KURUMSAL BİLGİ GÜVENLİĞİ ve MUHASEBE BİLGİ SİSTEMİ

Doç. Dr. Ali ALAGÖZ*

Öğr. Gör. Metin ALLAHVERDİ**

ÖZET

Bilgi ve iletişim teknolojilerindeki gelişmeler, kurum ve kuruluşların elindeki mevcut bilginin muazzam ve büyük miktarlara ulaşmasına neden olmuştur. Bilişim teknolojilerinin gelişimi aynı zamanda internet kullanımını da artırmıştır. Bu durum, bilgiyi muhafaza eden sistemlerin ve onların altyapıları için önemli riskleri de beraberinde getirmektedir. Kötü niyetli uygulamaların da bu paralelde çoğalması ile kurum ve kuruluşların bilgi güvenliği konusuna önem vermelerine neden olmuştur. Yapılan bu çalışmada bilgi güvenliği kavramı genel olarak ele alınarak dünyada ve ülkemizdeki mevcut sorunlardan bahsedilmektedir. Çalışmada ayrıca, işletmelerin muhasebe uygulamalarında bilgi güvenliği alanında atılacak adımlar hakkında değerlendirmelerde bulunulmaktadır.

Anahtar Kelimeler: Bilgi Güvenliği, Muhasebe Bilgi Sistemi, Muhasebe Bilgi Sisteminde Bilgi Güvenliği.

Jel Kodlar: M40, M49

ABSTRACT

Improvements in information and communication technologies cause the present information that agencies and institutes have to reach to the enormous amount. Besides, development of information technologies have increased the usage of internet. This case leads to important risks for systems, which protect information, and their infastructures. Correspondingly, the increase of ill will applications cause organizations and

* *Öğretim Üyesi, Selçuk Üniversitesi, İktisadi ve İdari Bilimler Fakültesi*

** *Öğretim Görevlisi, Selçuk Üniversitesi, Beyşehir Ali Akkanat MYO*

institutes giving more importance to their own information security. In this study, dealing with the concept of information security generally, the current problems of our country and the world are semtinized. Furthermore, information systems of accounts, which is the new field in bookkeeping applications of managements, and things to do in these information systems' securities are examined in this study.

Keywords: Information Security, Accounting Information System, Information Security in Accounting Information System.

Jel Codes: M40, M49

1. Giriş

Dünyada ve ülkemizde bilgi ve iletişim sistemlerinin kullanımı hızla yaygınlaşmaktadır. Bilgi ve iletişim sistemleri, hayatımızın her alanının önemli bir parçası haline gelmekte, gerek kamu kurumları gerekse özel kuruluşlar verdikleri hizmetleri artık bilgi sistemleri üzerinden vermektedir. Bu sayede hem hizmet kalitesinin artırılması hem de iş verimliliğinin yükseltilmesi hedeflenmektedir. Kurum ve kuruluşların sundukları hizmetlerde bilgi ve iletişim sistemlerini giderek daha fazla kullanmaları ile birlikte, söz konusu bilgi ve iletişim sistemlerinin güvenliğinin sağlanması önem arz eden bir konu haline gelmiştir.

İşlerin ve süreçlerin sağlıklı yönetimi aynı zamanda ilgili bilgi güvenliği süreçlerinin de sağlıklı yönetimini zorunlu kılmaktadır. Bilgi güvenliği stratejileri ve bunları yönetecek uygun yöntemleri olmayan kurumlar, sadece güvenlik açısından değil, operasyonel ve diğer her türlü iş süreçlerinin yönetimi açısından da ciddi sıkıntılar, maddi ve/veya manevi kayıplarla yüzleşmektedir (Tipton ve Krause, 2007; 14).

Kurumlar için en kritik varlık bilgidir. Kurumların değerleri, sahip oldukları bilgi ile ölçülmektedir. Bilgi, sadece bilgi teknolojileriyle işlenen bir varlık olarak düşünülmemelidir. Bilgi bir kurum bünyesinde çok değişik yapılarda bulunabilmektedir. Dolayısıyla, bilgi güvenliğini sadece bilgi sistemlerinin güvenliği olarak değerlendirmemek gerekmektedir. Zira bilgi sadece sistemlerde bulunmamakta çeşitli ortamlarda yer almaktadır. Bu nedenle, bilgi güvenliği bilgi teknolojileri ile sınırlı tutulmamalıdır.

Bilgi güvenliği bir kurumun tüm departmanlarını kapsamaktadır. Bir departmanda meydana gelecek güvenlik açığı diğerlerini de önemli derecede etkileyebilmektedir. Kurumların tüm sırlarını bünyesinde barındıran muhasebe departmanı günümüzde bilgi güvenliğinden en etkili şekilde

faydalanmaktadır. Aksi durumda muhasebe bilgilerinin bulunduğu teknolojik değerlerle donatılmış sistemlerde bilgilerin zarar görme ihtimalleri yüksektir. Dolayısıyla kurumlar muhasebe bilgi sistemlerinde oluşan tehditleri ve alınacak önlemleri stratejik olarak hesaplamak zorundadırlar.

2. Bilgi Güvenliği Kavramı

İnternet, kişilerin değişik amaçlarla ve içerikte karşılıklı iletişim kurmalarını, bilgi alıp vermelerini sağlayan ortak bir haberleşme altyapısıdır (Alagöz, 2007: 12). Ocak 2008 itibariyle, internet sayesinde her kıtada 250'den fazla ülkede, hatta Antarktika da bile tahminen 541.700.000 bilgisayarı birbirine bağlandı. İnternet, bir ağ bağlantısı olan herkesin çeşitli şekillerde bir birine bağlandığı, bireysel bilgisayarlar tarafından erişilebilir gevşek bağlı şebekeler ve dünya çapında bir koleksiyondur. Bu durum, kişi ve kuruluşların ulusal ya da coğrafi sınırlarına günün saatine bağlı olmaksızın internet üzerinden herhangi bir noktadan ulaşabilmesini sağlamaktadır (http://www.us-cert.gov/reading_room/infosecuritybasics.pdf).

