KOBİ'LERDE BİLİŞİM TEKNOLOJİLERİ GÜVENLİĞİ SORUNU: TEHDİTLER VE ÖNLEMLER

Yrd.Doç.Dr. Ali ACILAR [*]

ÖZET

Günümüz iş hayatında, bir kişinin çalıştığı işyerlerinden binlerce kişinin çalıştığı büyük işletmelere kadar her büyüklükteki işletme, bilişim teknolojilerini kullanma gereksinimi duymaktadır. Bilişim teknolojileri, işletmelere sağladığı fayda ve avantajlar yanında çeşitli risk ve tehditleri de içermektedir. Özellikle bilişim teknolojileri sektöründe bulunmayan KOBİ'ler, bu teknolojilerin güvenliğini etkin bir şekilde sağlayamamakta ve güvenlik sorunlarından daha fazla etkilenebilmektedir. Bu çalışmada KOBİ'lerde bilişim teknolojileri güvenliği ele alınmakta, KOBİ'lerin karşılaşabilecekleri bilişim teknolojileri güvenliği tehditleri ve bunlara karşı alınabilecek önlemler değerlendirilmektedir.

Anahtar kelimeler: Bilişim teknolojileri güvenliği, KOBİ

ABSTRACT

Businesses in any size, whether it is a small business that employs one or a large corporation that employs thousands, need to use information technologies in today's business life. Although information technologies have many advantages and opportunities for businesses they contain threats as well. Especially SMEs that are not in the ICT sector fail to implement effective information security and can be affected by security problems more likely. In this study information technology security in SMEs is investigated. Security threats that may be confronted by SMEs and countermeasures are reviewed.

Key Words: Information technology security, SMEs

[*] Bilecik Üniversitesi, İ.İ.B.F., İşletme Bölümü, aliacilar@yahoo.com

I. GİRİŞ

Günümüzde bilişim teknolojilerinin kullanımı, dünya genelinde yaygınlaşmış ve işletmeler için bu teknolojilerin kullanımı kaçınılmaz hale gelmiştir. Hızla gelişen bilişim teknolojileri, iletişimde, bilgi paylaşımında ve ticarette sağladığı olanaklar ile işletmelere çok büyük faydalar ve avantajlar sağlamaktadır. Bu nedenle çoğu işletme, kayıtlarını tutma, saklama, para transferi yapma, iletişim vb. faaliyetler için bilişim teknolojilerine bağımlı hale gelmiştir[1]. Bilişim teknolojileri, sağladığı fayda ve avantajların yanı sıra bazı güvenlik sorunlarını da beraberinde getirmektedir. Bunlar içerisinde, kötü amaçlı yazılımlar, bilgi hırsızlığı, teknoloji casusluğu, İnternet korsanlığı örnek gösterilebilir. Bilişim teknolojileri ile ilgili güvenlik sorunları, bu teknolojilerin kullanımının yaygınlaşmasını engelleyen önemli tehditlerden birisi olarak kabul edilmektedir[2].

Büyük işletmeler, bilişim güvenliğini sağlayacak teknik bilgi ve maddi güce sahipken, KOBİ'ler bu yeteneklere tamamıyla sahip olamamaktadır. Her büyüklükteki işletme, bilgisayar kullandığı ve İnternet'e bağlı olduğu müddetçe güvenlik tehditleri ile karşı karşıyadır. Önemli olan; bu tehditlerin farkında olmak, gerekli yazılım ve donanım önlemlerini almak, çalışanları tehditler hakkında bilgilendirmek, güvenlik tehditleriyle ilgili gelişmeleri takip ederek, en kötü durumlara karşı bir acil eylem planı ile hazır olmaktır[3].

---

[1] Jeffrey M. STANTON, Kathryn R. STAM, Paul MASTRANGELO, Jeffrey JOLTON, "Analysis of end user security behaviors", *Computers & Security*, Cilt No: 24, 2005, s.124.; Atul GUPTA, Rex HAMMOND, "Information systems security issues and decisions for small businesses: An empirical examination" *Information Management & Computer Security*, Cilt No: 13, Sayı: 4, 2005, s.297.

[2] Steve HAWKINS, David C. YEN, David C. CHOU, "Awareness and challenges of Internet security", *Information Management & Computer Security*, Cilt No: 8, Sayı: 3, 2000, s.131.; Şule ÖZMEN, *Ağ Ekonomisinde Yeni Ticaret Yolu, E-Ticaret*, İstanbul Bilgi Üniversitesi Yayınları, 2. Baskı, İstanbul, 2006, s.234.

[3] Shannon KELLER, Anne POWELL, Ben HORSTMANN, Chad PREDMORE, Matt CRAWFORD, "Information Security Threats and Practices in Small Businesses", *Information Systems Management*, Cilt No: 22, Sayı: 2, 2005, s.7.; Diomidis SPINELLIS, Spyros KOKOLAKIS, Stephanos GRITZALIS, "Security requirements, risks and recommendations for small enterprise and home-office environments", *Information Management & Computer Security*, Cilt No: 7, Sayı: 3, 1999, s.121.

