilgili olarak hazırlamış olduğu süreç kılavuzu iyi bir örnektir. Bu kılavuzda ilk olarak, bir olay olduğunda, bilişim güvenliği ile ilgili yetkilendirilmiş kişilere erişim nasıl olacak ve aşağıdaki basamaklar olay ile ilgili olarak toplanacak delillendirme de yardımcı olacaktır denilmektedir.

İlk olarak sizin çalıştığınız yerin kural ve kaidelerine uygun davrandığınızdan emin olun,

1. Davetsiz misafir tarafından değiştirilen veya zarar gören, dosyaların bu işlemin olduğu andaki bilgisayar sistem kayıtlarının (system log) yedeğini alarak tespit edin.
2. Eğer davetsiz misafiri eylemini yaptığı anda tespit ettiyseniz, denetleme yazılımını aktif hale getirerek, eğer sistem kayıtlarında (system log) izinsiz giriş ikazı yanar ise, tuş darbelerini dikkate alarak izleyin.
3. CERT/CC ye ne olduğu ile ilgili bilgi almak üzere müracaat eder iseniz, size ne olduğunu bildirecektir.

   CERT/CC'nin olay başvuru formu belirtilen köprüdedir[9]; diyerek çalışma köprüsü belirtilmektedir.
4. Bir olaydan dolayı zarar gören ve tüm dokümanları kayıp olan kurumunuzun bilgileri içinde aşağıda sayılı konuların belli olması gerekir.

- Bu konu ile ilgili tahmini olarak kurtarma ve mücadeleye diğer iş kayıplarını da içine katarak ne kadar zaman harcadınız ?
- Geçici yardımın ücreti,
- Zarar gören ekipmanın ücreti,
- Kayıp olan bilginin değeri,
- Bu güçlükten dolayı müşterilere verilen kredinin miktarı,
- Gelir kaybı,
- Herhangi bir "Ticari Sırrın" değeri,

5. Polis ile iletişime geçin ve olay ile ilgili dokümanları verin.

- Davetsiz misafir hakkındaki bilgileri paylaşın.
- Olabilecek tüm fikirlerinizi paylaşın (CERT Coordination Center, 2002) şeklinde bir yönlendirme yapmaktadır.

9 10.08.2002 tarihi itibari ile, https://www.cert.org/reporting/incident_form.txt, adresinden bu hizmet verilmektedir.

Sonuç

Çağımızda bilginin kullanımı artık yetmemekte kullanılan bilginin korunması ve sağlıklı şekilde iletilmesi ön plana çıkmaktadır. Özellikle Amerika'da yaşanan 11 Eylül saldırıları da göstermiştir ki; çağdaş dünyada bilgiyi iyi koruyan ve onu ekonomik, siyasal, … güce dönüştürebilen ülkeler başarılı olabilecektir. Ülkemizin de bilgi politikasının değişen şartlara uygun hale getirilmesi artık temel bir mecburiyet haline gelmiştir.

E-devlet kavramının zaman ve mekan açısından sağladığı faydalar göz önüne alındığında yapılacak akılcı ve ilkeli çalışmalar devlet sistemimizi olumlu yönde geliştirecektir. Bulunduğumuz nokta henüz başlangıç noktasını ifade etmektedir, bu noktada sağlanacak sağlam tabanlı sistemler ve yasal düzenlemeler gelecekteki olası tehlikeleri önleyecek ve bilgi sisteminin sağlamlığını sağlayacaktır.

Bilgi Edinme Hakkı ile ilgili olarak düzenlenen yayım tarihinden altı ay sonra yürürlüğe girecek olan 09.10.2003 tarih, 4982 sayılı "Bilgi Edinme Hakkı Kanunu" hükmü uyarınca kamu kurumlarına yüklenen bilgi verme görevi ile internetten bilginin daha az kaynak, zaman, personel... harcayarak sunumu ile önümüzdeki zaman içinde internet uygulamalarının kamu alanında daha yoğun olarak kullanılacağı, aynen Amerikan örneğinde olduğu gibi ülkemizde de hızlı bir şekilde bilginin internet ile sunumuna yönelik daha ciddi ve profesyonel uygulamaların yapılacağı düşünülmektedir.