Bilgiye rahat ve kolay erişim beraberinde bazı riskler getirir. Bu riskler, değerli bilgilerin kaybolması, çalınması, değiştirilmesi veya kötüye kullanımı şeklinde olabilmektedir. Bilgi, elektronik ortamda kayıtlı ve ağ bilgisayarlarında kullanılabilir ise kağıtlara basılmış ve dosya dolabında kilitlenmiş bilgiden daha savunmasızdır. Davetsiz misafirlerin ofis veya evinize girmesi gerekmez; hatta aynı ülkede olmayabilir. Onlar kağıt ya da fotokopi parçasına dokunmadan bilgiyi çalabilir veya kurcalayabilir. Onlar kendi programlarını çalıştırarak ve izinsiz faaliyetlerini gizleyerek yeni dosyalar oluşturabilirler (http://www.us-cert.gov/reading_room/infosecuritybasics.pdf). Tüm bu saldırılar ve oluşturduğu risklerden korunmak amacıyla kurumlar için önemli olan bilgi ve belgeler yine ağ ortamında koruma altına alınmalıdır. Bilgi güvenliği kavramı kurumlar için önem taşıyan bilgilerin kötü kullanıcıların eline geçmesini engellemek için oluşturulan güvenlik tedbirleri ile birlikte ortaya çıkmıştır.

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 (Canbek ve Sağıroğlu, 2006: 168).

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" tanımlanılır. Bilgisayar teknolojilerinde güvenliğin amacı ise "kişi ve kurumların bu teknolojilerini kullanırken karşılaşabilecekleri tehdit ve tehlikelerin

analizlerinin yapılarak gerekli önlemlerin önceden alınmasıdır" (Canbek ve Sağıroğlu, 2006: 169).

Bilgi güvenliği, bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanmasını anlamına gelmektedir. Gizlilik, bütünlük ve erişilebilirlik bilgi güvenliğinin temel unsurları olarak değerlendirilebilir (Doğantimur, 2009: 7).

Gizlilik (Confidentiality): Bilginin yetkisiz kişilerce erişilememesidir.

Bütünlük (Integrity): Bilginin doğruluğunun ve tamlılığının sağlanmasıdır. Bilginin içeriğinin değiştirilmemiş ve hiçbir bölümünün silinmemiş ya da yok edilmemiş olmasıdır.

Erişilebilirlik (Availability): Bilginin bilgiye erişim yetkisi olanlar tarafından istenildiği anda ulaşılabilir, kullanılabilir olmasıdır.

Bu üç temel unsur birbirinden bağımsız olarak düşünülememektedir. Bilginin gizliliğinin sağlanması o bilginin erişilebilirliğini engellememelidir. Aynı zamanda erişilebilen bilginin bütünlüğünün de sağlanması önemlidir. Eğer bir bilgi için sadece gizlilik sağlanılıyor ve bilgiye erişim engelleniyor ise kullanılamaz durumda olan bu bilgi bir değer ifade etmeyecektir. Eğer erişimi sağlanıyor ancak bütünlüğü sağlanmıyor ise kurumlar ve kişiler için yanlış veya eksik bilgi söz konusu olacak ve olumsuz sonuçlara neden olabilecektir. Dolayısıyla bilgi güvenliği kavramı temel olarak bu üç unsurun bir arada sağlanması demektir (Doğantimur, 2009: 7).

Sonuç olarak bilgi güvenliği bilgiye sürekli erişimin sağlanması, bilginin göndericiden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlük içerisinde güvenli bir şekilde iletimi olarak tanımlanabilir (Pfleeger, 1997: 1).

2.1. Bilgi Güvenliğinin Önemi

Bilgi güvenliğinin sağlanmasına yönelik olarak kurumlar tarafından maddi yatırımlar yapılmadığında meydana gelen zararların ekonomik boyutu her geçen gün katlanarak artmaktadır. Bilgi güvenliği ihlallerinin meydana getirdiği zararlar yapılması gereken güvenlik yatırımlarıyla kıyaslandığında farkın çok büyük olduğu güvenlik firmalarının yapmış olduğu araştırmalar tarafından açıkça görülmektedir.

Uluslararası denetim ve danışmanlık firması Ernst & Young, Türkiye'nin de içinde bulunduğu 50'yi aşkın ülke ve çeşitli sektörlerden yaklaşık 1400 kuruluşun katılımıyla "2008 Küresel Bilgi Güvenliği Anketi" adlı bir çalışma gerçekleştirip bilgi güvenliğinin önemini vurgulayan sonuçlarını yayımlamıştır (http://www.computerworld.com.tr/bilgi-guvenliginin-neresindeyiz-detay_2107.html, 19.03.2011).

Ankette, bilgi güvenliğinin doğru uygulanmasının kurum itibarını doğrudan etkilediği sonucu ortaya çıkmıştır. Katılımcıların yüzde 85'i bir bilgi güvenliği ihlali durumunda ortaya çıkan durumun, marka kimliği ve itibarına zarar verdiğini savunurken, yüzde 72'si gelir kaybına neden olduğuna değinmiştir (http://www.computerworld.com.tr/bilgi-guvenliginin-neresindeyiz-detay_2107.html, 19.03.2011).

Söz konusu ankette Türk katılımcıların, bilgi güvenliğinin kağıt üzerinde bir zorunluluktan ibaret olmadığını düşündüğü görülmüştür. Bilgi Güvenliği Yönetimi Sistemi'ni, ISO 27001 gibi sertifikasyon amacı gütmeden kurduğunu belirtenlerin oranı, ankete katılanların yarısını oluşturmaktadır (http://www.pctime.com.tr/habergoster.asp?id=1950, 19.03.2011).

2.2 Bilgi Güvenliği İlkeleri

Bilgi güvenliği ilkeleri, kurumdaki bilgi güvenliği ile ilgili genel kuralları ortaya koyar. Bu ilkeler kullanıcılara çeşitli konu ve kavramlarla ilintili beklenen davranışları tanımlar. Bilgi güvenliği ilkeleri aşağıda başlıklar halinde açıklanmıştır;

Gizlilik (Confidentiality): Gizli bilginin yetkisi ve izni olmayan kişilerin eline geçmesinin engellenmesidir (Fussell, 2005: 2977). Gizlilik, statik ortamlar (disk, teyp, cd, dvd vb.) veya ağ üzerinde bir göndericiden bir alıcıya gönderilen dinamik ortamdaki veriler için sağlanmak zorundadır. Saldırganlar, yetkileri olmayan gizli bilgilere birçok yolla erişebilirler. Şifre dosyalarının bulunduğu veritabanlarının çalınması, sosyal mühendislik yöntemleriyle mümkün olabilir. Bilgisayar başında çalışan bir kullanıcı gözetlenerek ya da ona fark ettirmeden özel bir bilgisi (şifre v.b.) ele geçirilebilir. Gizlilik ilkesinin sağlanmasında şifreleme algoritmaları kullanılır. Algoritma belirli bir görevi yerine getiren sonlu sayıdaki işlemlerdir. Şifreleme algoritmasında, taraflardan biri şifreyi belirlerken diğer taraf algoritmayla bunu çözer ve gerekli bilgiyi elde eder.