Bu çalışmada, KOBİ'lerde bilişim teknolojileri güvenliği çeşitli yönleriyle ele alınmıştır. Bu bağlamda, KOBİ'lerde bilişim teknolojileri kullanımı, bilişim teknolojileri güvenliği, güvenlik tehditleri, bunlara karşı alınabilecek önlemler ve KOBİ'lerde bilişim teknolojileri güvenliğini etkileyen etmenler üzerinde durularak, KOBİ'lerde bilişim teknolojileri güvenliğinin yaygınlaştırılması için önerilere yer verilmiştir.

II. KOBİ'LERDE BİLİŞİM TEKNOLOJİLERİ KULLANIMI

Bilgisayar fiyatlarının düşmesi, İnternet'in dünya genelinde yaygınlaşması, işletmelere yönelik yazılımların artması gibi faktörler her büyüklükteki işletmeyi bilgi saklamak, yönetmek ve iletmek için bilgisayar kullanmaya zorlamaktadır[4]. Günümüz bilişim teknolojileri, üretimden satışa kadar işletmelerde her aşamada kullanılabilmektedir. Bilişim teknolojileri, işletmelerarası ilişkilerde, tedarik zincirinde satıcı araştırma, sipariş verme, stoklama, teslimat vb. faaliyetlerin gerçekleştirilmesinde veya otomatik hale getirilmesinde işletmelere büyük kolaylıklar sağlamaktadır[5]. Bilgi sistemleri ve bilgi teknolojileri geleceğin esnek örgütlerinin anahtarları olarak kabul edildiğinden dolayı[6], KOBİ'ler, bulundukları rekabet şartlarında hayatlarını sürdürebilmeleri için bu teknolojileri kullanmak zorundadır. Fakat, büyük işletmelere göre sınırlı finansal olanakları ve sınırlı uzman insan kaynakları ile faaliyet gösteren KOBİ'ler, bilişim teknolojilerinden yeterince yararlanamamaktadır. Büyük işletmelerle karşılaştırıldığında KOBİ'lerin bu teknolojileri benimseme hızı ve oranı daha düşüktür[7].

---

[4] GUPTA ve HAMMOND, a.g.e., 2005, s.297.

[5] Nunzia CARBONARA, "Information and communication technology and geographical clusters: opportunities and spread", *Technovation*, Cilt No: 25, 2005, s.213.

[6] Margi LEVY, Philip POWELL, "SME Flexibility and the role of Information Systems", *Small Business Economics*, Cilt No: 11, 1998, s.183.

[7] Jungwoo LEE, "Discriminant analysis of technology adoption behavior: a case of internet technologies in small business", *The Journal of Computer Information Systems*, Cilt No: 44, Sayı: 4, 2004, s.57.

KOBİ'lerin çoğunluğu bilişim teknolojileri sektörü dışında faaliyet gösterdiğinden güncel bilişim teknolojilerini takip etmek çoğu KOBİ için bir öncelik taşımamaktadır. Genellikle, KOBİ'lerde bilişim teknolojileri para kazandıracak bir değer olarak görülmemektedir. KOBİ'lerde bilişim teknolojileri kullanımı ile elde edilebilen en büyük kazanım, iletişimin geliştirilmesi olarak gözükmektedir[8].

İşletmelerin büyüklüğü arttıkça teknolojik yenilikler için kullanabilecekleri kaynakların miktarı da artmaktadır. Bu nedenle, büyük işletmeler teknolojik yenilikleri daha önce temin edebilmekte, bunlar için daha fazla yatırım yapabilmekte ve bu teknolojileri kullanabilecek nitelikte insan kaynaklarına sahip olabilmektedir. Araştırmalar, işletme büyüklüğünün bilişim teknolojilerinin benimsenmesini etkileyen en önemli faktörlerden birisi olduğunu ortaya koymaktadır[9].

III. BİLİŞİM TEKNOLOJİLERİ GÜVENLİĞİ

Donanım, yazılım, bilgi ve iletişimi kapsayan bilgi sistemlerinin gizliliğinin, güvenliğinin, bütünlüğünün ve her zaman çalışır olmasının sağlanması, bilişim teknolojileri güvenliği kapsamına girmektedir[10]. İşletmelerin bilişim sistemlerine bağlılığı arttıkça bu sistemlerde meydana gelebilecek arıza ve saldırılara karşı duyarlılığı da artmaktadır. Bilgi işlem sistemine yapılacak bir saldırı ciddi miktarda para, zaman, prestij ve bilgi kaybına sebep olabilmektedir[11].

---

[8] David CHAPMAN, Leon SMALOV, "On Information Security Guidelines for Small/Medium Enterprises" ICEIS 2004, *Proceedings of the 6th International Conference on Enterprise Information Systems*, Porto, Portugal, 2004, s.3.

