Bilgi Merkezlerinde Bilgi Güvenliği Farkındalığı: Ankara'daki Üniversite Kütüphaneleri Örneği

Awareness of Information Security in Information Centers: Sample of Academic Libraries in Ankara

Semanur ÖZTEMİZ[*] ve Bülent YILMAZ[**]

Öz

Kurumsal düzeyde bilgi güvenliğine ilişkin bilinç ya da farkındalığın artırılması kurumsal faaliyetlerin amaca uygun ve sorunsuz bir şekilde yürütülmesinde büyük önem taşımaktadır. Bu araştırma, toplumsal birer kurum olan bilgi merkezlerinde bilgi güvenliği farkındalığını ortaya koymak amacıyla yapılmıştır. Nitel yönteme dayalı olarak yapılan araştırma, Ankara'da bulunan toplam 14 üniversite kütüphanesi üzerinde gerçekleştirilmiştir. Araştırma verileri kütüphane ve dokümantasyon daire başkanları ya da yardımcıları ile yüz yüze ya da telefonla yapılan görüşmelerden elde edilmiştir. Araştırma bulguları doğrultusunda, kütüphanelerin büyük bir kısmında bilgi güvenliğinin sağlanması gerekli ve önemli bulunurken, bilgi güvenliğinin ne olduğu ve ne tür uygulamaları içerdiği hususunda yeterince bilgi sahibi olunmadığı, hali hazırda yürütülen güvenlik uygulamalarının bilgi işlem daire başkanlıkları tarafından gerçekleştirildiği sonucuna ulaşılmıştır.

Anahtar sözcükler: *Bilgi güveliği farkındalığı, Kütüphaneler, Ankara*

Abstract

Enhancing consciousness or awareness, regarding information security on the institutional level, has a great importance on carrying out institutional activities in purpose and without any problem. This study is carried out in order to put forth information security awareness in information centers, which are also public institutions. The study, which is based on a qualitative method, is performed over 14 university libraries in Ankara. Data were gathered from the interviews in person or by phone. In accordance with the study findings, it's found that information security is essential and required to be maintained in most of the libraries however there is lack of adequate information on the definition of information security and the applications it covers. Therefore it's concluded that currently ongoing applications have been carried out by information processing departments.

Keywords: *Awareness of information security, Libraries, Ankara*

* Arş.Gör.; Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, Beytepe, Ankara. (scaliskan@hacettepe.edu.tr)

** Prof.Dr.; Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü, Beytepe, Ankara. (byilmaz@hacettepe.edu.tr)

Giriş

İçinde bulunduğumuz döneme "bilgi toplumu/çağı" olarak adını veren bilgi olgusu, aynı zamanda çeşitli boyutlarıyla ele alınabilecek bir sorunsal durumuna gelmiştir.19. yüzyılın ikinci yarısından itibaren yarı iletkenlerin bilgisayara dayalı teknolojilerle birleşmesi, sayısı her geçen gün artan yeni iletişim araçlarının geliştirilmesine ortam hazırlamıştır (Atabek,2001,s.59). Çeşidi ve miktarı her geçen gün artan ve hayatın hemen her alanında pratik çözümler sunan bilgi teknolojileri, sağladıkları pek çok yararla birlikte kimi zaman bir saldırı aracı, kimi zaman ise söz konusu saldırılara maruz kalan bir hedef niteliği taşımaktadır (Civelek, 2011, s.2; Eminağaoğlu ve Gökşen, 2009, s.2; Pro-G,2003, s.5-6; Wooding, Anhal ve Valeri, 2003, s.3). 2008 yılında yapılan bir araştırmaya göre ülkemiz, siber güvenlik saldırılarına uğrama sıralamasında dünya genelinde 9. sırada yer almakta ve saldırılar her yıl bir öncekinin iki katı oranda artarak devam etmektedir (Eminağaoğlu ve Gökşen, 2009, s.3-5).

Bilgi güvenliği ile ilgili teknolojik çözümler, standartlar ve birtakım yasal düzenlemeler olmakla birlikte, güvenlik açıklarının ve bilişim saldırılarının her geçen gün artması, sorunun yalnızca teknik yöntemlerle çözümlenebileceği varsayımını zayıflatmaktadır (Şahinaslan, Kandemir ve Şahinaslan, 2009, s.190). Bilgi güvenliğine dayalı problemlerin yalnızca teknik yöntemlerle çözümlenebileceği düşüncesi, bilgi güvenliğinin sağlanmasında belki de en önemli unsur olan insan faktörünün göz ardı edilmesine neden olmaktadır (Boujettif ve Wang, 2010, s.1; ISO, 2005). Oysa güvenlik açığı yazılım ya da donanıma dayalı olmaktan çok insan faktörüne bağlı olarak ortaya çıkmaktadır (Albrechtsen, 2007, s.277; ENISA, 2006, s.7). İnsan faktörünü aşan bir saldırganın antivirüs yazılımlarını, güvenlik duvarlarını ya da saldırıları rapor eden sistemleri aşması daha kolay olmaktadır (Şahinaslan, Kandemir ve Şahinaslan, 2009, s.3). Bazı araştırmalar güvenlik risklerinin indirgenmesinde belki de en etkili çözümün insan kaynaklı hataların giderilmesi ile mümkün olduğunu, bunun ise büyük ölçüde bilgi güvenliği bilinci yaratma ile gerçekleşebileceğini ortaya koymaktadır (Al Awadi ve Renaud, 2007, s.3; Albrechtsen, 2007, s.276; Al-Shehri, 2012, s.61; Bogart, 2012, s.3).

Bilgi Güvenliği Nedir?