Bütünlük (Integrity): Bilginin göndericiden çıktığı haliyle bir bütün olarak alıcısına ulaştırılmasıyla bütünlük ilkesi sağlanır (Fussell, 2005: 2977). Bilgi, haberleşme sırasında izlediği yollarda değiştirilmemiş, araya yeni veriler eklenmemiş, belli bir kısmı ya da tamamı tekrar edilmemiş ve sırası değiştirilmemiş şekilde alıcısına ulaştırılır. Verinin bütünlüğünün sağlanılması için özetleme algoritmaları kullanılmaktadır. Özetleme algoritmasında; uzunluğu belli olmayan bir metnin sabit uzunlukta özeti oluşturulur. Taraflar kullanacakları bilgiyi özetlenen bu bilgi şifresini algoritma yöntemiyle çözerek ulaşırlar.

Erişilebilirlik (Availability): Bilgiye zamanında erişim, bilgi sistemlerini kullanan kişiler tarafından büyük bir önem taşımaktadır. Bilgi sistemlerinden kendilerinden beklenen işlevi belirlenen bir zamanda yapmaları istenir. Bu başarım sayesinde elektronik işlemlere geçiş süreci hızlanır. Erişilebilirlik hizmeti, bilişim sistemlerini, kurum içinden ve dışından gelebilecek erişilebilirliği düşürücü tehditlere (Denial of Service Attack- DOS, DDOS) karşı korumayı hedefler. Bu bileşen sayesinde, kullanıcılar erişim yetkileri dâhilinde olan verilere güncel, zamanında ve hızlı bir şekilde ulaşabilirler. Sistem erişilebilirliği, bilgisayar yazılımlarındaki hatalar, sistemin yanlış, bilinçsiz ve eğitimsiz personel tarafından kullanılması veya konfigüre edilmesi, doğal felaketler gibi faktörleden etkilenebilir (Fussell, 2005: 2977). Sisteme erişilebilirliğin sürekli sağlanması için fiziksel önlemlerin yanısıra güvenlik duvarları, atak tespit sistemleri, antivirüs yazılımlarından yararlanılmalıdır.

Kimlik Tespiti (Authentication): Bilgi güvenliğinin bir diğer ilkesi olan kimlik tespiti ise "bilgi sistemlerinden hizmet alan alıcının, iddia ettiği kişi olduğundan emin olunması" anlamına gelmektedir (Marcinkowski ve Stanton, 2003: 2528). Örneğin, izniniz olan herhangi bir ortama eriştiğinizde size sorulan şifreler, bilgisayarınızı açarken şifre girilmesi kullanıcının kimliğinin tespit edilmesinde yararlanılan yöntemlerdir. Günümüzde kimlik tespiti, sadece bilgisayar ağları ve sistemleri için değil, fiziksel sistemler için de çok önemli bir hizmet haline gelmiştir. Akıllı kartlar, one time password (tek kullanımlık şifre), token (simge), biyometrik teknolojiler kimlik tespitinde kullanılan diğer teknolojilerdir.

Güvenirlik (Reliability): Bilgisayar sistemlerinden beklenen davranış ile elde edilen sonuçlar arasındaki tutarlılık durumudur (Marcinkowski ve Stanton, 2003: 2528). Başka bir deyiş ile güvenirlik, sistemden ne yapmasını bekliyorsak, sistemin kendisinden beklenileni yapmasını ve her çalıştırıldığında da aynı şekilde davranması olarak tanımlanabilir. Örneğin, ağ içerisinde yer alan dağıtıcı anahtardan sürekli çalışması beklenmektedir. Cihazın çalıştığı zaman dilimi ile çalışması gereken zaman dilimi kıyaslanarak cihazın güvenirliği ortaya çıkarılabilir.

İnkâr Edememe (Non-Repudiation): Bu bileşenle, ne gönderici alıcıya bir mesajı gönderdiğini, ne de alıcı göndericiden bir mesajı aldığını inkâr edebilir. Bu hizmet, özellikle gerçek zamanlı işlem gerektiren bankacılık ve finans bilgi sistemlerinde kullanım alanı bulmaktadır. Gönderici ile alıcı arasında ortaya çıkabilecek anlaşmazlıkların en aza indirilmesini sağlamaya yardımcı olmaktadır. Sayısal imza teknikleriyle inkâr edememe ilkesi sağlanır (Campbell, 2003: 238).

2.3. Bilgi Güvenliğinin Amacı

Bir bilgi sistemi güvenlik programının amacı, bilginin kabul edilir bölümünün gizlilik, doğruluk ve uygunluk kaybı riskini azaltarak korumaktır (INTOSAI, 1995: 7).

Bilgi güvenliğinin amacı, kullanılabilirlik, gizlilik ve bütünlük hatalarından kaynaklanan zarardan, bilgiyi sunan sistemler ve iletişimlerden, bilgi kullanıcılarının çıkarlarına dayanarak onu korumaktır (Salazar, 2006: 2).

3. Kurumsal Bilgi Güvenliği

Bilgi güvenliği, bilgiye sürekli olarak erişilebilirliğin sağlandığı bir ortamda, bilginin göndericisinden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlüğünün sağlanması ve güvenli bir şekilde iletilmesi süreci olarak tanımlanılmaktadır. Kurumsal bilgi güvenliği ise, kurumların bilgi varlıklarının tespit edilmesi, bilgi sistemlerindeki zaafiyetlerinin belirlenmesi ve istenmeyen tehdit ve tehlikelerden korunma amacıyla gerekli güvenlik analizleri yapmak ve önlemler alma olarak düşünülebilir (Vural ve Sağıroğlu, 2008: 509).

Öncelikle bu tanımda geçen bilgi varlıkları sözcüğünün içerdiği anlam önemlidir. Bilgi varlığı, kurumun sahip olduğu, kurumun işlerini aksatmadan yürütebilmesi için önemli olan varlıkları ifade etmektedir. Bu bilgi varlığı, kurumun bilgi sistemlerinde yer alan bir veri olabileceği gibi, çalışanların veya yöneticilerin masasının üzerinde bulunan bir kağıtta ki notlar, bilgisayarında kayıtlı bir dosyada olabilir (Doğantimur, 2009: 8-9).

Kurumsal bilgi güvenliği insan faktörü, eğitim, teknoloji gibi birçok faktörün etki ettiği tek bir çatı altında yönetilmesi zorunlu olan karmaşık süreçlerden oluşmaktadır (Doğantimur, 2009: 9).