[9] Gültekin YILDIZ, Ali ACILAR, Muzaffer AYDEMİR, "İşletme Büyüklüğünün KOBİ'lerde İnternet Kullanımına Etkileri: Görgül Bir Araştırma" *6. Bilgi, Ekonomi ve Yönetim Uluslararası Kongresi*, İstanbul, Cilt II, 2007, s.959.

[10] Cyril ONWUBIKO, Andrew P. LENAGHAN, "Managing Security Threats and Vulnerabilities for Small to Medium Enterprises", *2007 IEEE International Conference on Intelligence and Security Informatics*, New Brunswick, NJ, A.B.D., 2007, s.244.

[11] Burak DAYIOĞLU, "Ağ ve işletim sistemi güvenliği", *Türkiye Bilişim Derneği 9. Bilgi İşlem Merkezi Yöneticileri Semineri (İMY9)*, 2002, Belek/Antalya.

Gupta ve Hammond'a göre işletmelerin elektronik ağlarla birbirlerine bağlandığı günümüzde güvenlik kaygısı zirvededir[12].

İnternet, çok önemli bir bilgi ve kazanç kaynağı olmasına karşın, kullanımında karşılaşılan en önemli engellerden birisi, güvenliğin sağlanamaması veya potansiyel kullanıcılar tarafından İnternet'in güvenli olarak algılanmamasıdır. Bu sorunun ana kaynaklarından birisi de İnternet'in herkese açık bir kaynak olmasıdır. Bu durum, güvenlik için bir tehdit unsurudur. Herkesin kullanımına açık olma, bilgi güvenliğinin sağlanması ile çelişen bir durum olduğundan dolayı, geleneksel bilgi güvenliği önlemleri, İnternet gereksinimlerine uymamaktadır[13]. Damaskopoulos ve Evgeniou, KOBİ yöneticilerinin online işlemlere güven ve güvenlik ile ilgili ciddi kaygılarının bulunduğunu saptamıştır[14].

Özellikle küçük işletmeler finansal kaynak yetersizliği ve güvenliği sağlayacak teknik kadro ve deneyime sahip olmadıkları için bilişim sistemlerine gelecek saldırılara ve bunların sonucunda oluşacak zararlara karşı daha dayanıksızdır[15].

IV. GÜVENLİK TEHDİTLERİ

Donanım, yazılım, bilgi ve iletişimi kapsayan bilgi sistemlerinin gizlilik, güvenlik, bütünlük ve her zaman çalışır olmasını engelleyebilecek veya sisteme zarar verebilecek her türlü kişi, durum veya olay bilişim sistemleri için bir tehdit olarak değerlendirilmektedir[16]. Bilişim teknolojilerinin hızlı bir şekilde gelişimi, bilginin saklanması ve iletilmesini kolaylaştırmakla beraber bilginin kolay bir şekilde değiştirilebilme, çalınabilme ve imha

---

[12] GUPTA ve HAMMOND, a.g.e., 2005, s.297.
[13] Craig ALLAN, Justin ANNEAR, Eric BECK, John Van BEVEREN "A Framework for the Adoption of ICT and Security Technologies by SMEs", *16th Annual Conference of Small Enterprise Association of Australia and New Zealand*, 2003.
[14] Panagiotis DAMASKOPOULOS, Theodoros EVGENIOU, "Adoption of New Economy Practices by SMEs in Eastern Europe", *European Management Journal*, Cilt No: 21, Sayı: 2, 2003, s.133.
[15] GUPTA ve HAMMOND, a.g.e., 2005, s.297.
[16] ONWUBIKO ve LENAGHAN, a.g.e., 2007, s.244.

edilebilmesi gibi önemli güvenlik risklerini de beraber getirmiştir. Çoğu durumda bu risk, kontrol ve güvenlik uygulamalarının gelişmesinden ve çalışanların bu konularda bilgilenmesinden daha hızlı gelişmektedir[17].

Genellikle İnternet üzerinden bulaşan virüsler, solucanlar, truva atları, mesaj sağanakları, telefon çeviriciler, klavye izleme sistemleri, tarayıcı soyma ve casus yazılımlar gibi kötü amaçlı yazılımlar, artan bir çeşitlilikle kişisel kullanıcıları ve kurumları zarara uğratmaktadır[18]. Müşteri veri tabanlarının silinmesi, çalınması, işletme finansal bilgilerinin çalınması, sisteme virüs bulaştırılması, ticari sır içeren dosyaların çalınması, personel kayıtlarının alınması, müşteri kredi kart bilgilerinin çalınması işletme sistemine yapılacak saldırılardan bazılarıdır[19]. Bilişim sistemleri için tehlike ve tehdit oluşturan unsurlar aşağıdaki gibi gerçekleşebilir[20]:

- Donanım hatası,
- Virüsler, truva atları, solucanlar gibi kötü amaçlı yazılımlar,
- Sel, yangın, deprem gibi doğal felaketler,
- İnternet saldırıları,
- İşletme çalışanlarının neden olduğu tehlike ve tehditler.