Bilginin; gelinen noktada önemi ortadadır. Bilgiye sahip olan ister devlet, isterse özel sektör olsun artık ekonomik değer ifade eden bu metadan dolayı hedef haline gelmiştir. Çalışmada ortaya konan tehlikeler elbetteki buzdağının görünen kısmıdır. Bilgi sunumu ile ilgili teknik, hukuki, idari, sosyal, alanlarda ciddi düzenlemelere ihtiyaç bulunmaktadır. Özellikle sunulan bilgi standart ve bilgiye erişmede kişisel haklar ile ilgili düzenlemeler öncelikli olmalıdır. Devletimizin yapacağı bu çalışmalar çağdaş dünyada ülkemizin ciddi ve bilinçli sunumunun yanında, ulusal alanda da vatandaşlara sürdürülebilir ve kesintisiz hizmeti sağlayacaktır.

Kaynakça

CERT Coordination Center, (1999), "International Coordination for Cyber Crime and Terrorism in the 21 st Century", http://www.cert.org/reports/stanford_whitepaper-V6.pdf, (01.07.2002).

CERT Coordination Center, (2002), "How the FBI Investigates Computer Crime",http://www.cert.org/tech_tips/FBI_investigates_crime.html., (19.05.2002).

Cliff, Edwards, (2000), "News", http://abcnews.go.com/sections/tech/DailyNews/transmetaspy000701.html, (13.05.2002).

Computer Security Institute, (2002), "FOR IMMEDIATE RELEASE Cyber crime bleeds U.S. Corporations, Survey Shows; Financial Losses From Attacks Climb For Third Year In A Row", http://www.gocsi.com/press/20020407.html, (16.06.2002).

Eisenberg, Daniel, (1999), "Eyeing The Competition", *Time BUSINESS*, March 22, 1999 Vol. 153, No. 11.

Gordon Murnane, Laura, (2002), "Access to Government Information In A Post 9/11 World", *Searcher: The Magazine For Database Professionals*, Volume:10, Number:6, June, ss. 51-62.

Hart, Teeter, (2002), "E-Government: To Connect, Protect, and Serve Us", http://egov.gov/documents/egovreport.htm, (18.08.2002).

Perton, Victor, (2000a) Aktaran, "Victoria's Proposals for a 21. Century Legal System", *Journal of Information*, Law and Technology, Issue:1, ss. 1-13. (K. Wigg (1999), 'Introducing Knowledge Management into the Enterprise' in J. Liebowitz (ed) *Knowledge Management Handbook*, CRC Press, New York.)

---------(2000b) Aktaran, "Victoria's Proposals for a 21st Century Legal System", Journal of Information, Law and Technology, Issue 1, ss. 1-13. (T. Davenport ve L. Prusak (1998), "Working Knowledge: How Organisations Manage What they Know", Harvard Business School Press, Boston, p. 1.)

Power, Richard, (2002), "CSI/FBI Computer Crime And Security Survey", *Computer Security Issuses&Trends*, Vol:VIII,No:1, Spring.

Robinson, Shane W., (2002), "Corporate Espionage 101", http://rr.sans.org/social/espionage.php, (13.05.2002).

Scarponi, Diane, (1997), *Newspaper & Magazine Articles*, http://www.phonelosers.org/dd.html., (13.05.2002).

Stevens, George, (2001), "Enhancing Defenses Against Social Engineering", *SANS Institute*, http://www.sans.org/infosecFAQ/social/social.htm, 28.07.2002.

U.S. Supreme Court CALIFORNIA v. GREENWOOD, 486 U.S. 35 (1988) http://laws.findlaw.com/us/486/35.html, Argued January 11, 1988, Decided May 16, 1988.

Wendy, Arthurs, (2001), 02.08. "A Proactive Defence to Social Engineering", *SANS Institute*, http://www.sans.org/infosecFAQ/social/defence.htm, (20.06.2002).

Widdison, Robin, (1997), "Electronic Law Practice: An Exercise in Legal Futurology", *Modern Law Review*, N: 60, ss.143-163.

Köprüler

<http:// www.mi2g.com>

<http:// www.nicx.com>