Bilgi güvenliği, sadece bir Bilgi Teknolojisi (BT) ya da yaygın söylemle Bilgi Sistemleri işi değildir; kurumun her bir çalışanının katkısını ve katılımını gerektirir. Ciddi boyutta bir kurum kültürü değişimi gerektirdiği için, en başta yönetimin onayı, katılımı ve desteği şarttır. BT'nin teknik olarak gerekli olduğunu saptadığı ve uyguladığı teknik güvenlik çözümleri, iş süreçleri ve politikalarla desteklenmemiş ve kurum kültürüne yansıtılmamışsa etkisiz kalacaklardır. Gerekli inanç ve motivasyon yaratılamamışsa, çalışanlar şifrelerini korumakta özensiz, hassas alanlarda gördükleri yabancı kişilere karşı aldırmaz, kağıt çöpüne gerekli imha işlemini yapmadan atacakları bilgilerin değeri konusunda dikkatsiz olabilecekler ve yapılan güvenlik yatırımlarına karşın büyük bir açık oluşturmaya devam edebileceklerdir (http://www.infosecurenet.com/macroscope/macroscope6.pdf. 04.04.2011).

3.1 Kurumsal Bilgi Güvenliği Oluşturma Süreci

Kurumsal yönetim anlayışının getirdiği yenilikle bilgi sistemlerinde güvenliğin sağlanması için bilgi güvenlik politikasının hazırlanması ile başlayan süreç aşağıdaki temel adımları izleyecektir (Ünal, 2006: 13).

1. Politika Oluşturulması: Bilgi güvenliğinin sağlanması için gerekliliklerde göz önüne alınarak Bilgi Güvenlik Politikası hazırlanmalıdır. Bu adım Özellikle 3. adımdan sonraki faaliyetler ile sağlanacak geri dönüşlerle güncellemeye tabi olacaktır.

2. Planlama ve Kaynak Tespiti: Planlama ve Kaynakların Tespiti olarak adlandırılan çalışma ile politikanın uygulanması için organizasyonel yapının oluşturulması, rol ve sorumlulukların belirlenerek, belgelenmesi ve gerçekleştirilmesi yapılmalıdır.

3. Risk Yönetimi: Risk Yönetim Çalışması içerisinde birden fazla aktiviteyi kapsayan bir risk analizi çalışması ile; varlıklar tespit edilerek, sınıflandırılması sağlanmalı, varlıkların karşı karşıya olduğu riskler tespit edilmelidir.

4. Uygulama: Bilgi güvenlik planları uygulamaya alınmalı ve gerekli eğitimler verilmelidir.

5. Geri Bildirim-Gözden Geçirme: Uygulama sonuçları ile tüm bilgi güvenlik yapısı; politikalar, prosedürler, risk yönetimi, bilgi güvenlik planları gözden geçirilmeli ve periyodik olarak güncellenmelidir.

4. Dünyada ve Türkiye'de Mevcut Durum

Symantec'in yaptığı araştırmaya göre, dünya genelinde 2008 yılı boyunca yeni tehditlerin yayılması ve amacına ulaşmasında internet ortamı ve web sitelerinin yine ana kaynak olarak kullanıldığını özellikle vurgulanmıştır. Aynı çalışmada, saldırganların bu tehditleri geliştirirken ve kullanıcılara yöneltirken eskisine oranla çok daha fazla "kişiye özel" zararlı kod aktiviteleri düzenlediklerinin de altı çizilmektedir. Dahası, 2008 yılı boyunca Symantec firması tarafından saptanan tüm saldırıların neredeyse %90'ı, kullanıcıya ait kritik bilgilerin çalınması amacını taşımaktadır. Klavye tuş basımlarının kaydedilmesi yolu ile çevrim içi banka hesap bilgileri gibi kritik bilgilerin çalınmasına yönelik aktiviteler, saldırıların %76'sını oluşturmaktadır ki bu oran, 2007 yılında %72 olarak saptanan oranla kıyaslandığında, bir senede yaşanan artışı açıkça ortaya koymaktadır (Eminağaoğlu ve Gökşen, 2009; 3).

Aynı araştırmada ülkemizle ilgili çarpıcı istatistiksel değerler ve bulgular da mevcuttur. Geçmişte herhangi bir saldırı yaşadıklarını ifade eden Tür-

kiye'deki kurumların %50'si, saldırının "sistemin durmasına neden olduğunu" belirtmiştir. Sistemi duran kurumların %50'inde ise 8 saati aşan bir kesinti yaşanmıştır. Herhangi bir saldırıya maruz kalan kurumların % 35'i, bu saldırının "bilgi kaybına" neden olduğunu belirtirken, %10'u ise "sistemin yavaşladığını" belirtmişlerdir (Eminağaoğlu ve Gökşen, 2009; 3)

Bu araştırmanın dikkat çekici bir tarafı da, Türkiye'nin bilgi güvenliğindeki dünyadaki konumuna ait verilerdir. 2008 yılında, Türkiye geneli güvenlik saldırıları, dünya bazında çok kaygı verici bir düzeyde olduğu bulgulanmaktadır. Örnek vermek gerekirse; 2008 yılında bir önceki yıla göre ülkemizdeki zararlı kod saldırıları 2 misline yakın artmış, dünyadaki tüm zararlı kod eylemlerinin %6'sını oluşturarak genel sıralamada 9. sıraya yükselmiştir (Eminağaoğlu ve Gökşen, 2009; 3-4). (Bknz. Tablo 1)

Symantec'in 2009 raporuna göre, çöp (İng. spam) e-posta eylemleri de Türkiye'de bir önceki yıla göre yaklaşık 3 kat artarak dünya genelinde 3., Avrupa-Orta Doğu (EMEA) bölgesinde de 2. sıraya yükselmiştir (Bknz. Tablo 2). Ama diğer dereceye giren ülkelere göre Türkiye'nin internet hat kullanım kapasiteleri ve internet kullanıcısı sayısı oranları göz önüne alındığında, aslında Türkiye'nin dünyadaki diğer tüm ülkelerden daha yüksek düzeyde bilgi güvenliği sorunları yaşadığı anlaşılmaktadır (Eminağaoğlu ve Gökşen, 2009; 4). Microsoft'un yaptığı araştırmaya göre Türkiye, son birkaç senedir dünyada 1000 bilgisayar başına düşen kötücül yazılım enfeksiyonu oranı itibarıyla en fazla enfeksiyona rastlanan ülkeler arasında yer alıyor. Son rapor sonuçlarına göre de Türkiye geçtiğimiz bir sene içerisinde 1000 bilgisayara 36.8 enfekte cihaz oranı ile lider olurken, İspanya (36.1), Kore (34.8), Tayvan (29.7) ve Brezilya (24.7) oranları ile Türkiye'yi izledi. Ayrıca önceki dönemlere ait raporlarda Türkiye, SQL Enjeksiyonu olarak tabir edilen saldırı kategorisinde zafiyet taşıyan ".tr" uzantılı 88.378 sayfa adedi ile de maalesef açık ara dünya lideriydi. Tüm ".com" uzantılı alanda bile 43.144 adet bu zafiyeti taşıyan sayfa mevcutken Türkiye'de bunun iki katına denk gelen zafiyeti taşıyan sayfa sayısının bulunması ciddi bir güvenlik tehdidini beraberinde getiriyor. (http://blog.microsoft.com.tr/turkiyede-bilgi-guvenligi.html, 23.06.2011)

