Politeknik Dergisi
Cilt: 9 Sayı: 3 s. 165-174, 2006

Journal of Polytechnic
Vol: 9 No: 3 pp. 165-174, 2006

Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme

Gürol CANBEK, Şeref SAĞIROĞLU
Gazi Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü
06570 Maltepe, ANKARA

ÖZET

Bu inceleme çalışmasında, bilgi olgusu geniş bir açıdan irdelenmiş, veri, bilgi ve özbilgi kavramları açıklanmış, bilişim teknolojilerinin bilgi üzerindeki etkileri ve boyutları ortaya konulmuş, elde edilmesi zor olan bilginin korunması ihtiyacından doğan bilgi güvenliği incelenmiş ve bilgi güvenliğini oluşturan ana unsurlar üzerinde durulmuştur. Bilgi güvenliğine yönelik saldırıların, zaman içinde hem sayı hem de çeşitlilik açısından arttığı bir ortamda etkin bir bilgi güvenliği oluşturabilmek için gerekli olan, güvenlik süreçleri bu çalışma da özetlenmiştir. Sonuçta, açıklanan, incelenen, irdelenen ve özetlenen hususlar genel olarak değerlendirilmiştir.

Anahtar Kelimeler: Bilgi, Özbilgi, Bilgi Güvenliği, Güvenlik Süreçleri

A Review on Information, Information Security and Security Processes

ABSTRACT

In this article, the concept information is evaluated in details, the influence and dimension of information technologies on information and information security have been expressed and information security requirements have been revised. The security processes designating the security policy which is necessary to establish an effective information security in an environment where the attacks against the information security are increased in quantity and variety we summarized. Finally, the work has been evaluated on the basis of explanations given in this article.

Key Words: Information, Knowledge, Information Security, Security Processes

1. GİRİŞ

Dünyada olduğu gibi ülkemizde de bilişim teknolojilerinin yaygınlaşması ve kullanımı hızla artmaktadır (1–3). Bu teknolojilerin kullanımı ülkemizde hızla yaygınlaştırılmaya çalışılırken, geliştirilmesi ve etkin kullanımı konusunda birçok yetersizlik söz konusudur. Gelişen bilişim teknolojilerinin etkin kullanımında olması gereken seviyenin oldukça altında bulunduğumuz ve bilgi toplumunun ana unsurları olan kullanım yaygınlığı, etkin kullanım, kültür ve üretim gibi konularda ise gerilerde olduğumuz bilinmektedir (3). Bilişim teknolojileri ile bu teknolojilerin hammaddesi, girdisi ve çıktısı olan bilginin önemi tam olarak anlaşılmış değildir. Bilginin ne olduğu ve ne gibi bir öneme ve potansiyele sahip olduğu yeterince anlaşılmadığından; bilişim teknolojileri ve bilgi güvenliği konusunda gereken ehemmiyet gösterilememektedir (3–9). Bu çalışmada; bilgi güvenliğine gerekli önemin verilebilmesi için genel olarak önemli kavramlar incelenmiş, bilgi ve bilgisayar güvenliği konuları, unsurları ve süreçleri üzerinde durulmuş ve yüksek derecede bir güvenlik için uygulanması gerekenler açıklanmıştır. Bunun sonucunda; bilgi ve bilgisayar güvenliğine neden önem verilmesi gerektiği ve bilgi güvenliğinin en temel anlamda nasıl oluşturulabileceği gibi sorulara kapsamlı cevaplar aranmaya çalışılmıştır. Bu çalışmanın bilginin ve onun daha ilerisinde özbilginin önemi, bu önemi algılayıp elde bulunan ve kullanılan bilginin korunmasına yönelik güvenlik süreçlerinin oluşturulması aşamaları, belirli bir sistematik içerisinde açıklanmıştır.

Bu çalışmada, Bölüm 2'de veri, bilgi ve özbilgi kavramları genel olarak incelenmektedir. Bilginin ne gibi özellikler içerdiği; gerçeklikten hikmete ulaşmak için aşılması gereken veri, bilgi ve özbilgi basamakları bu bölümde aktarılmaktadır. Bilgi kullanımında bilişim teknolojilerinin etkisi ve yaygınlığı yine bu bölümde istatistiklerle ortaya konulmuştur. Bilgi ve bilgisayar güvenliği ile bu sistemlere yapılan saldırılar Bölüm 3'de incelenmiştir. Eksiksiz bir bilgi güvenliğinin taşıması gerektiği unsurlar Bölüm 4'de aktarılmaktadır. Bilgi güvenliğinin bu unsurları karşılaması için oluşturulması gereken güvenlik politikasını meydana getiren temel güvenlik süreçleri; önleme, saptama ve karşılık verme Bölüm 5'de açıklanmıştır. Bölüm 6'da bu çalışmadan elde edilen sonuçlar ve yapılan değerlendirmeler sunulmuştur.

2. VERİ, BİLGİ ve ÖZBİLGİ

Bilginin yaşadığımız çağa damgasını vuran bir varlık olduğu bir gerçektir. Bu açıdan bakıldığında, ça-

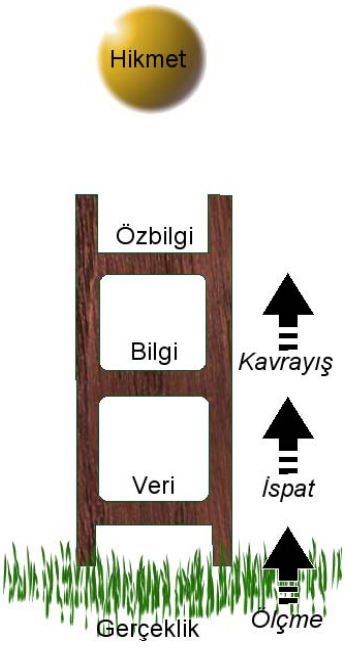
Digital Object Identifier 10.2339/2006.9.3.165-174

ğımızın altın değerindeki hammaddesi olan bilgiyi tanımlamak, kavramak ve bilgi ile ilgili hususları incelemek, insanlığın başlangıcından itibaren geçen süreçte ileriye yönelik gelişimimizi şekillendirmenin en önemli anahtarıdır (6). Günümüzde bilgi ön plana çıkmış gibi gözükse de, aslında bilgi; dünün ve bugünün anahtarları iken, geleceğin şekillenmesinde de her zaman anahtar rollere sahiptir.

Bilginin doğası ile ilgili aşağıda derlenen sözler, bilginin değerini ve boyutlarını bir kez daha gözler önüne sermek açısından faydalı olabilir (10).

Bilgi;

- boşlukta ve zamanda yer kaplar.
- gürültü çıkarmadan hareket edemez.
- hareketi için enerji gerekir.
- yaşam ve herhangi bir düzenli etkinlik için gereklidir.
- hem maddesiz biçim, hem biçimsiz maddedir.
- ağırlığa sahiptir. Bir giga bayt, bir parmak izinden daha az ağırlıktadır.
- zaman içinde hareketli veya donmuş olabilir.
- bir soruya tatmin edici, belki de rahatsızlık verici bir cevaptır.
- katı hale sahiptir, donarak katılaşır (depolama).
- sıvı hale sahiptir, akar (iletişim).
- bir yerlerde bilgi hareket eder, evren gümbürder ve gerçeği gürler.
- maddeden farklı olarak bilgi aynı anda birden fazla yerde olabilir.
- el sıkışma, baş sallama, bakış veya iç çekiştir.
- rastsallık denizinde parlar.