Bu tehdit ve tehlikeler, insanların neden olduğu ve insanların neden olmadığı şeklinde iki kategoride incelenebilir[21]. İnsanların neden olduğu tehditler aşağıdaki gibi sıralanabilir:

- Donanım ve yazılım geliştirilirken yapılan yanlışlar,
- Fiziksel ortamda yapılan yanlışlar (sistemin aşırı sıcak veya soğuk bir ortamda kalması, sisteme fiziksel zarar verilmesi),
- İşlemsel yanlışlar (sistemde yapılan yanlış işlemler).

İnsanların sebep oldukları bu yanlışlar, kasıtlı veya kasıtsız olabilmektedir. İşletmeler, bilişim güvenliği için dikkatlerini işletme

[17] GUPTA ve HAMMOND, a.g.e., 2005, s.297.
[18] Gürol CANBEK, Şeref SAĞIROĞLU, "Casus Yazılımlar- Bulaşma Yöntemleri ve Önlemler", *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, Cilt No: 23, Sayı: 1, 2008, s.165.
[19] GUPTA ve HAMMOND, a.g.e., 2005, s.297.
[20] ONWUBIKO ve LENAGHAN, a.g.e., 2007, s.244.; GUPTA ve HAMMOND, a.g.e., 2005, s.297.
[21] ONWUBIKO ve LENAGHAN, a.g.e., 2007, s.244.

dışına yoğunlaştırmış olsalar da işletme çalışanları daha fazla zarar verebilecek ve yakalanması daha zor olan bir tehdit unsurudur[22].

İşletmelerin İnternet ortamında karşılaşabileceği gizlilik, bilgi bütünlüğü ve bilgi kayıpları ile ilgili güvenlik sorunları aşağıdaki gibi ortaya çıkabilmektedir[23]:

Gizlilik: Yanlışlıkla farklı adrese gönderilen bilgiler, hacking, pasif gözlenme (bilgilerin yetkili olmayan kişilerce gözlenmesi), e-ticaret bilgilerini içeren donanımların çalınması,

Bilgi Bütünlüğü: Yasal olmayan bilgi aktarımı, bilgilerin tekrarlanması, sistemin yanlış kullanımı, bilgi aktarımının çeşitli nedenlerle engellenmesi,

Bilgi Kayıpları: Yanlış yönlendirme, kontrol dışı dosya silinmesi (virüs veya hacking), dosyaların yanlışlıkla silinmesi, elektrik kesintisi veya donanım bozulması sonucu bilgi kaybı.

Küçük işletmeler, genellikle dünya genelinde yaygın olan Windows, Word ve Excel gibi popüler işletim sistemi ve yazılımları kullandıkları için daha çok saldırıya maruz kalabilmektedir[24].

V. GÜVENLİK ÖNLEMLERİ

İşletme yöneticileri, bilişim sistemlerinde meydana gelecek aksaklık ve saldırı sonuçlarının neler olabileceğini bilirlerse, güvenlik uygulamalarına daha fazla önem verebilirler[25]. Bu nedenle, KOBİ'lerde güvenliğin sağlanması için öncelikle işletme yöneticileri ve çalışanlarının bilişim teknolojileri güvenliği bilincinin sağlanması gerekmektedir. Güvenlik, sadece bir yazılım ve donanım konusu değildir, işletmede çalışan herkesin bu konuda sorumluluğu vardır[26].

---

[22] GUPTA ve HAMMOND, a.g.e., 2005, s.297-310.; STANTON ve diğerleri, a.g.e., 2005, s.124.

[23] Recep Baki DENİZ, *İşletmeden Tüketiciye İnternette Pazarlama ve Türkiye'deki Boyutları*, Beta Basım Yayım Dağıtım, 1. Baskı, İstanbul, 2001, s.69.

[24] KELLER ve diğerleri, a.g.e., 2005, s.7-19.; David A. BRADBARD, Dwight R. NORRIS, Paramjit H. KAHAI, "Computer Security in Small Business: An Empirical Study", *Journal of Small Business Management*, Cilt No: 28, Sayı:1, 1990, s.9.

[25] GUPTA ve HAMMOND, a.g.e., 2005, s.297.

[26] ÖZMEN, a.g.e., 2006, s.228.

İşletmelerde bilgi ve bilişim teknolojileri güvenliği sağlanırken, neyin, hangi tehdit ve tehlikelerden, ne derece korunması gerektiği, güvenliğin nasıl sağlanacağı ve alınacak önlemin maliyetinin değerlendirilmesinin yapılması gerekmektedir[27]. İşletmeler, hiçbir zaman yüzde yüz güvenliklerini sağlayamazlarsa da[28] bilişim teknolojileri güvenliğinin sağlanması ile ilgili alabilecekleri bazı önlemler bulunmaktadır. Bunlar, aşağıdaki gibi sıralanabilir [29]:

a) Kötü Amaçlı Yazılımlar İçin Korunma: Virüsler, solucanlar ve truva atları gibi zarar verme amaçlı yazılımlardan korunmak için öncelikle bilgisayarlarda bir anti-virüs programı yüklü olmalı ve bu program her zaman güncelleştirilmelidir. Ayrıca e-posta ile gelen şüpheli dosyalar açılmamalı ve e-posta programının güvenlik özellikleri kullanılmalıdır.