Symantec araştırmasınınnın ülkemizle ilgili ortaya koyduğu çarpıcı sonuçlardan birisi de, 2008 yılında virüs tipindeki zararlı kodların üretildiği ve yayılma kaynağı olarak çıktığı ülkeler arasında Türkiye, Avrupa-Orta Doğu bölgesi genelinde 2. sırada yer almaktadır (Symantec, 2009: 26). (Bknz. Tablo 3)

Tablo 1: 2007 ve 2008'de dünya genelinde zararlı kodların tiplerine göre sıralamalar ve genel sıralamalar

2008 tüm saldırı tipleri Dünya sıralaması	2007 tüm saldırı tipleri Dünya sıralaması	Ülke	2008 tüm saldırı tipleri içinde oranı	2007 tüm saldırı tipleri içinde oranı	Zararlı kod	Spam yayıcı sistem	Phishing web siteleri	Bot sistemler	Tüm saldırılar geneli
1	1	ABD	23%	26%	1	3	1	2	1
2	2	Çin	9%	11%	2	4	6	1	2
3	3	Almanya	6%	7%	12	2	2	4	4
4	4	Birleşik Krallık	5%	4%	4	10	5	9	3
5	8	Brezilya	4%	3%	16	1	16	5	9
6	6	İspanya	4%	3%	10	8	13	3	6
7	7	İtalya	3%	3%	11	6	14	6	8
8	5	Fransa	3%	4%	8	14	9	10	5
9	15	Türkiye	3%	2%	15	5	24	8	12
10	12	Polonya	3%	2%	23	9	8	7	17

Kaynak: *Symantec Global Internet Security Threat Report Trends for 2008, 2009, s. 18.*

Tablo 2: Dünya geneli ve Avrupa-Orta Doğu bölgesinde çöp (spam) e-posta oranları ve Sıralamaları

2008 Avrupa ve Ortadoğu Sıralaması (spam)	2007 Avrupa ve Ortadoğu Sıralaması (spam)	2008 Dünya Geneli Sıralama (spam)	Ülke	2008 Avrupa ve Ortadoğu Oranları (spam)	2007 Avrupa ve Ortadoğu Oranları (spam)
1	3	2	Rusya	14%	10%
2	8	3	Türkiye	13%	4%
3	1	6	Birleşik krallık	7%	15%
4	4	7	Almanya	6%	9%
5	5	8	İtalya	6%	6%
6	2	9	Polonya	6%	10%
7	6	10	İspanya	5%	6%
8	7	13	Fransa	5%	6%
9	20	19	Romanya	3%	1%
10	10	20	Hollanda	3%	1%

Kaynak: *Symantec EMEA Internet Security Threat Report, 2009, s. 39*

Tablo 3: Truva atı, virüs, arka kapı ve solucan tipinde zararlı kod saldırılarında ilk 3 sıradaki ülkeler

Sıralama	Zararlı kod türlerinde ilk 3 sıra (Avrupa ve Ortadoğu bölgesi geneli)			
	Arka Kapı	Truva Atı	Virüs	Solucan
1	Birleşik Krallık	Birleşik Krallık	Mısır	Suudi Arabistan
2	İspanya	Fransa	Türkiye	Birleşik Krallık
3	Fransa	Almanya	Birleşik Krallık	İspanya

Kaynak: *Symantec EMEA Internet Security Threat Report, 2009, s. 26*

5. Muhasebe Bilgi Sisteminde Bilgi Güvenliği

Bilgi sistemleri önceleri sadece işletme içi bilgi akışını sağlamak amacıyla kullanılmakta iken rekabetin artması ve özellikle de teknolojik gelişimlerin de etkisiyle hem işletme içi hem de işletme dışından olan bilgi akışını yürütme amacına yönelik olarak tasarlanmakta ve kullanılmaktadır. Günümüzde bilgi sistemlerinin alt yapısını oluşturan en önemli unsur teknolojik alt yapı olarak karşımıza çıkmaktadır. Gerek kullanılan donanımlar gerekse de bilgisayar yazılımları günümüz bilgi sistemlerinin vazgeçilmez unsurlarıdır. Bilgisayarların gündelik yaşamımızdaki yerinin artmasıyla birlikte, işletmeler de bilgisayarların sağlamış oldukları kolaylıkları bünyelerine taşımaya başlamışlardır. Önceleri, işletmelerdeki tek elektronik alet hesap makinesi iken günümüzde işletmeler insan eli değmeden sadece bilgisayarlar kontrolünde üretim yapabilir duruma gelmişlerdir. Hatta bilgisayarlar sadece programlandıkları rutin işleri yapmanın dışında karar destek sistemleri olarak karar alıcıların karar almalarına yardımcı olmakta; yapay zeka sistemleri olarak olası işletme stratejilerinin geliştirilmesinde büyük rol oynamaktadırlar (Karagül, 2005: 73-75).

Finansal muhasebe ve raporlama, maliyet ve yönetim muhasebeleri, denetim ve vergi gibi muhasebenin temel konularının bu değişimlerin etkilerinin bir uzantısı olarak işletmelerde uygulanan sistemlerin yeni teknolojilerle entegrasyonu bir gereksinim olarak ortaya çıkmıştır (Gökdeniz, 2005: 86). Diğer yandan bilgi teknolojilerindeki gelişmeler, yönetici-müşteri ve üçüncü kişilerin gerek duydukları muhasebe bilgisinin yapısını da değiştirmiş, bu durum da muhasebede yeni kavram ve yaklaşımların ortaya çıkmasına neden olmuştur (Türk, Aygen ve Yıldız, 2009: 240).