Şekil 1. Gerçeklikten hikmete ulaşmak için aşılması gereken bilgi basamakları

Bilgi çağında ilerlemek, bir merdivenin basamaklarını kullanarak bir üst seviyeye çıkmaya benzetilebilir (11). Şekil 1'de gerçeklik (reality) ile hikmet (wisdom) arasında gösterilen bu merdivenin basamakları, veri (data), bilgi (information), özbilgi (knowledge) basamaklarıdır. Çoğu durumda, her basamak, atlanmadan teker teker geçilir. Yukarıya çıktıkça elimizdeki şeyin miktarı azalırken, değeri artar. Yine yukarıya çıktıkça, bir sonraki basamağa adım atmak daha da zorlaşır veya daha çok çaba ister. Bu yüzden, merdivenin alt basamaklarında verinin ve bilginin paylaşımı daha kolay iken yahut insanlar veya çalışanlar elde ettikleri veri ve bilgileri paylaşmaya daha açık iken, daha yukarı çıkıldığında özbilginin paylaşımı için aynı şey söylenemez (12). Genel olarak bilimin getirdiği yöntemlerden, ölçme ile eldeki gerçeklikten veriye, ispat ile veriden bilgiye ve kavrayış ile bilgiden özbilgiye ulaşılır (13). Özbilgiden hikmete ulaşma, sentezleme içeren bir düşünüş gerektirir. Bu düşünüş, fikirlerin öyle bir şekilde bir araya getirilmesidir ki ulaşılan bütün parçalarının toplamından daha büyüktür (14).

Bir başka gözlem de, merdivenin alt basamaklarında, daha algoritmik ve programlanabilir bir yaklaşıma ihtiyaç duyulurken, daha yukarı basamaklar, algoritmik olmayan ve programlanamayan bir yapı arz etmesidir (15). Veri ve bilginin iletiminde bilişim teknolojileri kullanılabilirken, özbilgi de buna ek olarak insan etkeni de işin içine girmektedir (16). Bir özbilginin gerçeklik haline dönüştürülmesi için yönetim biliminden yararlanılır.

Bilgi ve özbilgi kavramları veya basamakları, ülkemizde çoğu kez birbirleri ile karıştırılmaktadır (3). Bu sebepten dolayı, ilgili kavramlar takip eden paragraflarda detaylı olarak tanımlanmış ve açıklanmıştır.

Verinin; İngilizce karşılığı olarak kullanılan "data", Latince "datum" kelimesinden (çoğul şekli "data" ve "vermeye cesaret etmek" fiilinin geçmiş zamanı, dolayısıyla "verilen şey") gelmektedir. Latince "data" (dedomena) kavramının M.Ö. 300 yıllarında Öklid'in bir çalışmasında geçtiği bildirilmektedir (17). Dilimizde de "verilen şey" anlamında, "veri" olarak kullanılmaktadır. Bilişim teknolojisi açısından veri, bir durum hakkında, birbiriyle bağlantısı henüz kurulmamış bilinenler veya kısaca, sayısal ortamlarda bulunan ve taşınan sinyaller ve/veya bit dizeleri olarak tanımlanabilir.

Bilgi; verinin belli bir anlam ifade edecek şekilde düzenlenmiş halidir. Bu aşamada, veri ve ilişkili olduğu konu, bilgi üretecek şekilde bir araya getirilir. İşlenmiş veri olarak da ifade edilebilecek bilgi, Shannon tarafından "bir konu hakkında var olan belirsizliği azaltan bir kaynak" olarak tanımlanmıştır. Kısaca, veri üzerinde yapılan uygun bütün işlemlerin (mantığa dayanan dönüşüm, ilişkiler, formüller, varsayımlar, basitleştirmeler, v.s.) çıktısı, bilgi olarak ifade edilebilir.

Özbilgi; tecrübe veya öğrenme şeklinde veya iç gözlem şeklinde elde edilen gerçeklerin, doğruların veya bilginin, farkında olunması ve anlaşılmasıdır.

Çizelge 1. Dünya İnternet Kullanım ve Nüfus İstatistiği (1)

Bölgeler	Nüfus (2005 tahmini)	% Dünya Nüfusu	İnternet Kullanımı	Kullanım Büyümesi 2000-2005	% Nüfus Yaygınlık	% Dünya Kullanıcı
Afrika	896 721 874	% 14,0	23 867 500	% 428,7	% 2,7	% 2,5
Asya	3 622 994 130	% 56,4	327 066 713	% 186,1	% 9,0	% 33,9
Avrupa	804 574 696	% 12,5	283 482 940	% 169,7	% 35,2	% 29,4
Ortadoğu	187 258 006	% 2,9	15 452 500	% 370,4	% 8,3	% 1,6
Kuzey Amerika	328 387 059	% 5,1	223 971 489	% 107,2	% 68,2	% 23,2
Latin Amerika/Karayip	546 723 509	% 8,5	72 792 797	% 302,9	% 13,3	% 7,5
Okyanusya/Avustralya	33 443 448	% 0,5	17 655 762	% 131,7	% 52,8	% 1,8
DÜNYA TOPLAM	**6 420 102 722**	**% 100,0**	**964 289 701**	**% 167,1**	**% 15,0**	**% 100,0**

Verileri bir araya getirilip, işlenmesiyle bilgiyi oluştursa da özbilgi, kullanılan bilgilerin toplamından daha üstte bir kavramdır. Bir güç oluşturabilecek, katma değer sağlayabilecek veya bir araç haline dönüşmek üzere, daha fazla ve özenli olarak işlenmiş bilgi, asıl değerli olan özbilgidir. Özbilgi, ne olduğunu (know-what), niçin olduğunu (know-why), nasıl olduğunu (know-how) ve kim olduğunu (know-who) bilmek şeklinde dört sınıftan oluşur. Ne olduğunu bilmek, gerçeklerin toplamıdır ve bilgiye en yakın olan sınıftır. Niçin olduğunu bilmek, teknolojik gelişmenin altında yatan ilke ve yasaların açıklandığı bilimsel özbilgidir. Nasıl olduğunu bilmek, bir şeyi yapabilme becerisidir. Kimin olduğunu bilmek, kimin neyi ve kimin neyi nasıl yapılacağını bildiğini bilmek olarak özetlenebilir (18).

Hikmet (wisdom), tasavvur, ileri görüş ve ufkun ötesini görme yetisi ile en ileri seviyede soyutlama ve bir kişinin özel bir iş sahasındaki meslek hayatı boyunca elde edilmiş deneyimin özüdür (19). Hikmet, ayrıca, güvenilir yargıda bulunmak ve karar vermek için özbilginin nasıl kullanılacağını kavramak olarak da tanımlanmaktadır (20).

Veri, bilgi, özbilgi ve hikmet gibi kavramların bilişim teknolojilerinin temel yapı taşları olduğunu göz ardı etmemek gerekir. Bu bakış açısı, bilginin önemini ve bilgi ve bilgisayar güvenliğini her zaman öncelikli bir konumda tutmakta yardımcı olacaktır. Her ne kadar, bilgi ile ilgili belirtilen kavramlar, burada bilişim teknolojileri ve özbilgi yönetimi açısından değerlendirilse de bu kavramların altında binlerce yıllık bir insanlık medeniyetinin yattığını da hatırlatmak gerekir. Bilginin önemini kavrayan tarihteki her uygarlık, onu korumaya yönelik olarak, farklı güvenlik yöntemleri geliştirmişlerdir (7–9).

Günümüzde bilginin üretilme, depolanma, korunma, kullanılma, paylaşma, yayılma, etkileşme ve artma hızı, teknolojinin getirdiği hızlı bilgi işleme ve iletişim araçları ile baş döndürücü bir hal almıştır. Bilgisayar ve haberleşme teknolojilerinde yaşanan baş döndürücü gelişmeler ve özellikle İnternet'in katalizör etkisi ile insanların çalışma, iletişim kurma ve her türlü günlük ihtiyaçlarını karşılama biçimi sürekli bir dönüşüm halindedir (21).

İnternet'in ulaştığı boyutları ortaya koymak açısından yapılan bir çalışmanın sonuçlarını burada aktarmak yerinde olacaktır. Çizelge 1'de Kasım 2005 tarihi itibari ile dünyada İnternet kullanımının her bir bölge için ne kadar olduğu ve 2000–2005 yılları arasındaki İnternet kullanımı artışı gösterilmektedir. Sunulan raporda, dünya nüfusunun %15'i (964 289 701 kişi) İnternet kullanmaktadır. İnternet kullanıcı sayısındaki artış 2000–2005 yılları arasında %167,1'dir. Bu süreler zarfında kullanıcı artışının en çok olduğu bölgeler %428,7 ile Afrika, %370,4 ile Ortadoğu ve %302,9 ile Latin Amerika/Karayip bölgeleridir.