b) Yazılımların Güncellenmesi: Yaygın bir şekilde kullanılan işletim sistemleri ve yazılımların hataları ve açıkları kötü amaçlı kişilerce bunları kullanan kişilere zarar vermek amacıyla kullanılabilmektedir. Bunun için yazılımları üreten firmanın güvenlik açıklarını gideren güncelleme ve yamaları yüklenmelidir.

c) Fiziksel Güvenlik Önlemleri: Bilişim sisteminin fiziksel güvenliği sağlanmalıdır. Sunucu veya veritabanlarının bulunduğu oda herkese açık olmamalı ve havalandırması iyi olmalıdır. Ancak kullanım izni olanlar, sistemi kullanabilmelidir. İşletme içi ve gerekli görülürse işletme dışı bilgi ve/veya sistem yedeklemesi yapılmalıdır. Ayrıca, kesintisiz güç kaynağı kullanılmalıdır.

d) İyi Bir Şifreleme Politikası: İşletme tarafından önemli görülen dosyalar veya yazılımlar şifre ile korunmalıdır. Ayrıca çalışanlar iyi bir şifre seçme ve şifreyi koruma konusunda eğitilmelidir. İyi bir şifre, en az 8 karakterden oluşmakta olup küçük, büyük harf, rakam ve işaret (örneğin &) içermektedir. Fakat, karmaşık şifreler güvenlik için önerilse de bunların hatırlanması zor olduğundan bu durum güvenlik için bir ikilem oluşturmaktadır.

---

[27] ÖZMEN, a.g.e., 2006, s.230.; ONWUBIKO ve LENAGHAN, a.g.e., 2007, s.244.
[28] ÖZMEN, a.g.e., 2006, s.231.
[29] KELLER ve diğerleri, a.g.e., 2005, s.7.; ÖZMEN, 2006, 239, MICROSOFT, *Bilgisayar Güvenliği Denetim Listesi,* http://www.microsoft.com (12.10.2008)

e) Bilişim Teknolojileri İle İlgili Politika ve Eğitim: İşletmenin bilgisayar ve İnternet kullanımı ile ilgili ilkelerinin olması ve bu ilkelerin sıkı bir şekilde uygulanması gerekmektedir. Çalışanlar İnternet'te güvenli gezinme konusunda eğitilmeli ve İnternet kullanımı filtrelenmelidir. İşletmenin çalışanlar tarafından İnternet kullanımında aşağıdaki konulara çözüm bulması gerekir[30]:
   - Çalışanların iş amaçları dışında kişisel amaçlarla da İnternet'te gezinmesine izin verilip verilmediği,
   - Çalışanların İnternet'i kişisel amaçlarla kullanabileceği saatler,
   - İnternet kullanımının izlenip izlenmeyeceği, izleyecekse nasıl yapılacağı ve çalışanların bekleyebileceği gizlilik düzeyi,
   - İzin verilmeyen İnternet etkinlikleri ve İnternet'te kabul edilmeyecek davranışlar.

f) Ağ Güvenliği: İşletmenin her zaman açık olan geniş bant bağlantısı varsa İnternet üzerinden saldırıya uğrayabilir. Bu saldırıları engelleyebilmek için güvenlik duvarları kullanılabilmektedir. İşletmede kullanılan ağ için güçlü parola ve şifreler kullanılmalıdır. Ağın güvenliğini arttırmak ve yetkisiz erişimi önlemek için, kullanılmayan veya gereksiz ağ bağlantı noktaları kapatılmalıdır. Kablosuz ağ kullanılıyorsa güvenlik seçenekleri ayarlanmalıdır. İşletmenin sistemine işletme dışından erişen çalışanlar veya başka işletmeler varsa bu bağlantının güvenliği özel sanal ağ (virtual private network) gibi ağlarla sağlanmalıdır.

g) Sunucuların Güvenliği: Sunucuların fiziki güvenliği sağlanmalı ve kullanımı güvenlik altına alınmalıdır. Kullanıcılara, ihtiyaca uygun kullanım izni verilmelidir. Sunucuların güvenlik seçenekleri ayarlanmalıdır.

h) İşletme Uygulamalarının Güvenliği: İşletmeler, muhasebe, finans, pazarlama ve tedarik zinciri yönetimlerine özel sistemler kullanabilmektedir. Bu sistemler için de anti-virüs yazılımlarının kurulması, güvenlik duvarı, yazılım güncelleştirme, güçlü

[30] MICROSOFT, *Bilgisayar Güvenliği Denetim Listesi,* http://www.microsoft.com (12.10.2008)

şifreleme, yedekleme gibi temel güvenlik önlemleri alınmalı ve erişimleri sınırlandırılmalıdır.