Güvenliğinin sağlanması beklenen bilgi; fiziksel bir ortama kaydedilmiş, düzenlenebilen, saklanabilen herhangi bir iletişim aracıyla başkalarına iletilebilen anlamlı veriler topluluğudur (Dura ve Atik, 2002, s.114). Bilgi teknolojilerine dayalı uygulamalar sağladığı pek çok yararla birlikte gerekli güvenlik önlemleri alınmadığı takdirde kurumları zarara uğratabilmektedir (Eminağaoğlu ve Gökşen, 2009, s.2).

Bilgi güvenliği, kurumsal varlıklar arasında belki de en önemli yere sahip olan bilginin tahribat, silinme, bozulma gibi zarar verici unsurlara ve olası saldırılara karşı korunmasını sağlayan birtakım uygulamaları kapsamaktadır (Önel ve Dinçkan, 2007, s.6). Bilgi güvenliği, bilginin yetkisiz kişilerce kullanımının önlenmesi, doğruluk ve

bütünlüğünün korunması ve yetkisi olan bireyler tarafından erişilmesini sağlamak şeklinde tanımlanmaktadır (Canbek ve Sağıroğlu, 2006, s.169; Marks, 2007, s.50). Bilgi güvenliği kimi zaman bilgisayar güvenliği gibi algılansa da bilgisayar güvenliği bilgi güvenliğinin kısmi bir parçasını ifade etmektedir (Newby, 2002, s.1). Kurumsal düzeyde bilgi güvenliği ise kurumun ortaya koyduğu ürün ya da hizmetin devamlılığını sağlamak amacıyla kurumsal bilginin olası tehlikelere karşı korunması anlamına gelmektedir (Bensghir, 2008). Bilgi güvenliğinikurumsal bilgi kaynaklarını olası tehditlere karşı korumak şeklinde tanımlayan Qureshi (2011, s.3) söz konusu tehditlerin insan ya da doğa kaynaklı (yangın, sel, deprem vb.) olabileceğini öne sürmektedir. Yapılan pek çok çalışmada tehditlerin kaynağına göre kurum içi ve kurum dışı olmak üzere ikiye ayrıldığını vurgulayan Al Awadi ve Renaud (2007, s.3) kurum içi tehditlerin yanlış ya da hatalı kullanım, yazılım ya da donanım hırsızlığı, mevcut sistemlerle uyumsuz donanım araçları kullanımı, lisansı olmayan yazılımların kullanımı gibi nedenlerle; kurum dışı tehditlerin ise virüsler, yığın (spam) iletiler, saldırganlar (hacker, sosyal mühendis gibi) ya da doğal afetler gibi nedenlerle ortaya çıktığını ifade etmektedirler.

Bilgi güvenliğinin üç temel ilkesi, başka bir ifadeyle bilginin sürekli korunmasını gerektiren birtakım nitelikleri bulunmaktadır (Şahinaslan, Kandemir ve Şhinaslan, 2009, s.191). Söz konusu nitelik ya da ilkelerden biri olan gizlilik; bilginin yetkisi olmayan kişilerce erişilemez hale getirilmesini sağlamaya yönelik uygulamaları kapsar (Önel ve Dinçkan, 2007, s.6; Şahinaslan, Kandemir ve Şahinaslan, 2009, s.191). Ancak saldırganlar kullandıkları birtakım yöntemlerle yetkileri olmadığı halde bilgilere erişebilmekte ve gizlilik prensibini ihlal etmektedirler. Şifrelerin ele geçirme, çalma ya da tahmin yöntemleriyle kırılması, alıcı ve gönderici arasındaki iletişimin deşifre edilmesi gizlilik ilkesine aykırı davranışlar kapsamında değerlendirilir (Canbek ve Sağıroğlu, 2006, s.169; Pro-G, 2003, s.8). Bütünlük ilkesi göndericiden alıcıya iletilen bilginin değiştirilmeden ya da bozulmadan alıcıya ulaşmasını sağlamaya yönelik uygulamaları içerir (Canbek ve Sağıroğlu, 2006, s.169; Önel ve Dinçkan, 2007, s.6; Pro-G, 2003, s.9). Erişilebilirlik ya da süreklilik ilkesi ise sistemin kurum içi ve dışı kimselerce zarar verilmeden kullanılmasını ve sürekliliğinin korunmasını sağlayan uygulamaları kapsar. Süreklilik prensibi ile sistem erişim izni olan kullanıcılar tarafından güvenilir bir şekilde erişilebilir (Canbek ve Sağıroğlu, 2006, s.169; Pro-G, 2003, s.10).

Bilgi güvenliği oldukça kapsamlı ve karmaşık bir süreci kapsar (Wright ve Kakalık, 2007, s.187). Bilgi güvenliğinin sağlanması üç temel sürecin bütünsel bir şekilde gerçekleşmesi ile yakından ilgilidir. Bunlardan biri doğru plan, strateji ve politikalarla doğru bilgi güvenliği yönetimi uygulamalarını kapsayan yönetsel süreç, ikincisi şifreleme, güvenlik duvarları, anti virüs yazılımları, yedekleme, denetim gibi teknik içerikli çözümleri kapsayan teknolojik önlem süreci, ve son olarak kullanıcıların eğitim yoluyla bilgi güvenliği bilinci kazanmalarını sağlayan eğitim ve farkındalık sürecidir (Pro-G, 2003, s.16-19).

Kurumlar İçin Bilgi Güvenliği Farkındalığı ve Önemi

Ağ kaynaklarının kurumsal amaçlar dışında kullanımı ve bunun neden olduğu verimlilik kaybı, zararlı yazılımlara maruz kalmak, uygunsuz içerikte siteleri ziyaret etmenin kurum itibarını zedeleyici ve yasal yükümlülükler gerektiren sonuçlar doğurması güvenlik açıklarının sebep olduğu sorunlardan yalnızca birkaçıdır (Eskiyörük, 2008, s.6). Bilgi güvenliği farkındalığı yaratmanın temel amaçlarından biri kurumsal bilgi varlıklarının yanlış kullanımından kaynaklı riskleri en aza indirgemek, sistem kullanımında karşılaşılması muhtemel sorunlardan haberdar olarak olası çözüm yolları geliştirmek, kurumun genel güvenlik politikasına uyum sağlayarak katkıda bulunmaktır (Şahinaslan, Kandemir ve Şahinaslan, 2009, s.3).