Ülkemizde bilişim teknolojilerin kullanımına yönelik bir araştırma mevcuttur. Çizelge 2'de Devlet

Çizelge 2. Cinsiyete göre Türkiye, kent-kır ayrımında bilgisayar ve İnternet yüzde kullanım oranları (2)

		Bilgisayar kullanım oranı			İnternet Kullanım oranı		
		Toplam	Kadın	Erkek	Toplam	Kadın	Erkek
Son üç ay içinde (Nisan-Haziran 2005)	Türkiye	17,65	5,77	11,88	13,93	4,33	9,60
	Kent	23,16	7,92	15,24	18,57	6,06	12,51
	Kır	8,28	2,12	6,16	6,05	1,39	4,66
Üç ay - bir yıl önce	Türkiye	1,88	0,71	1,17	1,52	0,54	0,99
	Kent	2,44	0,95	1,49	1,96	0,72	1,24
	Kır	0,92	0,29	0,63	0,78	0,22	0,56
Bir yıldan çok oldu	Türkiye	3,42	1,53	1,89	2,10	0,74	1,36
	Kent	3,98	1,83	2,16	2,54	0,92	1,61
	Kır	2,45	1,03	1,42	1,36	0,43	0,92
Hiç kullanmadı	Türkiye	77,06	42,28	34,78	82,45	44,68	37,76
	Kent	70,41	38,65	31,77	76,94	41,65	35,29
	Kır	88,35	48,45	39,90	91,81	49,84	41,97

İstatistik Enstitüsü tarafından Nisan-Haziran 2005 aylarında 10151 hanedeki 27013 birey ile yapılan yüz yüze görüşme ile gerçekleştirilen Hanehalkı Bilişim Teknolojileri Kullanımı Araştırması sonuçlarına göre kent-kır ve cinsiyete göre bilgisayar ve İnternet kullanım oranları gösterilmektedir. Bu araştırmada, hanelerin %8,66'sının İnternet'e erişim imkânına sahip olduğu, bilgisayar ve İnternet kullanım oranlarının sırasıyla %17,65 ve %13,93 olduğu belirtilmektedir. Çizelge 1'den de görülebileceği gibi kırsal kesimde bilgisayar ve İnternet kullanımı kentlere göre daha düşüktür ve kullanıcıların çoğunluğu erkektir.

Çizelge 2'de verilen araştırma sonuçlarından da görülebileceği gibi gerek ülkemizde gerekse dünyada bilgisayar ve İnternet kullanımı gittikçe yaygınlaşmaktadır. İnsanlar, İnternet'i bilgiye ulaşmak için daha uygun bir ortam olarak değerlendirmekte ve kullanmaktadır. Amerika Birleşik Devletleri'nde 2003 Ocak ayında Google, AOL Search, Yahoo, MSN Search, Ask Jeeves, InfoSpace, AltaVista, Overture, Netscape, Earthlink, Looksmart ve Lycos İnternet arama motorlarında günlük yapılan arama sayısı toplam olarak 319 milyon olarak belirtilmiştir (22). Bu sayının günümüzde çok daha fazla olduğu değerlendirilmektedir.

Üretilen bilgilerin büyüklüğü, saklanması ve aktarılması da önemli konulardandır. Üretilen bilgi; kâğıt (kitap, gazete, büro belgeleri, süreli yayınlar, mektup v.s.), film (fotoğraf, sinema, televizyon film ve dizileri, video, x ışını), manyetik (video, ses ve sayısal bant, miniDV, disket, zip, flash ve sabit disk) ve optik (ses CD, CD ROM ve DVD) saklama ortamlarında depolanmakta; telefon, radyo, televizyon ve İnternet gibi elektronik kanallar aracılığıyla akmaktadır.

Yıllara göre üretilen toplam bilgiyi çıkartmaya yönelik bir araştırmaya göre 2002 yılında bu dört bilgi saklama ortamında depolanan yeni bilginin kapasitesi toplam 5 eksa bayt'tır (10^{18} bayt'tır). Amerikan Kongresi Kütüphanesinde var olan basılı koleksiyonun tamamının 10 tera bayt'lık bir bilgi kapasitesinde olduğu düşünülürse, 2002 yılında üretilip depolanan yeni bilgi, 100 000 Amerikan Kongresi Kütüphanesindeki bilgiye denk düşmektedir. 2002 yılında üretilen 5 eksa bayt'lık verinin %92'si çoğunlukla sabit disk olmak üzere manyetik ortamda saklanmaktadır. Yine bu araştırmanın sonuçlarına göre 2002 yılında 18 eksabayt'lık yeni bilgi telefon, radyo, televizyon ve İnternet aracılığıyla akmaktadır. Bu bilginin %98'i hem ses hem de veri dâhil olmak üzere telefon aracılığıyla gönderilmiş ve alınmıştır. 2002 yılında İnternet üzerinden akan veri miktarı 0,5 eksa bayt'tır (23).

Günümüz insanı, günlük yaşamında bile yoğun bir bilgi bombardımanı altındadır. Bu yüzden bilgiye erişimde seçici yöntemler kullanılarak, doğrudan ulaşılmak istenilen bilgiye eriştirecek yöntemler geliştirilmelidir. Bilgiye etkin bir şekilde ulaşım ve bilgi işleme ile ilgili bu konular bu çalışmanın kapsamı dışındadır.

Bilgi ile ilgili bir başka önemli konu da, bilginin taşıdığı değerdir. Bilginin değerli veya değersiz olduğunu belirlemek veya bilginin taşıdığı değeri ölçmek, en az bilginin kendisi kadar önemlidir. Elde edilen bilgiyi değerlendirirken, bilginin kalitesini gösteren özelliklere bakılması gerekir. Doğruluk, güncellik, konuyla ilgili olma, bütünlük ve öz, gereksinimlere uyum gösterme, iyi sunulma ve fiziksel ve idrak yolu ile erişim gibi ölçütler bilginin kalitesini belirleyen etmenlerden bazılarıdır (24).

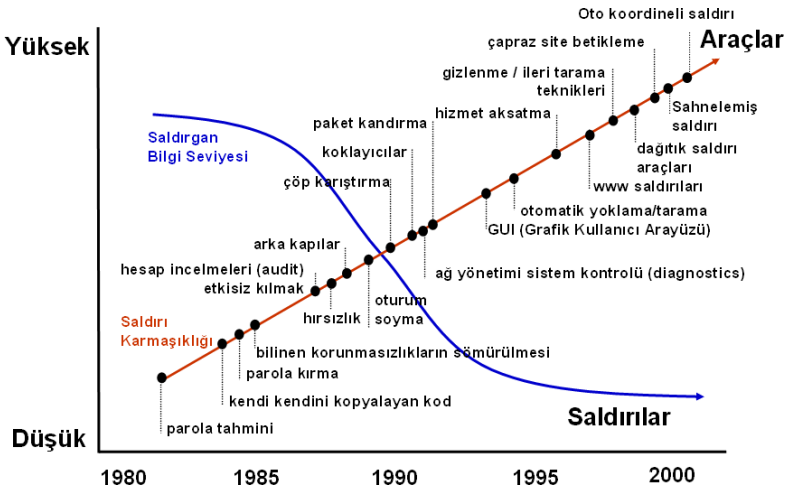
Bilginin çok önemli bir varlık olması, ona sahip olma ile ilgili bazı konuların düzenlenmesi ve yeni şartların getirdiği özelliklere göre ayarlanmasını gerekmektedir. Bilgi, en basit benzetme ile para gibi bir metadır. Kişiler, kurumlar ve ülkeler için bilgi, elde edilmesi zor, aynı zamanda elde tutulması da zor bir metadır. Entelektüel mülk (intellectual capital, property) olarak tanımlanan bu meta, bir kurumun bilgi ve özbilgi varlığıdır (25). Bu mülkün korunması, hayati bir önem arz etmektedir. Bu korunma, hem bilgi kullanımındaki karmaşayı, yozlaşmayı ve kötüye kullanımı önleyeceği gibi hem de bilgiyi bir çaba göstererek elde eden tüzel veya gerçek kişilerin haklarının korunmasını da sağlayacaktır. Bu sayede firmalar, çetin rekabet ortamında, sahip oldukları fark yaratan ve aynı zamanda koruyabildikleri entelektüel mülk ile avantajlı konumlarını koruyabilmektedirler (26). İşte bu yüzden patent, telif hakkı ve ticari marka gibi haklar, entelektüel mülkü korumak amacıyla oluşturulmuştur (27). Fakat bilginin korunması, daha doğrusu bilginin güvenliği, özellikle elektronik ortamda çok daha kapsamlı bir konudur.