Bilişim sistemlerinin ve İnternet trafiği güvenliğinin sağlanmasında olduğu gibi, kullanılan kelime işlemci, İnternet tarayıcıları ve veri tabanları vb. yazılımların da güvenlik özelliklerinin ayarlanması, çoğu kullanıcı tarafından yapılmamaktadır. Temel amacı güvenlik olmayan Word, Excel gibi yazılımlarda güvenlik seçenekleri genellikle kullanıcı arayüzünde değildir ve kullanıcı tarafından programın menusundan ulaşılması gerekmektedir. Çoğu kullanıcı, bu programları kullanırken güvenliğin sağlanması gerektiğini düşünmese de bunların da güvenlik seçeneklerinin ayarlanması gerekmektedir.[31]

Büyük işletmeler, bilgisayar sistemlerinin ve ağlarının güvenliğini sağlayacak teknik bilgi ve maddi güce sahipken, küçük işletmeler bu yeteneklere tamamıyla sahip olamamaktadır. Dolayısıyla küçük işletmeler, İnternet üzerindeki tehditlere daha açık ve daha savunmasız durumdadır. Bu nedenle küçük işletmelerin İnternet üzerindeki risklerini ve karşılaşabilecekleri zararları göz önüne alarak bütçesine uygun güvenlik önlemlerini alması gerekmektedir[32].

Küçük veya büyük işletmeler, bilgisayar kullandıkları ve İnternet'e bağlı oldukları müddetçe güvenlik riskleri ile karşı karşıyadır. Önemli olan, bu risklerin farkında olmak, gerekli yazılım ve donanım önlemlerini almak, çalışanları güvenlik tehditleri hakkında bilgilendirmek, devamlı olarak güvenlik tehditleri ile ilgili gelişmeleri takip ederek, en kötü durumlara karşı acil eylem planı ile hazır olmaktır[33].

Güvenlik problemleri nedeniyle bilişim sisteminin belirli bir zaman kullanılamaması işletmenin para, müşteri ve itibar kaybetmesine neden olabilmektedir. Küçük işletmeler, genellikle yedekleme için yeterli kaynak kullanmadığı için bilişim sistemlerinde istenilmeyen bir durum karşısında daha fazla risk altındadır. İşletmeler, bir dosyanın yanlışlıkla silinmesinden, bilgisayarların bozulmasına veya sistemin tamamen çökmesine kadar

[31] Steven FURNELL, "Why users cannot use security", *Computers & Security*, Cilt No: 24, 2005, s.274.
[32] SPINELLIS ve diğerleri, a.g.e., 1999, s.121.
[33] KELLER ve diğerleri, a.g.e., 2005, s.7.

karşılaşabilecekleri en kötü durumlara karşı hazırlıklı olmalıdır. İşletmelerin bir felaket yaşadıkları zaman bilgilerini kurtarabilmeleri için bir acil eylem planına sahip olmaları gerekmektedir. İstenmeyen durumlara karşı işletmeler, sadece bilgileri yedekleyebileceği gibi işletmede kullanılan sistemi de yedekleyebilmektedir.[34]

Yedekleme, işletme içi veya işletme dışı yapılabilmektedir. İşletme içi manyetik yedekleme ortamları, her zaman güvenli olmayabilir. Bellek teypleri, zaman içerisinde bozulabilmekte ve manyetik alanlardan etkilenmektedir. Ayrıca, işletmenin yangın, sel gibi bir felaket geçirmesi durumunda işletme içi yedek sistem de zarar görebilmekte, bilgiler kaybedilebilmektedir. İşletme dışı yedeklemeyi işletme kendisi yapabileceği gibi bu hizmeti satın da alabilmektedir[35].

VI. KOBİ'LERDE BİLİŞİM TEKNOLOJİLERİ GÜVENLİĞİNİ ETKİLEYEN ETMENLER

Allan ve diğerlerine göre çoğu KOBİ yöneticisi, bilişim ve güvenlik teknolojilerinin önemine ve faydasına inanmasına rağmen bazı KOBİ yöneticileri bu teknolojilerin işletmenin yürüttüğü işlevlerle pek ilgisi olmadığını düşünmekte ve bu teknolojileri kullanmaya karşı direnmektedir[36]. Çoğu zaman da işletme yöneticisi, teknolojiyi denemek için yeterince zaman ayıramadığından teknoloji hakkında yeterli bilgi edinememektedir.

Küçük işletmeler, büyük işletmelere göre daha sınırlı finansal olanaklara sahip oldukları için dünya genelinde yaygın olarak kullanılan işletim sistemi ve yazılımları kullandıklarından dolayı daha çok saldırıya maruz kalabilmekte ve saldırılardan daha fazla etkilenebilmektedir[37]. Büyük işletmeler bilişim teknolojileri güvenliğini arttırdıkça, güvenlik altyapıları büyük işletmeler kadar güçlü olmayan küçük işletmeler İnternet'te saldırganlar için hedef durumuna gelmektedir[38].