Bilgi güvenliği farkındalığı, bilgi güvenliğini riske atan faktörlerden ve söz konusu faktörlere karşı ne tür önlemler alınabileceğini kapsayan güvenlik politikalarından haberdar olunması şeklinde tanımlanabilir (Şahinaslan, Kandemir ve Şahinaslan, 2009, s.189). Siponen (2001, s.26), bilgi güvenliği farkındalığını sağlık durumu ile örneklendirmeye çalışırken, insanların herhangi bir sağlık problemi ortaya çıkmadan hastaneye gitmedikleri gibi bilgi güvenliğini tehlikeye atan bir tehditle karşılaşmadan bilgi güvenliğine ilişkin farkındalık yaratma çabası da göstermediklerine dikkat çekmektedir.

Kurumsal işleyişin sağlıklı bir şekilde yürütülebilmesi için kurumsal varlıkların belki de en önemlisi olan bilginin güvenli olması zaruridir. Aksi halde kurumlar açısından maddi ve manevi kayıplar kaçınılmazdır (Eminağaoğlu ve Gökşen, 2009, s.2). Etkili bir bilgi güvenliği kurumsal işleyişin süreklilik kazanmasına ve kurumsal itibarın artmasına neden olurken, kurumsal hedeflerin başarıyla gerçekleşmesine de katkı sağlar (Qureshi, 2011, s.3).

Kurumlarda bilgi güvenliğini sağlamanın teknik içerikli çeşitli uygulamaları olmakla birlikte en önemli rol insana düşmektedir (Kjorvik, 2010, s.5). Bu nedenle kurumsal düzeyde bilgi güvenliğine ilişkin bilinç ya da farkındalığın artırılması kurumsal faaliyetlerin amaca uygun ve sorunsuz bir şekilde yürütülmesinde büyük önem taşımaktadır (Marks ve Rezgui, 2009, s.4; Qureshi, 2011, s.3). Kurumsal yapıda etkili bir bilgi güvenliği farkındalığı yaratmak gerçekçi hedeflerle tasarlanmış bir eğitim programı oluşturmaya ve ortak iş çevreleriyle güvenlik önlemleri hususunda birlikte hareket etmeye bağlıdır (Wright ve Kakalık, 2007, s.187). Bilgi güvenliği farkındalığı yaratma süreci kurumsal yapının her kademesinden bireyi ilgilendirmekle beraber söz konusu sürecin gerçekleştirilmesini yönlendiren kurum yöneticileri birincil düzeyde sorumlu grubu oluşturmaktadır (Dinçel, 2008, s.7; Eminağaoğlu, Uçar ve Eren, 2009, s.224; Rotvold, 2008, s.1). Kurum yöneticileri bilgi güvenliği farkındalığı yaratma sürecinde; kurum içinde bilgi güvenliği yönetiminden sorumlu bir çalışan grubu oluşturmak, bilgi güvenliği bilinçlendirme sürecini konu ile ilgili uzmanlarca verilecek eğitimlerle desteklemek, bilgi güvenliği bilinçlendirme sürecine finansal destek sağlamak gibi faaliyetlerin yürütücüsü ve yönlendiricisidir. Bilgi güvenliği farkındalığı yaratma

uygulamalarını denetleyerek sürecin disiplinli bir şekilde gerçekleşmesini sağlamak, personel ya da kullanıcıların bilgi güvenliği farkındalıklarının yetersiz seviyede olmasından kaynaklı zararı en aza indirgemek de yine yöneticilerin sorumluluğundadır (Emiral, 2012, s.4; ENISA, 2007, s.9; Önel, 2008, s.7).

Kullanıcılar ya da personel ise bilgi güvenliği sürecinde kullandıkları yazılımların güvenlik eklentilerinin güncellenmesive saklanan verilerin yedeklenmesi gibi tedbir uygulamalarını gerçekleştirerek sürecin başarıyla gerçekleşmesine katkı sağlayabilirler (Önel, 2008, s.9).

Kütüphanelerde Bilgi Güvenliği Farkındalığı

Bilgi güvenliği yalnızca ticari şirketleri değil, büyük şirketlerle kıyaslandığında düzeyi farklı olmakla birlikte kamu kurumlarını ve kar amacı gütmeyen kuruluşları da ilgilendirmektedir (Eminağaoğlu ve Gökşen, 2009, s.3). İnternetin sağladığı olanaklarla birlikte kütüphanelerin uzaktan erişilebilir hale gelmesi, kullanıcılar açısından pek çok kolaylık sağlamakla birlikte, bilgi sistemlerinin bilişim saldırılarına uğramasına da olanak vermiştir (Anday, Francese, Huurdeman, Yılmaz, ve Zengenene, 2012, s.134; İsmail ve Zainab, 2011, s.45). Thompson (2006, s.222), sosyal mühendis olarak da bilinen saldırgan grubunun kütüphane veri tabanlarına kolaylıkla erişip, kullanıcıların kimlik, adres, e-posta ve telefon bilgilerine ulaşabildiklerini öne sürmektedir. Zimerman (2009), kütüphanelerde bulunan bilgisayarların fiziksel hasara olduğu kadar, kötü niyetli saldırılara karşı da son derece zayıf olduklarına dikkat çekmektedir. Bilgi profesyonelleri, mesleklerini gerçekleştirirken yaptıkları bazı ihmal ve kusurlar nedeniyle saldırganların tehditleri ile karşı karşıya kalabilmektedir. Personeldeki bilgi güvenliği bilincinin yetersizliği söz konusu ihmal ve kusurların nedenleri arasında gösterilmektedir (Thompson, 2006, s.224).