Bilginin değerinin olması, bu değeri elde etmek için emek ve zamanın harcanması ve kazanılan bilginin fark yaratması nedeniyle bilgi, korunması gereken bir varlık olarak görülmektedir (28). Bu açıdan bilginin korunmasına yönelik olarak, bilgi güvenliği, dünya gündeminde olan ve bundan sonra daha da önemini arttırarak devam eden bir konu olarak karşımıza çıkmaya devam edecektir.

3. BİLGİ VE BİLGİSAYAR GÜVENLİĞİ

Bilgi güvenliği, elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür. Bunun sağlanması için, uygun güvenlik politikasının belirlenmeli ve uygulanmalıdır. Bu politikalar, faaliyetlerin sorgulanması, erişimlerin izlenmesi, değişikliklerin kayıtlarının tutulup değerlendirilmesi, silme işlemlerinin sınırlandırılması gibi bazı kullanım şekillerine indirgenebilmektedir. Bilgi güvenliği daha genel anlamda, güvenlik konularını detaylı olarak ele alan "güvenlik mühendisliği"nin bir alt alanı olarak görülmektedir.

Bilgi ve bilgisayar güvenliğinde, karşı taraf, kötü niyetli olarak nitelendirilen kişiler (korsanlar veya saldırganlar) ve yaptıkları saldırılardır. Var olan bilgi ve



Şekil 2. Saldırı Karmaşıklığı ile Saldırgan Teknik Bilgisi (31).

bilgisayar güvenliği sistemini aşmak veya atlatmak, zafiyete uğratmak, kişileri doğrudan veya dolaylı olarak zarara uğratmak, sistemlere zarar vermek, sistemlerin işleyişini aksattırmak, durdurmak, çökertmek veya yıkmak gibi kötü amaçlarla bilgisayar sistemleri ile ilgili yapılan girişimler saldırı veya atak olarak adlandırılmaktadır. Saldırganlar, amaçlarına ulaşmak için çok farklı teknikler içeren saldırılar gerçekleştirmektedirler. Saldırı türlerinin bilinmesi, doğru bir şekilde analiz edilmesi ve gereken önlemlerin belirlenmesi, bilgi güvenliği için büyük bir önem arz etmektedir.

Bilgi güvenliği, "bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önleme olarak" tanımlanır. Bilgisayar teknolojilerinde güvenliğin amacı ise "kişi ve kurumların bu teknolojilerini kullanırken karşılaşabilecekleri tehdit ve tehlikelerin analizlerinin yapılarak gerekli önlemlerin önceden alınmasıdır".

Özellikle ülkemizde, ne yazık ki, birçok kurum ve kuruluşun ve her seviyeden bilgisayar kullanıcısının çoğunlukla bilgi ve bilgisayar sistemlerine ve bilgi güvenliğine bakış açısının yeterli seviyede olmadığı tespit edilmiştir (4, 29). Kasım-Aralık 2004 tarihleri arasında yapılan bir araştırmada, 800 civarında ADSL abonesi ve 500'ün üzerinde şirketin güvenlik sisteminin denetlenmesi ile gerçekleştirilen "Türkiye İnternet Güvenliği Araştırması" sonuçlarına göre şirketlerin %27'sinin bilişim sistemlerinde çok yüksek seviyede açıklar gözlenmiş, ADSL abonelerinin %72'sinin güvenlik duvarı yapılandırmalarında ciddi açıklar görülmüştür (4).

Türkiye Bilimsel ve Teknik Araştırma Kurumu TÜBİTAK'ın Yönlendirme Kurulu, yapmış olduğu "Bilim ve Teknoloji Strateji Belgesi" çalışmasında (30), ülkemizin 2023 yılına ışık tutacak bilim, teknoloji ve yenilik ufkunu belirlerken, bilgi toplumuna geçiş için, teknolojik altyapının güçlendirilmesi hedefi doğrultusunda yapılması gerekenler arasında bilgi güvenliği konusunun göz ardı edilmeyip çeşitli stratejilerin belirlenmiş olması ümit vericidir.

Şekil 2'de gösterildiği gibi, saldırılar zamanla ve gelişen teknoloji ile oldukça farklılıklar göstermektedir. Parola tahmin etme ya da işyerlerinde kâğıt notların atıldığı çöpleri karıştırma gibi basit saldırılar, günümüzde artık yerini daha kapsamlı olan çapraz site betikleme (cross site scripting), oto koordineli (auto coordinated), dağıtık (distributed) ve sahnelenmiş (staged) saldırılara bırakmıştır. Saldırılar veya saldırılarda kullanılan araçlar, teknik açıdan gittikçe karmaşıklaşırken, bu saldırıyı yürütecek saldırganın ihtiyaç duyduğu bilginin seviyesi de gittikçe azalmaktadır. Bu durum saldırı ve saldırgan sayısını, saldırılar sonucunda oluşacak zararları artırırken, saldırıyı önlemek için yapılması gerekenleri de zorlaştırmaktadır.

Son günlerde, bilgi sistemlerinde bilgi güvenliği konusunda zafiyet oluşturan, virüsler, solucanlar, Truva atları, arka kapılar, mesaj sağanakları, kök kullanıcı takımları, telefon çeviriciler, korunmasızlık sömürücüleri, klavye dinleme sistemleri, tarayıcı soyma ve casus yazılımların yanında, reklâm, parazit, hırsız, püsküllü bela yazılım, tarayıcı yardımcı nesnesi, uzaktan yönetim aracı, ticari RAT, bot ağı, ağ taşkını, saldırgan ActiveX, Java ve betik, IRC ele geçirme savaşı, nuker, paketleyici, ciltçi, şifre yakalayıcılar-soyguncular, şifre kırıcılar, anahtar üreticiler, e-posta bombardımanı, kitle postacısı, web böcekleri, aldatmaca, sazan avlama, web sahtekârlığı-dolandırıcılığı, telefon kırma, port tarayıcılar, sondaj aracı, arama motoru soyguncusu, koklayıcı, kandırıcı, casus yazılım ve iz sürme çerezleri, turta, damlatıcı, savaş telefon çeviricileri ve tavşanlar adı altında ve her biri farklı amaçlara yönelik değişik yöntemler kullanan çok çeşitli kötücül yazılımın var olduğu da tespit edilmiştir (6).