---

[34] KELLER ve diğerleri, a.g.e., 2005, s.7.
[35] KELLER ve diğerleri, a.g.e., 2005, s.7.
[36] ALLAN ve diğerleri, a.g.e., 2003.
[37] KELLER ve diğerleri, a.g.e., 2005, s.7.
[38] Jan GESSIN, "Introduction to Security and SME's", *OECD-APEC Workshop on Security of Information Systems and Networks - Seoul*, 5-6 Eylül 2005,

Küçük işletmelerin çoğunluğu, bilişim teknolojileri uzmanı istihdam edemediği gibi yöneticilerinin de bilgi güvenliği tehditlerinden ve bunların işletme faaliyetlerinde neden olacağı sonuçlardan çok az bilgisi vardır[39]. Gessin'e göre bazı KOBİ yöneticileri "bize bir şey olmaz" görüşünde olup[40];

- Kendilerinin çok küçük olduğu için İnternet'te bulunamayacağını düşünmektedir.
- İşletmelerinin saldırganların dikkatini çekmeyecek kadar küçük olduğunu düşünmektedir.
- Hiç kimsenin ilgisini çekecek bir şeyi olmadığını düşünmektedir.
- Yakınlarında saldırıya uğramış hiç kimse tanımamakta ve bu konudaki haberlerin çok abartılı olduğunu düşünmektedir.
- İnternet'ten alışveriş yapmadıklarından endişelenmeye gerek görmemektedir.
- İnternet'te çok kısa zaman kaldıkları için saldırıya maruz kalmayacağını düşünmektedir.
- Anti-virüs yazılımı ve güvenlik duvarını yeterli görmektedir.

Küçük işletme yöneticileri, genellikle kendilerini saldırganların dikkatini çekemeyecek kadar küçük olduklarını düşündüklerinden dolayı İnternet'te kendileri için risk görmese de günümüz kitlesel iletişim ortamında herkes ve her bilgi saldırganların dikkatini çekebilmektedir[41].

SONUÇ VE DEĞERLENDİRME

Günümüzde sunduğu fayda ve avantajlar nedeniyle bilişim teknolojilerin kullanımı işletmeler için kaçınılmaz hale gelmiştir. Fakat, hızla gelişen bu teknolojiler, çok çeşitli fayda ve avantajlar sağlamasının yanında bazı güvenlik sorunları ve tehditlerini de içermektedir. Bu çalışmada, KOBİ'lerde bilişim teknolojileri güvenliği çeşitli yönleriyle ele alınmıştır.

[39] KELLER ve diğerleri, a.g.e., 2005, s.7.
[40] GESSIN, a.g.e., 2005.
[41] KELLER ve diğerleri, a.g.e., 2005, s.7.

Büyük işletmeler, bilişim teknolojileri güvenliğini sağlayacak teknik bilgi ve maddi güce sahipken, küçük işletmeler bu yeteneklere tamamıyla sahip olamamaktadır. Bu nedenle küçük işletmeler, güvenlik tehditlerine daha açık ve daha savunmasız durumdadır. Dünya genelinde yaygın olan yazılımları kullanan KOBİ'ler, saldırganlar için kolay bir hedef olabilmektedir.

İşletmeler, bilişim teknolojilerini kullandıkları müddetçe çeşitli güvenlik tehditleri ile karşı karşıyadır. KOBİ sahip ve yöneticilerinin "bize bir şey olmaz" düşüncesi önemli bir güvenlik açığıdır. Bunun için KOBİ'lerde güvenliğin sağlanması amacıyla öncelikle yönetici ve çalışanların bilişim teknolojileri güvenliği bilincinin oluşturulması gerekmektedir. Güvenlik sadece teknik bir konu olmayıp, işletmede her kademedeki çalışanın bu konuda bir sorumluluğu bulunmaktadır. Güvenlik konusunda en önemli iş çalışanlara düşmektedir. Çalışanların bilinçli veya bilinçsiz neden olduğu zararlar en önemli bilişim tehditleri içerisindedir.

Bilişim teknolojileri güvenliği sağlanırken, neyin, hangi tehdit ve tehlikelerden, ne derece korunması gerektiği, güvenliğin nasıl sağlanacağı ve güvenlik önlemlerinin maliyetinin değerlendirilmesi gerekmektedir. Bu değerlendirmeler yapıldıktan sonra güvenlik önlemleri uygulamaya geçirilmelidir. Çalışmada bu önlemler üzerinde durulmuştur.

Bilişim sektörü dışında çalışan bir çok KOBİ, bilişim teknolojilerine ve bu teknolojilerin güvenliğine yabancıdır. KOSGEB vb. yetkili kurumlar ve örgütler KOBİ'lerde bilişim teknolojilerinin yaygınlaşması için sağladıkları teşvik ve eğitimler ile birlikte KOBİ'lerde bu teknolojilerinin güvenliği bilincinin sağlanması ve arttırılması konusunda da eğitim ve desteklerini sunmalıdır.