Kütüphaneler açısından bilgi güvenliğinin yeterince önemsenmeyenve belki de henüz anlaşılmamış bir konu olduğuna dikkat çeken Newby (2002, s.2-6), bilgi güvenliğinin yalnızca bilgisayar güvenliğini sağlamakla sınırlı olmadığını öne sürmekte ve söz konusu güvenliğin sağlanmasında etkili olabilecek önlemleri şöyle sıralamaktadır:

- Kütüphaneciler arasında bilgi güvenliğini sağlamaya yönelik etkili bir iş bölümü yapılması,
- Bilgi güvenliği sorunları ve çözümüne ilişkin yöntemler hakkında tüm kütüphane personelinin eğitilmesi,
- Bilginin gizliliğinin, materyallerin ve bilgisayarların güvenliğinin sağlanması hakkında belirli birtakım kurallar içeren bir politikanın geliştirilmesi,
- Fiziksel güvenlik planlarının yapılması,
- Bilginin bütünlüğünün sağlanması,
- Bilgi erişim yollarının denetlenmesi.

Fakeh, Zulhemay, Shabibi, Ali ve Zaini (2012, s.1733) kütüphanelerde bilgi güvenliği farkındalığının, etkili bir bilgi güvenliği politikası (bilginin güvenli kullanımı hakkında takip edilmesi gereken kurallar ve ilkeler), bilgi güvenliği eğitimi (seminer, konferans, tartışma platformları ve çeşitli kurslar aracılığıyla), teknoloji bilgisi (bilgisayarlar ve internet araçlarının güvenli ve doğru kullanımı) ve duyarlı personel faktörlerinin bütünsel bir şekilde sağlanması ile mümkün olabileceğinin altını çizmektedirler.

Ankara'daki Üniversite Kütüphanelerinde Bilgi Güvenliği Farkındalığı

Araştırmanın Yöntemi

Nitel araştırma yöntemine dayalı olarak yapılan bu araştırmanın verileri, yarı yapılandırılmış sorular odağında görüşme tekniği ile toplanmıştır. Yüz yüze ve telefonla yapılan görüşmeler 17 Aralık 2012-15 Ocak 2013 tarihleri arasında gerçekleştirilmiştir. Araştırma örneklemi, amaçlı örnekleme yöntemlerinden ölçüt örneklem tekniği ile belirlenmiştir. Amaçlı örneklem; araştırmanın amacı çerçevesinde bilgi açısından daha kapsamlı durumların seçilmesi anlamına gelmektedir (Büyüköztürk, Çakmak, Akgün, Karadeniz, ve Demirel, 2011, s.2). Bu çerçevede bilgi merkezlerini temsilen, bilginin daha yoğun kullanıldığı kütüphane türü olması nedeniyle üniversite kütüphaneleri örnekleme alınmıştır. Amaçlı örnekleme yöntemlerinden ölçüt örneklem; araştırma örnekleminin araştırma problemi ile ilgili önceden belirlenen ölçütlere uygun nitelikler taşıyan kişiler, olaylar, nesneler ya da durumlar arasından seçilmesidir (Büyüköztürk, , Çakmak, Akgün, Karadeniz, ve Demirel, 2011, s.3). Bilgi güvenliği farkındalığı yaratma sürecinde yöneticiler birincil derecede sorumlu grubu oluşturmaktadır (Emiral, 2012, s.4). Bu nedenle katılımcıların kütüphane ve dokümantasyon daire başkanı ya da yardımcısı olması önceden belirlenen ölçütlerden biridir. Araştırma takvimi çerçevesinde katılımcıların Ankara ilinde bulunan üniversite kütüphanelerinde görev yapıyor olmaları yine önceden belirlenen ölçütler arasındadır. Araştırma verileri içerik analizi yöntemiyle analiz edilmiştir. İçerik analizinde araştırma verileri kendilerini açıklayan kavramlar altında çözümlenerek kodlanmaktadır. Kodlama işlemi önceden belirlenen ya da toplanan verilerden çıkarılan kavramlarla yapılabilmektedir (Yıldırım ve Şimşek, 2000). Yapılan bu araştırmada görüşmeci notlarından elde edilen veriler önceden belirlenen kavramlarla kodlanarak beş tema (Tablo II) ile açıklanmış ve bulguların yorumlanması ile araştırma süreci tamamlanmıştır.

Araştırma Ankara'da bulunan 5'i devlet 9'u vakıf olmak üzere toplamda 14 üniversitede gerçekleştirilmiştir. Katılımcı bilgileri Tablo I'de gösterildiği gibidir.

Tablo I. Katılımcı Bilgileri

Kurum Sıra Numarası	Statü	Üniversite Adı	Üniversite Türü
1	Kütüphane ve Dokümantasyon Daire Başkan Vekili	Ankara Üniversitesi	Devlet
2	Kütüphane ve Dokümantasyon Daire Başkanı	Atılım Üniversitesi	Vakıf
3	Kütüphane ve Dokümantasyon Daire Başkanı	Başkent Üniversitesi	Vakıf
4	Kütüphane ve Dokümantasyon Daire Başkanı Yardımcısı	Bilkent Üniversitesi	Vakıf
5	Kütüphane ve Dokümantasyon Daire Başkanı	Çankaya Üniversitesi	Vakıf
6	Kütüphane ve Dokümantasyon Daire Başkanı	Gazi Üniversitesi	Devlet
7	Kütüphane ve Dokümantasyon Daire Başkanı	Hacettepe Üniversitesi	Devlet
8	Kütüphane ve Dokümantasyon Daire Başkanı	Orta Doğu Teknik Üniversitesi	Devlet
9	Kütüphane ve Dokümantasyon Daire Başkanı	TED Üniversitesi	Vakıf
10	Kütüphane ve Dokümantasyon Daire Başkanı	TOBB Üniversitesi	Vakıf
11	Kütüphane ve Dokümantasyon Daire Başkanı	Turgut Özal Üniversitesi	Vakıf
12	Kütüphane ve Dokümantasyon Daire Başkanı	Türk Hava Kurumu Üniversitesi	Vakıf
13	Kütüphane ve Dokümantasyon Daire Başkanı	Ufuk Üniversitesi	Vakıf
14	Kütüphane ve Dokümantasyon Daire Başkanı	Yıldırım Beyazıt Üniversitesi	Devlet

Verilerin Analizi

Araştırma verilerini açıklayan temalar Tablo II'de gösterildiği gibidir.