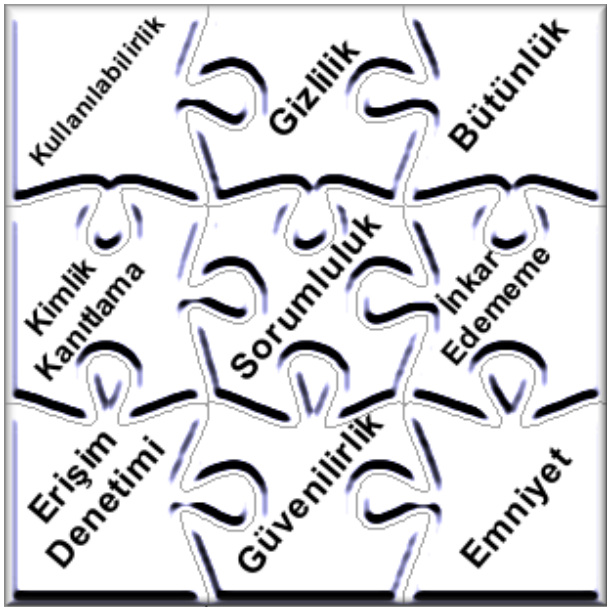
Bu saldırılar ve zafiyetler karşısında, bilgi güvenliğini sağlamak için bu güvenliği oluşturan unsurların belirlenmesi gereklidir. Bu unsurların yokluğu veya bu unsurlarda oluşabilecek zafiyetler, doğrudan oluşturulmak istenen güvenliğin etkinliğini belirleyecektir.

Bilgilerin, istenmeyen hasarlardan korunması için, en temel açıdan atılması gereken adımlar, güvenlik unsurlarının yerine getirilmesi ile sağlanmaktadır. Bu konu Bölüm 4'de ayrıntılı olarak incelenmiştir.

4. GÜVENLİK UNSURLARI

Gizlilik (confidentiality), bütünlük (integrity), kullanılabilirlik (availability), kimlik kanıtlama (authentication) ve inkâr edememe (non-repudiation) bilgi güvenliğinin en temel unsurlardır. Bunun dışında sorumluluk (accountability), erişim denetimi (access control), güvenilirlik (reliability) ve emniyet (safety) etkenleri de bilgi güvenliğini destekleyen unsurlardır. Bu unsurların tamamının gerçekleştirilmesiyle ancak bilgi güvenliği tam olarak sağlanabilecektir. Şekil 3'den de görülebileceği gibi, bu unsurların bir veya birkaçının eksikliği, güvenlik boyutunda aksamalara sebebiyet verebilecektir. Bu unsurların birbirini tamamlayıcı unsurlar olduğu hiçbir zaman unutulmamalıdır.

TSE-17799 "Bilgi Güvenliği Yönetim Standardı" belgesinde, gizlilik, "bilginin sadece erişim hakkı olan yetkili kişilerce erişilebilir olmasının temini" olarak; bütünlük, "bilgi ve bilgi işleme yöntemleri ile veri içeriğinin değişmediğinin doğrulanması" olarak; kullanılabilirlik, "yetkili kullanıcıların ihtiyaç duyulduğunda bilgi ve ilişkili varlıklara erişme hakkının olmasının temini" olarak tanımlanmıştır (32). Kimlik kanıtlama, geçerli kullanıcı ve işlemlerin tanınması ve doğrulanması ile bir kullanıcının veya prosesin hangi sistem kaynaklarına erişme hakkının olduğunun belirlenmesi sürecidir. İnkâr edememe, bir bilgiyi alan veya gönderen tarafların, o bilgiyi aldığını veya gönderdiğini inkâr edememesini sağlama işlemidir.



Şekil 3. Güvenlik unsurları

Sorumluluk, belirli bir eylemin yapılmasından, kimin veya neyin sorumlu olduğunu belirleme yeteneğidir. Tipik olarak etkinliklerin kayıtlarını tutmak için bir kayıt tutma (logging) sistemine ve bu kayıtları araştıracak bir hesap inceleme (auditing) sistemine ihtiyaç duyar. Erişim denetimi, bir kaynağa erişmek için belirli izinlerin verilmesi veya alınması olarak tanımlanabilir. Güvenilirlik, bir bilgisayarın, bir bilginin veya iletişim sisteminin şartnamesine, tasarım gereksinimlerine sürekli ve kesin bir şekilde uyarak çalışması ve bunu çok güvenli bir şekilde yapabilme yeteneğidir. Emniyet, bir bilgisayar sisteminin veya yazılımın işlevsel ortamına gömülü olduğunda, kendisi veya gömülü olduğu ortam için istenmeyen potansiyel veya bilfiil tehlike oluşturacak etkinlik veya olayları önleme tedbirlerini içermektedir.

Telekomünikasyon Kurumu tarafından 15 Ocak 2004 tarih ve 5070 sayılı "Elektronik İmza Kanunu"na temel alınarak hazırlanmış olan "Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik"te bilgilerin gizliliği ve korunması ile ilgili gerekli hususların sunulması ise bilgi ve bilgisayar güvenliği konusunda dünya ülkeleriyle beraber gerekli adımları zamanında atıyor olmamız açısından, bir diğer olumlu adım olarak değerlendirilmektedir (5).

Güvenlik unsurların gereklerini yerine getirmek, güvenlik süreçlerini ve politikalarını oluşturma ve uygulamayla başarıya ulaşacaktır. Güvenlik süreçleri Bölüm 5'de incelenmişte detaylı olarak incelenmiştir.

5. GÜVENLİK SÜREÇLERİ

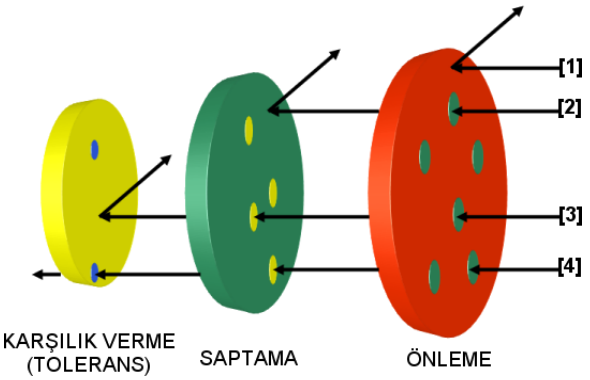
Bilgi güvenliği çerçevesinde kurulacak güvenlik sistemi altyapısının ve politikasının doğru bir şekilde belirlenebilmesi için, korunmak istenen bilginin değerlendirilmesi ve güvenlik yönetiminin doğru ve eksiksiz bir şekilde yapılması gerekir. Güvenlik yönetimi, bilgi ve bilgisayar güvenliğini olumsuz yönde etkileyecek faktörlerinin belirlenmesi, ölçülmesi ve en alt düzeye indirilmesi sürecidir.

ISO Rehber 73'e göre risk, bir olayın ve bu olayın sonucunun olasılıklarının birleşimi olarak tanımlanmaktadır. Risk yönetiminin bir adımı olan risk değerlendirmesi, risklerin tanımlandığı ve tanımlanan bu risklerin etkilerinin ve önceliklerinin belirlendiği bir süreçtir. Risk yönetimi, kabul edilebilir düzeyde bir riskin belirlenmesi, hali hazırdaki riskin değerlendirilmesi, bu riskin kabul edilebilir düzeye indirilebilmesi için gerekli görülen adımların atılması ve bu risk düzeyinin sürdürülmesidir. Bilgi ve diğer varlıklar, bu varlıklara yönelik tehditler, var olan sistemde bulunan korunmasızlıklar ve güvenlik sistem denetimleri, mevcut riski tayin eden bileşenlerdir. Korunması gereken bilgi ya da varlıkların belirlenmesi; bu varlıkların kuruluşlar açısından ne kadar değerli olduğunun saptanması; bu varlıkların başına gelebilecek bilinen ve muhtemel tehditlerden hangilerinin önlenmeye çalışılacağının ortaya konulması; muhtemel kayıpların nasıl cereyan edebileceğinin araştırılması; her bir varlığın maruz kalabileceği muhtemel tehditlerin boyutlarının tanımlanması; bu varlıklarda gerçekleşebilecek zararların boyutlarını ve ihtimallerini düşürmek için ilk planda yapılabileceklerin incelenmesi ve

ileriye yönelik tehditleri asgari seviyede tutmak için atılması gereken adımların planlanması, risk değerlendirmesinin belli başlı safhalarındandır (35).