İşletmede iyi bir yönetim doğru ve zamanlı bilgiye dayanır. Zamanlı, anlamlı ve doğru bilgiler, yönetim tarafından işletme faaliyetlerinin izlenmesinde, planlama, örgütleme ve kontrol gibi işlevlerin yerine getirilmesinde

çok önemli görevler üstlenmektedir. Çünkü bilgisizce, ileriye dönük planlar hazırlamak, uygulamak ve kontrol işlemleri yapmak imkânsızdır. Muhasebe bilgi sistemi de işletme yönetiminin karar almasında zamanlı ve doğru bilgi sunan bir sistemdir (Civan ve Kara, 2003: 111).

5.1. Muhasebe Bilgi Sistemi Kavramı

Muhasebe, gözlediği olaylar ve bu olaylara ilişkin ürettiği bilgiler açısından çok kapsamlı bir süreçtir. Muhasebe çeşitli kurumlarda karar alma durumunda olan kişiler için finansal bilgiler sağlayan bir süreç olarak tanımlanabilir. Bu süreç, karar alma durumunda olanların tutarlı karar alabilmeleri amacıyla varlıklar, kaynaklar ve faaliyet sonuçlarına ilişkin doğru ve güvenilir bilgileri zamanında sağlama amacına yönelik olarak faaliyet gösterir (Yılmaz, 2005: 96). Öte yandan muhasebe bilgi sistemi, muhasebe işlevinde başarı sağlamak için tasarlanmış bir bilgi sistemdir (Dalcı ve Danış, 2004: 47).

Muhasebe bilgi sistemi ile ilgili diğer bazı tanımlar şöyledir:

- Muhasebe bilgi sistemi; işletmelerde bilgi kullanıcılarına, planlama, kontrol ve işletmenin faaliyetlerini sürdürmede ihtiyaç duyacakları bilgileri sağlayan bir veri işleme sürecidir (Romney ve diğerleri, 1997: 2).

- Muhasebe bilgi sistemi, işletme hakkında karar verecek olan taraflar için, isletmenin ekonomik faaliyetleri ile ilgili verileri toplayan, işleyen, depolayan ve ilgililere sunan bir bilgi sistemidir (Julie ve diğerleri, 1999: 7).

- Muhasebe bilgi sistemin, işletme içi ve işletme dışı finansal bilgi kullanıcılarına, işletme faaliyetlerinin sağlıklı bir şekilde devam ettirilmesi, planlanması ve denetlenmesi için gerekli olan bilgileri finansal tablolarla sunan bir bilgi sistemidir (Dinç ve Varıcı, 2008: 70).

Yukarıdaki tanımlar sonucunda oluşan ortak tanıma göre, muhasebe bilgi sistemi (MBS), işletmenin varlıkları ve bu varlıkların kaynakları olan sermaye ve borçlar üzerinde değişme yaratan mali nitelikli işlemlere ait verileri toplayan, toplanan verileri süreçleyerek (işleyerek) bilgiye dönüştüren ve ortaya çıkan bilgileri raporlayan bir bilgi sistemdir (Sürmeli, 2005: 43).

5.2. Muhasebe Bilgi Sisteminde Güvenlik İhtiyacı

Son dönemlerde muhasebe bilgi sistemlerinin bilgi teknolojileri ile birleşmelerinden meydana gelen gelişmeler işlemlerin dijital ortamda yapılmasına neden olmuştur. Bu bağlamda; kâğıt, kalem ve bağımsız veri tabanları üzerinde depolanan verilere dayalı geleneksel muhasebe süreci yerini; elektronik veri değişimi, elektronik fon transferi, internet, intranet,

extranet, genişletilebilir biçimleme dili, genişletilebilir işletme raporlama dili, ilişkisel veri tabanı yönetim sistemleri, web araçları gibi bilgi ve iletişim teknolojilerinin kullandığı, işlerin bütünleşik veri tabanlarında ve web platformunda entegre olarak yürütüldüğü dijital uygulamalara bırakmıştır (Sevim, 2009: 4-5). Bilgisayarlı ortam muhasebe işlemlerini hızlandırma, kolaylaştırma ve güncelleme ile bilgi iletiminde kolaylık ve hız kazandırması yanında birçok güvenlik sorununu da beraberinde getirmiştir. İşletmenin bütün departmanlarındaki bilgisayarların iletişim ağlarıyla birbirlerine bağlanması ve Internet ile dış dünyaya açılması ile de güvenlik sorunları daha da artmıştır. Bu nedenle işletmeler yaşamları için çok önemli olan muhasebe bilgilerinin bilgisayarlı ortamdaki güvenliğini sağlamak için gerekli önlemleri almak zorunda kalmaktadırlar.

Muhasebe bilgi sisteminin güvenliğini sağlamak için öncelikle sistemi tehdit eden unsurların neler olduğunu belirlemek gerekmektedir. Muhasebe bilgi sisteminde yer alan ve dolaşan her türlü veri ve bilgi, hataların ve özellikle de hilelerin tehdidi altındadır. O halde burada hemen şu saptamayı yapabiliriz: Öncelikli hedef, sistemin hatalara ve hilelere açık bir yapıda olmamasını sağlamaktır.

5.3. Muhasebe Bilgi Sisteminde Bilgi Güvenliğini Tehdit Eden Unsurlar ve Bilgi Güvenliğinin Sağlanması

Teknolojik gelişmeler muhasebe bilgi sistemlerinde yeni güvenlik tehditleri yaratmıştır. Bunlar (Abu-Musa, 2003: 9):

— Bilgi gizliliğinin/mahremiyetinin kaybı,

— Bilginin çalınması,

— Onaylanmamış bilgi kullanımı,

— Bilginin ve bilgisayarların hileli kullanımı,

— Onaysız (kasti) değiştirme ya da veri manipülasyonunun sonucu olarak bilgi bütünlüğünün kaybı,

— Onaylanmamış ya da kasti, kötü niyetli hareketlere bağlı işlem hatası şeklinde sıralanabilir.

Doğru, tam ve güvenilir muhasebe bilgileri elde edebilmek için sadece bilgi oluştuktan sonra değil, verinin bilgisayara girilmesi, işlenmesi ve bilgiye dönüşüm süreçlerinde de gerekli önlemler alınmalıdır. Bu nedenle bilgisayarlı ortamdaki muhasebe veri/bilgilerinin güvenliği için (Demir, 2005: 151);

— Ağ güvenliği (Intranet ve Internet)

— Sistem güvenliği

— Veri güvenliği sağlanmalıdır.

İşletmelerin hayati önem taşıyan bilgi toplama ve depolama kaynağı olan muhasebe bilgi sistemi verilerinin, özellikle yönetim muhasebesi açısından alınacak kararlara etki edecek mali tabloların oluşturulmasında kullanılan veriler ile işletme faaliyetlerinin sürekliliğini sağlayan verilerin, başka veri depolama sistemlerinde, özellikle işletme binasının bulunduğu alanlardan başka alanlarda depolanarak korunması gerekmektedir.