Tablo II. Araştırma Temaları

TEMALAR	
Bilgi Güvenliği, Bilgi Güvenliğinin Gereği ve Önemi	Bilgi güvenliği nedir? Ne tür uygulamaları kapsar? Bilgi güvenliğini tehdit eden unsurlar nelerdir? Bilgi güvenliğinin üniversite kütüphaneleri açısından gereği ve önemi
Kütüphanelerde Bilgi Güvenliği Uygulamaları	Kurumsal politika Siber saldırılara yönelik önlemler (Anti-virüs,şifreleme, yedekleme, e-imza gibi)
Bilgi Güvenliğine İlişkin Bilgi Düzeyi	Bilgi güvenliğine bağlı sorumlulukların bilincinde olma Bilgi güvenliği uygulamalarının gereğini yerine getirme Bilgi güvenliği farkındalığı Farkındalık eğitimi Bilgi güvenliğini sağlamaya teşvik etme
Personel Denetimi	Denetim Erişimde sınırlama Toplantı, vb. etkinliklerle uyarıda bulunma, eksik yönleri tartışıp önlem alma Hatırlatıcı mesajlar Üst yönetime rapor etme
Kullanıcı Denetimi	Bilgisayar kullanımı ile ilgili İnternet kullanımı ile ilgili Güvenli kullanım hatırlatmaları Kimlik denetimi Fiziksel materyallerin denetimi

Kütüphaneler Açısından Bilgi Güvenliği, Bilgi Güvenliğinin Gereği ve Önemi

Üniversite kütüphanelerinde bilgi güvenliği kavramı daha çok bilgisayar ve iletişim teknolojilerine dayalı uygulamaların ortaya çıkardığı tehditlere karşı alınan önlemleri ifade etmektedir. Yetkisiz erişim girişimleri, kullanıcıların yasal olmayan ya da sahte içerikli web sitelerini ziyaret etmeleri ve bunun sonucunda maruz kalınan virüs saldırıları kütüphanelerde bilgi güvenliğini tehdit eden başlıca unsurlar arasındadır.

Kütüphane yöneticileri, hiç tereddüt etmeden verdikleri yanıtlarla bilgi güvenliğini kütüphaneler açısından son derece önemli bulduklarının altını çizmişlerdir. Yöneticiler ayrıca Üniversitelerin bilgi varlıklarının korunduğu kütüphaneler açısından bilgi güvenliğini sağlamaya yönelik çalışmaların gerekli olduğunu da düşünmektedirler. Bununla birlikte bazı yöneticiler güvenlik önlemlerinin bilgi erişimini sınırlandırma riski yaratmadan alınması gerektiğini savunmaktadırlar.

"Kütüphanelerin asıl işlevi olan bilgi erişime kısıtlama getirmediği sürece bilgi güvenliğine yönelik uygulamaları gerekli ve önemli bulurum" (Görüşmeci 6).

Bilgi güvenliği sorunlarının özellikle bilgi teknolojilerine dayalı uygulamaların kütüphanelerde yer bulmasıyla ortaya çıktığını düşünen kütüphane yöneticileri, bilgi güvenliğinin meslek çevrelerince dikkat çekilmesi gereken bir konu olduğunu öne sürmektedirler.

Kütüphanelerde Bilgi Güvenliği Uygulamaları

Kütüphanelerde bilgi güvenliğini sağlamaya yönelik uygulamalar genelde üniversitelerin bilgi işlem daire başkanlıkları tarafından yürütülmektedir. Bazı üniversite kütüphanelerinde bilgi işlem önlemlerine ek olarak kütüphaneye ait bilgi güvenliği uygulamaları bulunmaktadır.

"*Başlı başına kütüphane olarak bilgi güvenliğini sağlamaya yönelik bazı girişimlerimiz bulunmaktadır. Bilgi işlemin ön gördüklerine ek olarak kütüphanemizin kullandığı ve güvenliği sağlamada yararlandığımız bazı yazılımlar kullanıyoruz. Elektronik yayınların usulüne uygun kullanılması, sistematik bir veri kullanımının olmaması amacıyla web sayfamızdan birtakım duyurular yayınlıyor ve intihali önlemek için bilgi işlem destekli Ithenticate yazılımını kullanıyoruz"* (Görüşmeci 8).

Üniversite kütüphanelerinde bilgi güvenliği kapsamında takip edilmesi gereken kurumsal bir politikanın varlığından bahsetmek güçtür. Ancak kütüphanelerden birkaçı, politika belgesi niteliğinde birtakım dokümanlarının bulunduğuna dikkat çekmektedir.

"*Elektronik yayınların ya da standartların kullanımında dikkat edilmesi gerekenleri içeren birimlere yönelik olarak hazırlanmış ve içeriği itibariyle politika belgesi niteliği taşıyan bazı belgeler bulunmaktadır"* (Görüşmeci 8).

*"*Üniversite*nin bilgi teknolojileri birimi tarafından oluşturulmuş ve kütüphane olarak bizim de takip ettiğimiz bir politika belgesi bulunmaktadır"* (Görüşmeci 9).

"Üniversitenin tüm birimler için hazırlamış olduğu ve kütüphanenin de takip ettiği bir bilgi güvenliği poltikası bulunmaktadır" (Görüşmeci 2).