Risk yönetimi sonucunda kurulacak ve yürütülecek güvenlik sisteminin maliyeti, dikkate alınması gereken bir başka önemli hususdur. Güvenlik sisteminin maliyeti, korunan bilginin değeri ve olası tehditlerin incelenmesiyle belirlenen risk ile sınırlı olmalıdır. %100 güvenliğin olmayacağı ilkesi ile beraber, bilgi güvenliğinin ideal yapılandırılması üç süreç ile gerçekleştirilir. Bu süreçler, önleme (prevention), saptama (detection) ve karşılık vermedir (response ya da reaction).

Şekil 4'de güvenlik süreçlerine bir örnek verilmiştir. Bu şekilde, 4 farklı saldırı [1]-[4] ile gösterilmiştir. Şekilden de açıkça görülebileceği gibi, [1] numaralı saldırı, hemen önleme safhasında engellenirken; [2], [3] ve [4] numaralı saldırılar bu safhada önlenememiştir. Önleme sürecini atlatan bu saldırılardan [2] numaralı saldırı, saptama aşamasında tespit edilip, bertaraf edilirken; [3] ve [4] numaralı saldırılar, saptama aşamasından da geçebilmiştir. Belirlenen tolerans ile tasarlanmış son aşama olan karşılık verme safhasında, [3] numaralı saldırı önlenirken; bütün aşamaları atlatıp geçen [4] numaralı saldırı, bütün güvenlik süreçlerini geçip, sisteme zarar vermiştir. Takip eden kısımda güvenlik süreçlerinin her biri, temel özellikleri ile açıklanmaktadır.



Şekil 4. Güvenlik süreçleri ve saldırılara tepkileri

Güvenlik süreçleri takip eden kısımda alt başlıklar halinde açıklanmaktadır.

Önleme

Önleme, güvenlik sistemlerinin en çok üzerinde durduğu ve çalıştığı süreçtir. Bir evin bahçesine çit çekmek, çelik kapı kullanmak gibi güncel hayatta kullanılan emniyet önlemleri gibi, bilgisayar sistemlerine yönelik tehdit ve saldırılara karşı, sistemin yalıtılmış olması için çeşitli önlemler geliştirilmektedir. Kişisel bilgisayar güvenliği ile ilgili, virüs tarama programlarının kurulu olması, bu programların ve işletim sistemi hizmet paketlerinin ve hata düzeltme ve güncellemelerinin düzenli aralıklarla yapılması, bilgisayarda şifre korumalı ekran koruyucu kullanılması, bilgisayar başından uzun süreliğine ayrı kalındığında sistemden çıkılması, kullanılan şifrelerin tahmininin zor olacak şekilde belirlenmesi, bu şifrelerin gizli tutulması ve belirli aralıklarla değiştirilmesi, disk paylaşımlarında dikkatli olunması, İnternet üzerinden indirilen veya e-posta ile gelen dosyalara dikkat edilmesi, önemli belgelerin parola ile korunması veya şifreli olarak saklanması, gizli veya önemli bilgilerin e-posta, güvenlik sertifikasız siteler gibi güvenli olmayan yollarla gönderilmemesi, kullanılmadığı zaman İnternet erişiminin kapatılması, önemli bilgi ve belgelerin düzenli aralıklarla yedeklerinin alınması gibi önlemler, basit gibi gözükebilecek ama hayat kurtaracak önlemlerden bazılarıdır.

Kurumsal ortamlarda bilgisayar güvenliğinde uygulanması gereken önleme adımları daha geniş ve karmaşıktır. Güvenlik ile ilgili uzmanlaşmış kişilerin çalıştığı bu tür sistemlerde, önleme ile ilgili yapılanlardan bazıları:

- işletim sistemi ve yazılımların servis paketlerinin ve güncellemelerin düzenli aralıklarla incelenmesi,
- kullanıcı haklarının asgari seviyede tutulması, kullanılmayan protokol, servis, bileşen ve proseslerin çalıştırılmaması,
- veri iletişiminde şifreleme tekniklerinin, korunmasızlık tarayıcıları, Sanal Özel Ağ (Virtual Private Network) kullanılması,
- Açık Anahtar Altyapısı (Public Key Infrastructure) ve e-imza kullanımı ile
- biyometrik tabanlı sistemlerin kullanımı

olarak sıralanabilirler.

Aslında önleme sürecinde belirlenen işleyiş mükemmel olabilseydi, daha sonraki süreçlere hiç ihtiyaç duyulmazdı. Yapılan bütün saldırılar en baştan önlenmiş olurdu. Fakat hiç bir güvenlik ürünü kusursuz veya eksiksiz değildir. Ayrıca, hemen hemen her gün, işletim sistemleri, İnternet servisleri, web teknolojileri ve güvenlik uygulamalarında çeşitli açıklar tespit edilmektedir. Bu açıdan bakıldığında saptama ve karşılık verme süreçlerini kullanmak şarttır.

Saptama

Güvenlik, sadece önleme ile sağlanabilecek bir mesele değildir. Örneğin bir müzede iyi bir korunmanın sağlanmış olması, müzenin çevresinin çitlerle çevrili olması, kapıların kapalı ve kilitli olması, o müzede geceleri bekçi kullanılmamasını gerektirmez. Aynı şekilde bilgisayar sistemlerinde de saldırı girişimlerini saptayacak yöntemlerin de kullanılması şarttır. Önleme, saldırıları güçleştiren (ama imkânsız kılmayan) veya saldırganların cesaretini kıran (ama yok etmeyen) bir engel inşa etmeyi sağlar. Saptama ve karşılık verme olmadan önlemenin ancak sınırlı bir faydası olabilir. Sadece önleme ile yetinilseydi, yapılan çoğu saldırıdan haberdar bile olunamazdı. Saptama ile daha önce bilinen veya yeni ortaya çıkmış saldırılar, rapor edilip, uygun cevaplar verebilir. Saptamada ilk ve en temel basamak, siste-

min bütün durumunun ve hareketinin izlenmesi ve bu bilgilerin kayıtlarının tutulmasıdır. Bu şekilde ayrıca, saldırı sonrası analiz için veri ve delil toplanmış olur. Güvenlik duvarları, saldırı tespit sistemleri (intrusion detection system), ağ trafiği izleyiciler, kapı (port) tarayıcılar, bal çanağı (honeypot) kullanımı, gerçek zamanlı koruma sağlayan karşı virüs ve casus yazılım araçları, dosya sağlama toplamı (checksum) kontrol programları ve ağ yoklayıcı (sniffer) algılayıcıları, saptama sürecinde kullanılan en başta gelen yöntemlerden bazılarıdır.

Karşılık Verme

Bekçiler, köpekler, güvenlik kameraları, algılayıcılarla donatılmış bir yerin, hırsızların dikkatini çekmesi gibi, gerçek zamanlı saptama sistemlerine sahip bilgisayar sistemleri de bilişim korsanları ve saldırganlara cazip gelir. Hızlı karşılık verme, bu saldırıları püskürtmek için güvenlik sistemini tamamlayan esaslı bir öğe olarak ortaya çıkmaktadır. Karşılık verme, önleme süreci ile baş edilemeyen ve saptama süreçleri ile belirlenmiş saldırı girişimlerini, mümkünse anında veya en kısa zamanda cevap verecek eylemlerin ifa edilmesi olarak tanımlanabilir. Saldırı tespit sistemleri, bu tespite cevap verecek birilerinin veya bir sistemin olması ile anlam kazanabilir. Aksi takdirde bu durum, hiç kimsenin duyup da önemsemediği bir araba alarmının getireceği faydadan öteye gitmez. Bu açıdan karşılık verme güvenlik sürecini tamamlayan önemli bir halkadır. Saldırı tam olarak önlenmese bile; sistemin normal durumuna dönmesine, saldırıya sebep olan nedenlerin belirlenmesine, gerektiği durumlarda saldırganın yakalanmasına, güvenlik sistemi açıklarının belirlenmesine ve önleme, saptama ve karşılık verme süreçlerinin yeniden düzenlenmesine olanak verir. Saldırı tespit edilince yapılması gereken işlerin, daha önceden iyi bir şekilde planlanması, bu sürecin etkin bir şekilde işlemesini ve zaman ve para kaybetmemeyi sağlayacaktır. Yıkım onarımı (disaster recovery), bu aşama için gerçekleştirilen ve en kötü durumu ele alan esaslı planların başında gelir.