İşletmelerde kurulan sistemler mutlaka denetlenmeli ve yeni süreçlere göre güncellenmelidir.

Ayrıca, güvenilir bir bilgi sisteminin sağlanması için etkin bir iç kontrol sisteminin oluşturulması ve sürekliliğinin sağlanması da gerekmektedir.

Bunlardan birisinde gerekli güvenlik önlemlerinin alınmamış olması, diğerlerini de etkilemektedir. İşletmelerde bilgisayarlar ağ yoluyla birbirlerine bağlı oldukları için bilgisayar sisteminin güvenliğini ve uygulama güvenliğini sağlamak, özellikle ağ güvenliğinin sağlanmasına bağlıdır.

Muhasebe bilgi güvenliğini sağlamak için güvenlik hizmetleri sunan şirketler ile de çalışılabilir. İşletmenin güvenlik işini kendisinin yapmasının maliyeti yüksek ise güvenlik işini bu şirketlere devretmesinde yarar olacaktır.

Sadece teknolojik önlemlerle (anti-virüs, güvenlik duvarı sistemleri, kripto vb.) iş süreçlerinde bilgi güvenliğini sağlama olanağı yoktur. Bilgi güvenliği, süreçlerin bir parçası olmalı ve bu bakımdan bir iş anlayışı, yönetim ve kültür sorunu olarak ele alınmalıdır. Her kurum mutlaka birey-sel olarak ve kurum bazında bir güvenlik politikası oluşturmak, bunu yazılı olarak dökümante etmek ve çalışanlarına, iş ortaklarına, paydaşlarına aktarmak zorun-dadır. Tüm çalışanlar bilgi güvenliği konusunda bilinçli olmalı, erişebildikleri bilgiye sahip çıkmalı, özenli davranmalı, üst yönetim tarafından yayınlanan "Bilgi Güvenliği politikası" şirket açısından bilgi güvenliğinin önemini ortaya koymalı, sorumlulukları belirlemeli, çalışanları bilgilendirmeli ve BG sistemi, iş ortaklarını (müşteri, tedarikçi, taşeron, ortak şirket vb.) da kapsamalıdır (http://www.bilgiyonetimi.org/cm/, 01.05.2011).

6. Sonuç

21. yüzyılın en önemli değerlerinin başında "Bilgi" gelmektedir. Bilginin "güvenirliği" ise onun değerini azaltmakta, ya da arttırmaktadır. Bu bilginin

gerçekten değerli olabilmesi için "ehil" eller (ya da akıllar) tarafından üretilmesi gereklidir. Bilginin istenen yer ve zamanda kullanılabilmesi için de hem güvenilir bir korunma (arşivleme), hem de süratli bir erişim sistemine ihtiyaç vardır. Keza, mevcut bilgilerin yanlış manüplasyonlarla (sahtekarlıklarla) kirletilmemesi de büyük önem arz etmektedir.

Bilgi güvenliğinin sağlanmasında ve güvenlik kültürünün oluşturulmasında en zayıf halka insandır. İnsan faktörü uygun ve yeterli seviyede güvenliğin sağlanmasında anahtar role sahiptir. Bu çerçevede siber dünyanın olası tehdit ve tehlikeleri konusunda toplumun her kesiminin bilinçlendirilmesi ile toplumda bilgi güvenliği şuuru ve farkındalığının oluşturulmasına yönelik önlemlerin alınması gerekmektedir.

Başarılı ve etkin bir bilgi güvenliği yönetimi; üst yönetimin desteği ve sahiplenmesi, çeşitli eğitimler ve yönetimsel düzenlemelerle tüm çalışanların bilinçlendirilmesi, kurum için öncelikli riskler ve bu riskleri azaltacak uygun çözümlerin belirlenmesi, bu çözümlerin o kuruma en uygun şekilde uygulatılması, bu uygulamaların periyodik olarak denetlenmesi ve bunların sonucunda gerekli iyileştirmelerin yapılarak sürekli gelişim ve değişim sonucunda sağlanabilir.

İşletmede iyi bir yönetim doğru ve zamanlı bilgiye dayanır. Zamanlı, anlamlı ve doğru bilgiler, yönetim tarafından işletme faaliyetlerinin izlenmesinde, planlama, örgütleme ve kontrol gibi işlevlerin yerine getirilmesinde çok önemli görevler üstlenmektedir. Çünkü bilgisizce, ileriye dönük planlar hazırlamak, uygulamak ve kontrol işlemleri yapmak imkânsızdır. Muhasebe bilgi sistemi de işletme yönetiminin karar almasında zamanlı ve doğru bilgi sunan bir sistemdir.

Son dönemlerde muhasebe bilgi sistemlerinde meydana gelen gelişmeler işlemlerin dijital ortamda yapılmasına neden olmuştur. Bu bağlamda; kâğıt, kalem ve bağımsız veri tabanları üzerinde depolanan verilere dayalı geleneksel muhasebe süreci yerini; elektronik veri değişimi, elektronik fon transferi, internet, intranet, extranet, genişletilebilir biçimleme dili, genişletilebilir işletme raporlama dili, ilişkisel veri tabanı yönetim sistemleri, web araçları gibi bilgi ve iletişim teknolojilerinin kullandığı, işlerin bütünleşik veri tabanlarında ve web platformunda entegre olarak yürütüldüğü dijital uygulamalara bırakmıştır.

Muhasebe bilgi sistemlerinde bilgilerin bilgisayarlı ortamda üretilmesi, raporlanması ve ilgili kişilere sunulması sağladığı avantajlar yanında çeşitli güvenlik sorunlarını da beraberinde getirmiştir. Muhasebe bilgi sistem-

lerine güvenlik tehdidi, işletme içinden olabileceği gibi, faaliyetlerinde internet'in kullanımı sebebiyle işletme dışından da olabilmektedir. Doğru, tam ve güvenilir muhasebe bilgileri elde edebilmek için sadece bilgi oluştuktan sonra değil, verinin bilgisayara girilmesi, işlenmesi ve bilgiye dönüşüm süreçlerinde de gerekli önlemler alınmalıdır. Muhasebe bilgi güvenliğini sağlamak için güvenlik hizmetleri sunan şirketler ile de çalışılabilir. İşletmenin güvenlik işini kendisinin yapmasının maliyeti yüksek ise güvenlik işini bu şirketlere devretmesinde yarar olacaktır.