Kütüphanelerin bilgi güvenliğine dayalı uygulamalarının başında antivirüs programları, şifreleme, yedekleme, erişim denetimi, saldırı tespit uygulamaları gelmektedir. Yalnızca birkaç kütüphane elektronik imza uygulaması ile doküman güvenliği sağlama uygulamasını gerçekleştirmektedir.

Yedekleme işlemi harici disk, CD ve DVD gibi araçlar üzerinde yapılmanın yanı sıra çeşitli yazılımlar ya da sanal paylaşım alanları aracılığı ile de yapılabilmektedir.

"*Diğer yedekleme ortamlarına ek olarak Web temelli bir doküman yönetimi yazılımı olan Feng Office üzerinde de yedekleme faaliyetini gerçekleştiriyoruz*" (Görüşmeci 8).

"Linux tabanlı Oracle veri tabanı kullanılarak kaset üzerine ve dijital ortamda imaj olarak yedekleme yapılıyor" (Görüşmeci 6).

Bilgi Güvenliğine İlişkin Bilgi Düzeyi

Yöneticilerin büyük çoğunluğu kütüphanede çalışan personelin bilgi güvenliğine ilişkin bilgi düzeyinin yeterli seviyede olmadığını düşünmektedir. Bilgi güvenliğinin sağlanması çoğu kütüphanede bilgi işleme mal edilmiş olup, yöneticilere göre personel olası tehditlere karşı alması gereken önlemlerin yeterince farkında değildir. Bununla birlikte kütüphanelerde bilgi güvenliği farkındalığı yaratmayı amaçlayan herhangi bir uygulama bulunmamakta ve konuya ilişkin bir eğitim verilmemektedir.

Personel Denetimi

Kütüphanelerin neredeyse tamamında personel, bilgisayar ve interneti dilediği gibi kullanabilmektedir, ancak siyasi, pornografik, vb. içerikli bazı siteler bilgi işlem tarafından filtrelenmektedir.

"Denetimden çok herkesin kendini kontrol etmesinden yanayım. Dolayısıyla personeli denetleme eylemini doğru bulmuyorum" (Görüşmeci 6).

"Bireysel bilgisayarlarda yedekleme başta olmak üzere personel veri kaybını önleyici kullanım koşullarına teşvik ediliyor" (Görüşmeci 9).

Kütüphanelerin hemen hepsinde kütüphane içinde çözümlenemeyen güvenlik sorunları bilgi işlem birimine ve bağlı olduğu rektör yardımcısı makamına iletilmektedir. Zaman zaman yapılan toplantılarda bilgi güvenliğini de kapsayan konulara yer verilmektedir.

Kullanıcı Denetimi

Kütüphanelerde bilgi işlem birimi aracılığıyla güvenli kullanım hatırlatmaları ve web duyuruları yapılmaktadır. IP denetimi ile kullanıcıların sakıncalı sitelere erişimi tespit edilerek gerekli uyarılarla hatalı kullanımın tekrarlanması önlenmeye çalışılmaktadır. Şifre ya da kullanıcı bilgisine ulaşmak isteyen kullanıcılar önce kimlik denetimi ile sorgulanıp

daha sonra e-posta üzerinden talep ettikleri bilgilere erişim sağlayabilmektedirler. Fiziksel materyallerin korunmasında manyetik bantlar, RFID ve kapı güvenlik sistemleri kullanılmaktadır. Bazı kütüphanelerde bilgi işlem uygulamalarına ek olarak kablolu ve kablosuz tüm bağlantıların ağ hareketlerini takip eden yazılımlar kullanılmaktadır.

"*Ağ analizi sağlayan programlarla kullanıcıların kütüphane bilgisayarlarına indirdiği zararlı kodları saptayıp gerekli önlemleri alıyoruz*" (Görüşmeci 6).

Sonuç

Kütüphanelerde bulunan internet, bilgisayar, faks, telefon, mobil cihazlar gibi bilgi ve iletişim araçları kütüphane faaliyetlerinin gerçekleştirilebilmesi amacıyla kullanılmaktadır. Söz konusu araçların amacı dışında ya da kuruma zarar verecek şekilde kullanılması, ilgili araçların kullanımına ilişkin kuralların göz ardı edildiğini göstermektedir.

Yanlış ya da etik dışı kullanım kütüphane kurumunu birtakım yasal yaptırımlara maruz bırakabilir. Bu nedenle kütüphanelerde bilgi güvenliğinin sağlanması, üzerinde titizlikle durulması gereken bir konu olarak karşımıza çıkmaktadır. Ankara'da bulunan üniversite kütüphanelerinde bilgi güvenliği farkındalığını ortaya koymak amacıyla yapılan bu araştırmadan elde edilen sonuçlar şöyle özetlenebilir:

- ◊ Kütüphanelerin büyük bir kısmında bilgi güvenliğinin sağlanması gerekli ve önemli bulunmakla birlikte, bilgi güvenliğinin ne olduğu ve ne tür uygulamaları içerdiği hususunda yeterince bilgi sahibi olunmadığı sonucuna ulaşılmıştır.
- ◊ Kütüphanelerin çoğunda bilgi güvenliğini kapsayan kurumsal bir politikanın bulunmadığı saptanmıştır. Bununla birlikte bazı kütüphanelerde kaynak kullanım bilgilerinin yer aldığı birtakım belgelere rastlanmıştır. Kütüphane yöneticilerinin, içeriği itibariyle politika belgesi olarak nitelendirdiği bu belgeler, yalnızca elektronik kaynakların kullanım talimatları ile sınırlıdır.
- ◊ Bilgi güvenliğini sağlamaya yönelik uygulamalar kütüphanelerin neredeyse tamamında üniversitelerin bilgi işlem daire başkanlıkları tarafından yürütülmektedir. Kendi içinde güvenlik önlemleri almaya çalışan az sayıda üniversite kütüphanesi bulunmaktadır. Söz konusu kütüphanelerde bilgi güvenliği uygulamalarını da yürüten bilgi teknolojisi uzmanlarının varlığı göze çarpmaktadır.
- ◊ Olası saldırılara karşı savunma olarak antivirüs, şifre koyma, yedekleme, erişim denetimi gibi güvenlik önlemleri kullanılmakta ve yeterli olduğu düşünülmektedir. Oysa söz konusu uygulamaların her birinde birtakım eksiklikler bulunmakta ve bilgi güvenliğinin sağlanmasında tek başına yeterince anlamlı olmamaktadırlar.
- ◊ Bilgi güvenliği kurumsal toplantılarda nadiren dile getirilen bir konu olup, başlı başına bilgi güvenliği farkındalığı yaratmayı sağlayan herhangi bir etkinlik (toplantı, seminer, tartışma vb.) bulunmamaktadır.