6. SONUÇ VE DEĞERLENDİRMELER

Günümüzde bilişim teknolojilerinin yaygınlaşması ve günlük hayatımızda yapmış olduğumuz iş ve işlemlerin elektronik ortamlarda hızla yapılmaya başlanması, bilgi güvenliğinin sağlanmasını zorunlu hale getirmektedir. Bilgi güvenliğini sağlanabilmesi için, bilginin değerinin bilinmesi, yapılan iş ve işlemlerde bu çalışmada incelenen güvenlik unsurlarını, politikalarını ve süreçlerini uygulamak, büyük oranda karşılaşılacak sıkıntıları ve tehlikeleri azaltacak, işgücü, zaman ve parasal kayıpları önleyecek, Internet üzerinden gelebilecek zararlı yazılımları veya program parçacıklarına karşı kişisel ve kurumsal bilgi güvenliğinin sağlanmasında büyük katkılar sağlayacaktır.

Bilgi güvenliği konusunda zafiyetlerle karşılaşılmaması için, kişilerin ve kurumların alması gereken ve basitten en karmaşık yöntemlere kadar bir dizi önlemler vardır. Ancak, tüm önlemler alınmış dahi olsa, sürekli gelişen saldırı teknikleri yüzünden, hiç kimse ve hiç bir kuruluş kendini %100 güvende hissetmemelidir. Saldırıların elektronik ortamlardan kötü niyetli kişilerden gelebilmesinin yanı sıra, arkadaşlarımızdan ve tanıdığımız kişilerden de gelebilecek sosyal mühendislik altında incelenen tehditler de bulunmaktadır.

Genel olarak, bilgi ve bilgisayar sistemleri konusunda ne kadar önlem alınırsa alınsın, riskleri sıfıra indirgemenin çokta mümkün olmadığının farkında olunmasında fayda vardır. Alınması gereken en temel önlemler, risklere karşı sürekli uyanık olmak, bu çalışmada açıklanan süreçlerin meydana getirildiği güvenlik politikalarını etkin bir şekilde oluşturup kullanmak, oluşturulan süreçlerin başarımını sürekli olarak izlemek ve elde edilen sonuçlar ve yeni gelişmeler ışığında gerekli güncellemeleri yaparak saldırılardan etkilenme olasılığını en aza indirgemek olarak sıralanabilir.

Yüksek seviyede bir güvenlik için bu süreçlerin yanında, somut olarak kurumsal bilgi güvenliği standardı olan TSE 17799'de belirtilen hususların (33,34) bilinmesi ve uygulanması ile yüksek seviyede bir koruma sağlayan bir bilgi güvenliği modeli oluşturulmasına büyük katkılar sağlayacağı değerlendirilmektedir.

Literatür incelendiğinde, konuyla ilgili birçok çalışma mevcut olsa da "bilgi ve bilişim sistemleri güvenliğinin" akademik ortamlarda yeterince tartışılmadığı ve konuya gereken önemin fazlaca verilmediği tespit edilmiştir. Böyle bir çalışmanın, magazin ve ticari bilgilerin dışında bu konunun akademik gündeme taşınması açısından da önemli olacağı mütalaa edilmektedir.

İnceleme sonucunda, bilginin ve teknolojinin iç içe olduğu ve teknolojinin baş döndürücü bir hızla gelişen ve yayılan elektronik ortamları desteklemesi, her zaman yanı başımızda olacak bilgisayar korsanı gibi kötü niyetli kişilerin veya bu tür kişilerin yazdığı casus yazılımların, sistemlerin açığını bulma da, bu açıkları kullanıp sistemlere izinsiz erişmede ve sistemlere ve sistemi kullanan kişilere, kişisel veya kurumsal zarar vermede hemen hemen her yolu denemeye çalıştıkları tespit edilmiştir. Bu saldırı ve tehditlere karşı tedbir alınabilmesi için, bu tür yazılımların ve kullanılan yöntemlerin sürekli olarak incelenmesi gerektiği elde edilen bulgular arasındadır.

Dünyada ve ülkemizde bilgi güvenliğine yönelik en önemli tehditlerden olan kötücül ve casus yazılımların, yaygın olarak kullanımda olduğu fakat kullanıcıların bu tür saldırı ve tehditlerinden çoğunlukla haberdar olmadığı anlaşılmıştır. Her hangi bir zararla karşılaşılmaması için, konuya gereken önemin verilmesi, bilgi birikiminin arttırılması, hassasiyet gösterilmesi ve gereken önlemlerin alınması ve farkındalık oluşturulması gerekmektedir.

Bölüm 3'de de açıklandığı gibi, sistemlere yapılabilecek saldırıların boyutlarının hızla arttığı günümüzde, teknolojik olarak korunma teknikleri artarken tehditlerde de artış olduğu, kötücül yazılımların teknolojik yeniliklere göre şekil değiştirdiği, insanların zaaflarından çoğunlukla faydalanıldığı, kullanıcıların akıllarına bile gelmeyecek birçok masumane yaklaşımların kullanıldığı, bilgisayar teknolojilerinde var olan açıklardan faydalanmanın yanında genelde göz ardı edilen sosyal mühendislik yaklaşımlarına da çok sık başvurulduğu, web teknolojilerinin, bu yazılımların çok kısa sürede ve kolayca yayılmasına ve yaygınlaşmasına olanak verdiği, kullanıcıların bilgisayar kullanma alışkanlıklarından, internet gezinme geçmişini incelemeye, mevcut port açıklarını tespit etmeye, işletim sistemi ve program korunmasızlık açıklarından yararlanmaya, önemli kritik ve kişisel bilgileri kötü niyetli kişilere göndermeye, bilgisayar sisteminde fark edilmeden ve iz bırakmadan çalışmaya, kullanıcı bilgisizlik ve zaaflarından faydalanmaya, kullanılan şifrelerin kırılmasına ve yakalanmasına, kendilerini farklı yazılımlar içerisinde saklayarak kötücül ve casus yazılım tarayıcıları ve koruma programlarını atlatmaya, hatta bu yazılımları devre dışı bırakmaya, bant genişliği ve işlemci gibi sistem kaynaklarını fark ettirmeden dışarının kullanımına açmaya kadar birçok yöntem kullandıkları ve bilgi ve bilgisayar güvenliği konusunda güvenilir sistemler oluşturmak için, daha öncede vurgulandığı gibi, bilgi güvenliği unsurlarının yerine getirilmesi, ilgili süreçlerin bilinmesi, uygulanması ve denetlenmesi, belirli politikaların uygulanması gerekmektedir.

e-Dönüşüm Türkiye 2005 Eylem Planında (29), 5 ve 33 no'lu maddelerinde de bilgi güvenliğine önem verilmesi, çok olumlu bir gelişme olarak değerlendirilmektedir. Bu eylemler;

5 no'lu eylem "Başta kritik bilgileri kullanan merkezi kurumlar olmak üzere, kamu kuruluşlarının sahip olduğu mevcut sistemler analiz edilerek bilgi güvenliği konusunda izlenecek politikalar ve alınacak önlemlere ilişkin öneriler geliştirilecektir." ve

33 no'lu eylem "Kamu bilgi sistemlerinin acil durum yönetimi ihtiyaçları tespit edilerek çözüm önerileri geliştirilecektir." olarak verilmektedir. Bu eylemlerin acil olarak tamamlanmasının, bilgi ve bilgi sistemleri güvenliğine katkılar sağlayacağı değerlendirilmektedir.

Sonuç olarak, Elektronik İmza Kanunu'nun Ocak 2005'den itibaren elektronik ortamlarda atılacak imzalarında hukuken de geçerli olması, bilgi ve özbilgi güvenliğini sağlama açısından çok önemli bir gelişmedir. Dünya ülkeleriyle beraber, gerekli adımların ülkemizde de zamanında atılmış olması, elektronik ortamlara güveni kısa sürede arttıracağı ve bilgi güvenliğinin çok yüksek düzeyde sağlanmasına büyük katkılar sağlayacağı değerlendirilmektedir.