KAYNAKÇA

Abu-Musa, Ahmad A., (Sep. 2003) **"The Perceived Threats to the Security of Computerized Accounting Information Systems"**, Journal of American Academy of Business, Cambridge, Holywood, Vol.3, Iss. ½.

Alagöz, Ali, (2007) "**Web Sitesi Maliyetlerinin Muhasebeleştirilmesi**", Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Sayı: 18, Konya, 2007, s. 11-24.

Canbek, Gürol ve Şeref, Sağıroğlu, (2006) **"Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme"**, Politeknik Dergisi, Cilt: 9, Sayı: 3, s. 165-174.

Civan, Mehmet ve Kara, Ekrem, (Ekim 2003) **"İşletme Yönetiminde Muhasebe Bilgi Sisteminin Yeri ve Önemi"**, Muhasebe ve Finansman Dergisi, Sayı:20, s. 111-117.

Charles P. Pfleeger, (1997) **"The Fundamentals Of İnformation Security"**, Software, IEEE.

Dalcı, İlhan ve Danış, V. Naci, (2004) **"Benefits of Computerized Accounting Information Systems on the JIT Production Systems"**, Review of Social, Economic & Business Studies, Vol.2.

Demir, Berna, (2005) **"Muhasebe Bilgi Sistemlerinde Bilgi Güvenliği"**, Muhasebe ve Finansman Dergisi, Sayı: 26, s. 147-156.

Dinç, Engin ve Varıcı, İdris, (2008) **"Muhasebe Bilgi Sisteminin Kurumsallaşma Düzeyine Etkisi: Sanayi İşletmeleri Üzerine Bir Araştırma"**, Afyon Kocatepe Üniversitesi İİBF Dergisi, Sayı 1, s. 67-85.

Doğantimur, Fulya, (2009) **"ISO 27001 Standardı Çerçevesinde Kurumsal Bilgi Güvenliği"**, Mesleki Yeterlilik Tezi, TC Maliye Bakanlığı Strateji Geliştirme Başkanlığı, Ankara.

Eminağaoğlu, Mete ve Gökşen, Yılmaz, (2009) **"Bilgi Güvenliğ Nedir, Ne Değildir, Türkiye'de Bilgi Güvenliği Sorunları ve Çözüm Önerileri",** Dokuz

Eylül Üniversitesi Sosyal Bilimler Enstitü Dergisi, Cilt: 11, Sayı: 4, s. 01-15.

Gökdeniz, Ümit, (2005) **"İşletmelerde Muhasebe Bilgi Sistemine Yaklaşım"**, Muhasebe ve Finansman Dergisi, Sayı: 27, s. 86-93.

Harold, F. Tipton ve Krause, Micki, (2007) **"Handbook of Information Security Management",** Auerbach Publicaions.

http://www.us-cert.gov/reading_room/infosecuritybasics.pdf, **"Introduction to Information Security",** 02.04.2011.

http://www.computerworld.com.tr/bilgi-guvenliginin-neresindeyiz-detay_2107.html, 19.03.2011.

http://www.pctime.com.tr/habergoster.asp?id=1950, 19.03.2011.

http://blog.microsoft.com.tr/turkiyede-bilgi-guvenligi.html, 23.06.2011.

INTOSAI, (October 1995) **"Information System Security Review Methodology"**, Issued by EDP Audit Committee International Organisation of Supreme Audit Institutions.

Julie, David, S. ve digerleri, (Spring 1999) **"The Research Pyramid:A Framework For Accounting Information System Research"**, Journal of Information System, Vol.13, No.1.

Karagül, A. Aziz, (2005) **"Bilgi Yönetimi, Kurumsal Kaynak Planlaması ve Muhasebe Bilgi Sistemi İlişkisi Çerçevesinde Muhasebe Eğitimi"**, XXIV. Türkiye Muhasebe Eğitimi Sempozyumu.

Marcinkowski, S.J., Stanton, J.M., (2003) **"Motivational Aspects Of İnformation Security Policies"**, Systems, Man and Cybernetics, IEEE International Conference on 3.

Onur, Altay, (01.05.2011) **"Kurumsal Bilgi Güvenliğine Bakış"** http://www.bilgiyonetimi.org/cm/.

Robert, Richardson, (2008) **"2008 CSI/FBI Computer Crime & Security Survey. CSI"**, http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf.

Robyy, S. Fussell, (2005) **"Protecting İnformation Security Availability Via Self-Adapting İntelligent Agents"**. Military Communications Conference, IEEE.

Romney, Marshall B., Steınbart, Paul John, Cushıng, Barry E., (1997) **Accountingi Information Systems**, Seventh Edition, Addison-Wesley Publishing Co.

Scott, Campbell., (2003) **"Supporting Digital Signatures İn Mobile Environments"**, Enabling Technologies: Infrastructure for Collaborative Enterprises. Proceedings. Twelfth IEEE International Workshops.

Sevim, Adnan, (2009) **"Dijital Muhasebe"**, Anadolu Üniversitesi Yayınları, Eskişehir.

Sürmeli, Fevzi, (Ağustos 2005) **"Muhasebe Bilgi Sistemi"**, Anadolu Üniversitesi Yayınları, Eskişehir.

Symantec, (2009) **"Global Internet Security Threat Report 2008"**, vol.XIV., Symantec Corporation.

Symantec, (2009) **"EMEA Internet Security Threat Report 2008"**, vol.XIV., Symantec Corporation.

Küçükoğlu Şule, (04.04.2011) **"Uygun Güvenlik Çözümüne Yolculuk"**, http://www.infosecurenet.com/macroscope/macroscope6.pdf.

Türk, Dilek, A. Filiz, Y. Şule, (2009) **"Muhasebe Departmanlarında Bilgi Yönetimi: Sakarya Örneği"**, Muhasebe Finansman Dergisi, Sayı: 44, s.236-250.

Ünal, Ü. Zaim, (2006) **"Bilgi Güvenliği Politikası ve Bilgi Güvenlik Yapısı"**, Bilişim ve Hukuk Dergisi, Sayı: 1, Ankara, s.13-15.

Vima, Salazar, (October 2006) **"Management of Information Security"**.

Yılmaz, Baki ve diğerleri, (2005) **"Bilgi Çağında Entelektüel Sermaye Anlayışının Muhasebe Bilgi Sistemi Açısından Değerlendirilmesi"**, Selçuk Üniversitesi Sosyal Bilimler MYO Dergisi, Cilt:8, Sayı:1-2, s. 90-105.

Yılmaz, Vural ve Şeref, Sağıroğlu, (2008) **"Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme"**, Gazi Üniv. Müh. Mim. Fak. Der. Cilt :23 No: 2, s.507-522.