◊ Kütüphanelerin neredeyse tamamında bilgi güvenliği yalnızca "teknik" yönü olan uygulamaları kapsayan bir süreç gibi algılanmakta, güvenlik sürecinin belki de en önemli rolünü üstlenen insan faktörü göz ardı edilmektedir.

◊ Kütüphanelerin hemen hepsinde yöneticiler, kütüphane personelinin bilgi güvenliği ile ilgili bilgi düzeyinin düşük seviyede olduğunu düşünmektedirler. Bununla birlikte, bilgi güvenliği bilincini geliştirecek ve güvenlik kurallarını uygulamaya teşvik edecek herhangi bir eğitimin verilmiyor olması dikkat çekicidir.

Öneriler

Araştırmadan elde edilen sonuçlar doğrultusunda şu önerilere ulaşılmıştır:

◊ Kütüphanelerde bilgi güvenliğini sağlamanın teknik içerikli birtakım uygulamaları olmakla birlikte en önemli rol insana düşmektedir. Bu nedenle kütüphanelerde bilgi güvenliğine ilişkin bilinç ya da farkındalığın artırılması kütüphane faaliyetlerinin amaca uygun ve sorunsuz bir şekilde yürütülmesinde büyük önem taşıyacaktır. Bu çerçevede verilecek bir farkındalık eğitiminin, bilgi güvenliği bilincinin artırılmasında önemli bir rol üstleneceği düşünülmektedir.

◊ Bilgi güvenliği ile ilgili sorumlulukların bir görev anlayışıyla yerine getirilmesinin güvenlik ihlallerinin azalmasında önemli bir rol oynayacağı düşünülmektedir.

◊ Kütüphane personeli kullandıkları yazılımların güvenlik eklentilerinin güncellenmesi, antivirüs yazılımlarının kullanılması, saklanan verilerin yedeklenmesi gibi tedbir uygulamalarını gerçekleştirerek sosyal mühendislik saldırıları da dahil olmak üzere olası her tür tehdite karşı kütüphane materyallerinin korunmasına katkı sağlayabilirler.

◊ Kütüphane koleksiyonunda yer alan materyallerin ve internet araçlarının kullanımı kurumsal bir politika ile net bir şekilde ifade edilmelidir. Kural dışı kullanım için cezai yaptırımların uygulanmasının caydırıcı olabileceği düşünülmektedir.

◊ Kütüphane kaynaklarının güvenli bir şekilde kullanılması hususunda kullanıcılara verilecek eğitimin karşılaşılan güvenlik sorunlarını azaltacağı düşünülmektedir. Bu amaçla özellikle kullanıcı eğitimi ya da rehberlik hizmeti veren kütüphanecilerin gerçekçi hedeflerle tasarlanmış bir eğitim programı ile kullanıcılara gerekli eğitimi sunması çözümleyici olabilir.

Kaynakça

Al-Awadi, M. ve Renaud, K. (2007). *Success factors in information security implementation in organizations.* 20 Ekim 2012 tarihinde http://www.dcs.gla.ac.uk/~karen/Papers/sucessFactos2.pdf adresinden erişildi.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. C*omputer&Security, 26*(4), 276-289.

Aloul, F. (2010). Information security awareness. *IEEE International Conference for Internet Technology and Secured Transactions (ICITST)* içinde (s. 1-6), Londra: Birleşik Krallık.

Al-Shehri, Y. (2012). Information security awareness and culture. *British Journal of Arts and Social Sciences, 6*(1), 61-69.

Anday, A., Francese, E., Huurdeman, H., Yılmaz, M. ve Zengenene, D. (2012). Information security issues in a digital library environment: A literature review. *Bilgi Dünyası,13*(1),117-137.

Atabek, Ü. (2001*). İletişim ve teknoloji: Yeni olanaklar yeni sorunlar.* Ankara: Seçkin Yayıncılık.

Bensghir, T.K. (2008). *Kurumsal bilgi güvenliği yönetim süreci*. 5 Kasım 2012 tarihinde www.erzincan.edu.tr/userfiles/file/stratejidb/guvenlik.ppt adresinden erişildi.

Bogart, K.J. (2012). *Information security awareness: How to get users asking for more*. 20 Ekim 2012 tarihinde http://iasec.eller.arizona.edu/docs/whitepepers/IS_awrenes.pdf adresinden erişildi.

Boujettif, M. ve Wang,Y. (2010). *Constructivist approach to information security awareness in the Middle East*. 20 Ekim 2012 tarihinde http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnuber=633845 adresinden erişildi.

Büyüköztürk, Ş., Çakmak, E.K., Akgün, Ö.E., Karadeniz, Ş., ve Demirel, F. (2011). *Örnekleme yöntemleri: Bilimsel araştırma yöntemleri kitabı.* 1 Aralık 2012 tarihinde http://msbay.files.wordpress.com/2009/10/9haftaarac59ftc4b1rmalardac3b6rnekleme.pdf adresinden erişildi.