Güvenliğin statik değil dinamik bir sürece sahip olduğu, koruma ve sağlamlaştırma ile başladığını, bir hazırlık işlemine ihtiyaç duyulduğu, saldırıların tespit edilmesinden sonra hızlıca müdahale edilmesi gerektiği ve sistemde her zaman iyileştirme yapılması gerektiği unutulmamalı, Carnegie Mellon Üniversitesi tarafından 2001 yılında literatüre tanıtılmış olan "güvenlik yaşam döngüsü" mutlaka uygulanmalıdır. Bu süreçlerin planla, yap, denetle ve iyileştir kapalı döngüsü içerisinde her zaman takip edilmesi ve bu işlemleri belirtilen sıra içerisinde sürekli yapılması gerektiği unutulmamalıdır.

Bilgisayar ve İnternet kullanımının her geçen gün arttığı ve hayatımızı gün geçtikçe daha da fazla etkileyen, değiştiren ve yönlendiren sanal dünyanın getirilerinin, faydalarının, kazanımlarının ve olumlu yönlerinin yanında, eğer dikkat edilmez ise kişisel ve kurumsal işleyişi sekteye uğratacağı, verimliliği düşüreceği, büyük boyutlarda zararlara yol açacağı, hatta çok ciddi yerel veya küresel bir kaosa neden olabileceği de dikkate alınmalıdır.

7. TEŞEKKÜR

Bu çalışma, Gazi Üniversitesi BAP "06/2005–44 Bilgisayar Güvenliği Yazılımı Geliştirme Projesi" altında maddi olarak desteklenmektedir. Yazarlar, Gazi Üniversitesine desteklerinden dolayı teşekkür eder.

8. KAYNAKÇA

1 Internet Usage Statistics - The Big Picture, http://www.internetworldstats.com/stats.htm (2005).

2. Devlet İstatistik Enstitüsü, "Hanehalkı Bilişim Teknolojileri Kullanımı Araştırması Sonuçları, 2005", DIE Haber Bülteni, 16 Kasım 2005, Sayı 179.

3. Şağıroğlu, Ş., Etkin Bilişim Teknolojileri Kullanımı, Ufuk Kitabevi, Haziran 2001.

4. Koç.net Haberleşme Teknolojileri ve İletişim Hizmetleri A.Ş., "Türkiye İnternet Güvenliği Araştırma Sonuçları 2004", Koç.net, İstanbul, 1-9, 2004.

5. Sağıroğlu, Ş. ve Alkan, M., Her Yönüyle E-İmza, Grafiker, Ankara, Ekim 2005.

6. Canbek, G., Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme, Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, 10-11, Eylül 2005.

7. Canbek, G., Şağıroğlu, Ş., "Şifre Bilimi Tarihine Genel Bakış - I", Türk Telekom Dergisi, Mayıs (sayfa 34-42), 2005.

8. Canbek, G., Şağıroğlu, Ş., "Şifre Bilimi Tarihine Genel Bakış – II and III", Türk Telekom Dergisi, Haziran (sayfa 36-44), Temmuz (sayfa 56-58), 2005.

9. Canbek, G., Şağıroğlu, Ş., "Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma", Gazi Mühendislik Mimarlık Dergisi, Basımda, Temmuz 2006.

10. Housman, E. M., "The Nature of Information", Bulletin of the American Society for Information Science, 26 (4): (April/May 2000).

11. Schuler, A. J., "How to Build Wisdom and Prosper in an "Information Age"", "What's Up, Doc?" e-Newsletter, 3 (6): 5-7 (June 2003).

12. Tiwana, A., Knowledge Management Toolkit, The: Orchestrating IT, Strategy, and Knowledge Platforms, Prentice Hall PTR, 2nd Edition, 35-40, 2002.

13. "Data, Information, Knowledge and Knowledge Management", The OR (Operational Research) Society, http://www.theorsociety.com/about/topic/projects/notorious/2_2_Data_Info.htm (2005).

14. Courtney, J. F., Inquiring Organizations - Moving from Knowledge Management to Wisdom, Idea Group Inc (IGI), Londra, İngiltere, 91-92, 2005.

15. Montano, B., Innovations of Knowledge Management, Idea Group Inc (IGI), Londra, İngiltere, 302-303, 2004.

16. Grover, V., Davenport, T. H., "General Perspectives on Knowledge Management: Fostering a Research Agenda", Journal of Management Information Systems, 18 (1), 5-21, 2001.

17. "Euclid", Encyclopedia Britannica from Encyclopedia Britannica Premium Service. http://www.britannica.com/eb/article?tocId=2176 (2005).

18. OECD, Knowledge Management in the Learning Society, Paris, 14-15, 2000.

19. Awad, E. M., Ghaziri, H. M., Knowledge Management, Upper Saddle River, NJ, Pearson Education Inc., 40-41, 2004.

20. Kirrane, D.E., "Getting Wise to Knowledge Management", Association Management, 51 (8), 31-38, 1999.

21. Nagurney, A., Dong, J. and Mokhtarian, P.L. "Multicriteria Network Equilibrium Modeling with Variable Weights for Decision-Making in the Information Age with Applications to Telecommuting and Teleshopping", Journal of Economic Dynamics & Control, 1629-1650, 2002.

22. Sullivan, D., "Searches Per Day", http://searchenginewatch.com/reports/article.php/2156461 (2005).

23. Lyman, P., Varian, H., "How Much Information 2003?", School of Information Management and Systems, University of California at Berkeley.

24. Wang, R., Kon, H., Madnick, S., "Data Quality Requirements Analysis and Modelling", Ninth International Conference of Data Engineering, Vienna, Austria, 1993.

25. Kuusisto, R., Helokunnas, T., Ahvenainen, S, "Intellectual Capital and Time in information Superiority", Proceedings of the 2nd European Conference on Information Warfare and Security, 201-207, 2003.

26. Tipton, H. F., Krause, M., Information Security Management Handbook, CRC Pres, Danvers, A.B.D., 1475-1476, 2003.

27. Bouchoux, D. E., Protecting Your Company's Intellectual Property, AMACOM Div American Mgmt Assn, Jan 1, New York, A.B.D., 10-11, 2001.

28. Brykczynski, B., Small, B., "Securing Your Organization's Information Assets", CROSSTALK The Journal of Defense Software Engineering, 16 (5): 12-16, May 2003.

29. Kesmez, N., "Kişisel Verilerin Korunması Kanunu (Taslak)", Türkiye Bilişim Şurası, 2002, http://bilisimsurasi.org.tr/dosyalar/42.doc (2005).

30. Türkiye Bilimsel ve Teknik Araştırma Kurumu, "Ulusal Bilim ve Teknoloji Politikaları, 2003-2023 Strateji Belgesi", Versiyon 19 (2 Kasım 2004) TÜBİTAK, Ankara, 1-137, 2004.

31. Allen, J., The CERT® Guide to System and Network Security Practices, Addison-Wesley, 2001.

32. International Organization for Standardization, "Information technology -- Code of practice for information security management", ISO-17799, ISO, 2000.

33. TS ISO/IEC 17799, Bilgi Teknolojisi - Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri, Türk Standartları Enstitüsü, 11.11.2002, https://www.tse.org.tr/turkish/abone/StandardDetay.asp?STDNO=31987&sira=0 (2006).

34. TS 17799-2, Bilgi güvenliği yönetim sistemleri – Özellikler ve kullanım kılavuzu, Türk Standartları Enstitüsü, 17.02.2005, https://www.tse.org.tr/turkish/abone/StandardDetay.asp?STDNO=53846&sira=0 (2006).

35. Jones, A., Ashenden, D., Risk Management for Computer Security, First Edition: Protecting Your Network & Information Assets, Elsevier, 2005.