KAYNAKLAR

ALLAN Craig, ANNEAR Justin, BECK Eric, BEVEREN John Van "A Framework for the Adoption of ICT and Security Technologies by SMEs", *16th Annual Conference of Small Enterprise Association of Australia and New Zealand*, 2003.

BRADBARD David A., NORRIS Dwight R., KAHAI Paramjit H., "Computer Security in Small Business: An Empirical Study", *Journal of Small Business Management*, Cilt No: 28, Sayı:1, 1990, s.9.

CANBEK Gürol, SAĞIROĞLU Şeref, "Casus Yazılımlar-Bulaşma Yöntemleri ve Önlemler", *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, Cilt No: 23, Sayı: 1, 2008, s.165.

CARBONARA Nunzia, "Information and communication technology and geographical clusters: opportunities and spread", *Technovation*, Cilt No: 25, 2005, s.213.

CHAPMAN David, SMALOV Leon, "On Information Security Guidelines for Small/Medium Enterprises" ICEIS 2004, *Proceedings of the 6th International Conference on Enterprise Information Systems*, Porto, Portugal, 2004, s.3.

DAMASKOPOULOS Panagiotis, EVGENIOU Theodoros, "Adoption of New Economy Practices by SMEs in Eastern Europe", *European Management Journal*, Cilt No: 21, Sayı: 2, 2003, s.133.

DAYIOĞLU Burak, "Ağ ve işletim sistemi güvenliği", *Türkiye Bilişim Derneği 9. Bilgi İşlem Merkezi Yöneticileri Semineri (İMY9)*, 2002, Belek/Antalya.

DENİZ Recep Baki, *İşletmeden Tüketiciye İnternette Pazarlama ve Türkiye'deki Boyutları*, Beta Basım Yayım Dağıtım, 1. Baskı, İstanbul, 2001.

FURNELL Steven, "Why users cannot use security", *Computers & Security*, Cilt No: 24, 2005, s.274.

GESSIN Jan, "Introduction to Security and SME's", *OECD-APEC Workshop on Security of Information Systems and Networks - Seoul*, 5-6 Eylül 2005, http://www.oecd.org/dataoecd/11/18/35490254.pdf (13.10.2008).

GUPTA Atul, HAMMOND Rex, "Information systems security issues and decisions for small businesses: An empirical

examination" *Information Management & Computer Security*, Cilt No: 13, Sayı: 4, 2005, s.297.

HAWKINS Steve, YEN David C., CHOU David C., "Awareness and challenges of Internet security", *Information Management & Computer Security*, Cilt No: 8, Sayı: 3, 2000, s.131.

KELLER Shannon, POWELL Anne, HORSTMANN Ben, PREDMORE Chad, CRAWFORD Matt, "Information Security Threats and Practices in Small Businesses", *Information Systems Management*, Cilt No: 22, Sayı: 2, 2005, s.7.

LEE Jungwoo, "Discriminant analysis of technology adoption behavior: a case of internet technologies in small business", *The Journal of Computer Information Systems*, Cilt No: 44, Sayı: 4, 2004, s.57.

LEVY Margi, POWELL Philip, "SME Flexibility and the role of Information Systems", *Small Business Economics*, Cilt No: 11, 1998, s.183.

MICROSOFT, *Bilgisayar Güvenliği Denetim Listesi,* http://www.microsoft.com/turkiye/girisimci/themes/sgc/default.mspx (12.10.2008).

ONWUBIKO Cyril, LENAGHAN Andrew P., "Managing Security Threats and Vulnerabilities for Small to Medium Enterprises", *2007 IEEE International Conference on Intelligence and Security Informatics*, New Brunswick, NJ, A.B.D., 2007, s.244.

ÖZMEN Şule, *Ağ Ekonomisinde Yeni Ticaret Yolu, E-Ticaret*, İstanbul Bilgi Üniversitesi Yayınları, 2. Baskı, İstanbul, 2006.

SPINELLIS Diomidis, KOKOLAKIS Spyros, GRITZALIS Stephanos, "Security requirements, risks and recommendations for small enterprise and home-office environments", *Information Management & Computer Security*, Cilt No: 7, Sayı: 3, 1999, s.121.

STANTON Jeffrey M., STAM Kathryn R., MASTRANGELO Paul, JOLTON Jeffrey, "Analysis of end user security behaviors", *Computers & Security*, Cilt No: 24, 2005, s.124.

VOLPATO Giuseppe, STOCCHETTI Andrea, "The role of ICT in the strategic integration of the automotive supply-chain", *International Journal of Automotive Technology and Management*, Cilt No: 2, Sayı: 3/4, 2002, s.239.

YILDIZ Gültekin, ACILAR Ali, AYDEMİR Muzaffer, "İşletme Büyüklüğünün KOBİ'lerde İnternet Kullanımına Etkileri: Görgül Bir Araştırma" *6. Bilgi, Ekonomi ve Yönetim Uluslararası Kongresi*, İstanbul, Cilt II, 2007, s.959.