Canbek, G. ve Sağıroğlu, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. *Journal of Polytechnic, 9*(3), 165-174.

Civelek, D.Y. (2011). *Kişisel verilerin korunması ve bir kurumsal yapılanma önerisi*. Uzmanlık tezi, Devlet Planlama Teşkilatı, Bilgi Toplumu Dairesi Başkanlığı, Ankara.

Dura, C. ve Atik, H. (2002). *Bilgi toplumu, bilgi ekonomisi ve Türkiye*. İstanbul: Literatür Yayınları.

Eminağaoğlu, M. ve Gökşen,Y. (2009). Bilgi güvenliği nedir, ne değildir? Türkiye' de bilgi güvenliği sorunları çözüm önerileri. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 11*(4), 1-15.

Eminağaoğlu, M., Uçar, E. ve Eren, Ş. (2009). The positive outcomes of information security awareness training in companies: A case study. *Information Security Technical Report, 14*(4), 223-229.

Emiral, F. (2012). *Bilgi güvenliği bilincinin genele yayılması.* 20 Ekim 2012 tarihinde http://www.denetimnet.net/UserFiles/Documents/5051.pdf adresinden erişildi.

Eskiyörük, D. (2008). *Bilgi sistemleri kabul edilebilir kullanım politikası oluşturma klavuzu*. TÜBİTAK UEKAE(Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü): Ankara.

European Network and Information Security Agency (ENISA). (2007). *Information security awareness initiatives: Current practice and the measurements of success*. 20 Ekim 2012 tarihinde http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_metin_docs/contributions/ENIA_Measuring_Awareness_Final.pdf adresinden erişildi.

European Network and Information Security Agency (ENISA). (2006). *A users' guide: How to raise information security awareness*. 20 Ekim 2012 tarihinde http://www.iwar.org.uk/comsec/resources/ENISA/infoec-awareness.pdf adresinden erişildi.

Fakeh, S.K.M., Zulhemay, M.N., Shabibi, M.S., Ali, J. ve Zaini, M. K. (2012). *Information security awareness amongst academic librarians.* 1 Ocak 2012 tarihinde http://www.aensiweb.com/jasr/jasr/2012/17231735.pdf adresinden erişildi.

Ismail, R. ve Zainab, A.N. (2011). Information systems security in special and public libraries: An assesments of status. Malaysian *Journal of Library and Information Science, 16*(2), 45-62.

ISO International Organization for Standardization. (2005). *ISO/IEC 27001:2005* 22 Ekim 2012 tarihinde http://www.cert.sd/images/stories/iso27001.pdf adresinden erişildi.

Kjorvik, H. (2010). *Implementing and improving awareness in information security*. 20 Ekim 2012 tarihinde http://brage.bibsys.no/hia/bitstream/URN:NBN:nobibsys_brage_15269/1/Kjorvik.pdf adresinden erişildi.

Marks, A. (2007). *Exploring universities & information systems security awareness in a changing higher education environment: A comparative case study research*. 20 Ekim 2012 tarihinde http://usir.salford.ac.uk/26802/1/10581588.pdf adresinden erişildi.

Marks, A. ve Rezgui, Y. (2009). *A comparative study of information security awareness in Higher education based on the concept of design theorizing*. 20 Ekim 2012 tarihinde http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnuber=5302667&tag=1 adresinden erişildi.

Newby, G.B. (2002). *Information security for libraries.* 20 Ekim 2012 tarihinde http://www.petascale.org/papers/librarysecurity.pdf adresinden erişildi.

Önel, D. ve Dinçkan, A. (2007). *Bilgi güvenliği yönetim sistemi kurulumu*. TÜBİTAK UEKAE (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü).

Önel, D. (2008). *Bilgi güvenliği bilinçlendirme süreci oluşturma kılavuzu*. TÜBİTAK UEKAE (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü).

Pro-G. (2003). *Bilişim güvenliği*. 01 Kasım 2012 tarihinde http://www.pro-g.com.tr/whitepapers/bilisim-guvenligiv1.pdf adresinden erişildi.

Rotvold, G. (2008). How to create asecurityculture in your organization. *Information Management Journal, Nov-Dec*. 20 Ekim 2012 tarihinde http://content.arma.org/IMM/NovDec2008/How_to_Cr ate_a_Security_Culture.aspx adresinden erişildi.

Siponen, M.T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31–41.

Şahinaslan, E., Kandemir, R. ve Şahinaslan, Ö. (2009). *Bilgi güvenliği farkındalık eğitim örneği*. 20 Ekim 2012 tarihinde http://ab.org.tr/ab09/bildiri/117.pdf adresinden erişildi.

Thompson, S.T.C. (2006). *Helping the hacker? Library information, security and social engineering*. 21Ekim 2012 tarihinde http://www.ala.org/lita/ital/sites/ala.org.lita.ital/files/coent/25/4/thompson.pdf adresinden erişildi.

Qureshi, M.S. (2011*). Measuring efficiacy of information security policies: A case study of UAE based company*. 20 Ekim 2012 tarihinde http://kth.divaportal.org/smash/record.jsf?pid=diva2:50266 adresinden erişildi.

Wooding, S., Anhal, A., Valeri, L. (2003). *Raising citizen awareness of information security: A practical guide*. 20 Ekim 2012 tarihinde http://www.clusit.it/whitepapers/eaware_practical_guide.pdf adresinden erişildi.

Wright, M.A. ve Kakalık, J. (2007). *Information security: Contemporary cases*. Sudbury Jones and Bartlett.

Yıldırım, A. ve Şimşek, H. (2000). *Sosyal bilimlerde nitel araştırma yöntemleri*. Ankara: Seçkin Yayınevi.

Zimerman, M. (2010). Protect your library's computers. *New Library World, 111*(5/6), 203-212.