Bilgi Güvenliği Yönetimi

Mehmet TEKEREK
KSÜ, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, Kahramanmaraş

Geliş Tarihi: 12.12.2006 **Kabul Tarihi: 22.05.2007**

ÖZET: Günümüzde verimliliğin artırılması, iş akışlarının hızlandırılması, çalışanlar ve diğer kurumlarla daha hızlı iletişim kurulabilmesi, günlük yaşantımızı kolaylaştırması gibi birçok sebepten dolayı bilişim sistemleri hızla yaygınlaşmaktadır. Bilişim teknolojilerindeki gelişmeler sonucunda, merkezi yapılar yerlerini, dağıtık mimarilere, internet ve ağlar üzerinden erişilebilen elektronik uygulamalara bırakmıştır. Web uygulamaları, uzaktan erişimler, çevrimiçi sistemler, bilgisayar ağları, internet gibi elektronik bilgi altyapılarının kullanımının artması sonucunda e-kavramlar (e-ticaret, e-öğrenme, e-rezervasyon, e-sınav, e-okul, e-banka, e-devlet vb.) günlük yaşantımızın bir parçası haline gelmiştir. Bilişim ortamlarının kullanımının artması ve yaygınlaşmasına paralel olarak güvenlik tehditleri ve riskleri aynı oranda artmıştır. Teknik güvenlik önlemlerinin gelişmesine rağmen bilişim sistemlerine karşı yapılan saldırıların sayısının artması ve bilgi sistemleri üzerinde yüksek derecede etki yapan hasarlar oluşturması, teknik yöntemlerin bilgi güvenliğinin sağlanmasında yetersiz olduğunu göstermektedir. Bilgi güvenliğinin sağlanabilmesi için teknik önlemlerin yanında, idari önlemler (kurallar, cezalar, yaptırımlar vb), standartlar (ISO 27001,Ortak Kriterler vb) ve insan faktörü göz önüne alındığında bilgi güvenliği karmaşık çözümler içeren ve yönetilmesi zorunlu hale gelen bir süreç halini almıştır. Bu çalışmada bilgi güvenliği yaşayan bir süreç olarak ele alınmış ve yönetilebilirlik gerekliliği ortaya konarak, bir bilgi güvenliği yönetim modeli geliştirilmiştir.
Anahtar Kelimeler: Bilgi güvenliği, bilgi güvenliği standartları, bilgi güvenlik politikaları.

Information Security Management

ABSTRACT: Currently information service has been become widespread rapidly, because of several causes, such as increase of efficiency, facilitating of our daily life and establishing of quicker communication with employees and the other institutions as well. As a result of improvements in information technology, central bodies have been replaced by scattered architectural designs, and electronic applications that are accessible through internet and network. Several concepts beginning with "e-" (e-commerce, e-education, e-reservation, e-exam, e-school, e-bank…) have been become a part of our life as a consequence of an increase in using of electronic information infrastructures, for instance internet, computer networks, online systems, remote access and so on. In parallel with expansion and augmentation in using of informational environments, relevant risks and threats have been increased in same proportion. Increase in numbers of the malicious and harmful attacks against information systems demonstrates that present technical methods are inadequate for securing information systems properly. To provide security on an information system not only technical measures but also administrative measures (rules, punishments, sanctions e.g.) and humanitarian factors should be considered; thus the issue of information system security has become a compulsory management process including more complex solutions. By this study information security is dealt with as a living organic process, and an information security model is developed by emphasizing on necessity of some managerial means and models.
Keywords: Information security, information security standards, security policies.

GİRİŞ

Bilgiye sürekli erişimin sağlanması, bilginin göndericiden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlük içerisinde güvenli bir şekilde iletimi *bilgi güvenliği* olarak tanımlanabilir (Pfleeger, 1997). Bilgi güvenliğinin sağlanabilmesi için, bilgi sistemleri gizlilik, bütünlük, erişilebilirlik gibi temel güvenlik bileşenlerinin gereklerini sağlamak zorundadır. Bu üç temel bileşene, kimlik tespiti, güvenirlik ve inkâr edememe alt bileşenleri de eklenebilir.

Günümüzde bilgi güvenliğini tehdit eden unsurların başında, internet yoluyla yayılan virüsler, solucanlar, truva atları, kötü niyetli kodlar, yerel saldırganlar (internal hacker), korunmasızlıktan kaynaklanan sömürüler, yapılandırma hataları gelmektedir. Bilgi güvenliği ihlalleri veri kaybı, finansal kayıplar, itibar kayıpları, hizmetlerin sunulamaması veya aksaması, gizli bilgilerin çalınması gibi istenemeyen durumlara neden olmaktadır.

Bilgi güvenliğinin sağlanmasında güvenlik politikaları ve standartlarının önemi büyüktür. Güvenlik politikaları üst yönetim tarafından desteklenen, kullanıcılar tarafından uygulanabilir ve anlaşılır olmalıdır. Kurum kültürüne uyan ve kurum genelinde kabul görmüş güvenlik politikaları olmaksızın bilgi güvenliğinin sağlanması ve yönetilmesi çok zordur.

Bilgi güvenliğinin sağlanabilmesi için teknik önlemlerin yanında, idari önlemler (kurallar, cezalar, yaptırımlar vb), standartlar (ISO 27001,Ortak Kriterler vb) ve insan faktörü göz önüne alınmalıdır.

Tüm bu süreçler ele alındığında bilgi güvenliği karmaşık çözümler içeren ve yönetilmesi zorunlu olan yaşayan bir süreç halini almıştır.

Bu çalışma bilgi güvenliğinin yaşayan bir süreç olarak ele alınmasını ve yönetilebilirlik ihtiyacını ortaya koymaktadır. Bilgi güvenliğinin sağlanmasına yönelik gereklilikler göz önüne alınarak bir bilgi güvenliği yönetim modeli geliştirilmiştir. Bu model geliştirilirken var olan kurumsal kültür farklılıkları en aza indirgenerek, standart temelli bir yaklaşım ortaya konmuştur. Böyle bir yaklaşımın benimsenmesinin nedeni, kurumların kültürel farklılıkları ne olursa olsun globalleşen dünyamızda her kurumun birbiriyle ortak çalışmaları ihtiyaç halini almış durumda olmasıdır. Standart bir bilgi yönetim modelinin bu farklılıkları ortak yönetim çatısında toplayabilmesi amaçlanmıştır.

Bilgi güvenliğinin sağlanabilmesi için uyulması gereken birçok bileşen vardır. Gizlilik, bütünlük ve erişilebilirlik temel olarak ele alınabilecek üç ana ilkedir(Bilişim, 2003). Bu üç temel ilkeye alt bileşenler olarak kayıt tutma, kimlik tespiti, güvenirlik ve inkâr edememe bileşenleri de sayılabilir.

BİLGİ GÜVENLİĞİ İLKELERİ

Gizlilik (Confidentiality): Gizli bilginin yetkisi ve izni olmayan kişilerin eline geçmesinin engellenmesidir(Fussell, 2005). 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.

Bütünlük (Integrity): Bilginin göndericiden çıktığı haliyle bir bütün olarak alıcısına ulaştırılmasıyla bütünlük ilkesi sağlanır(Fussell, 2005). 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.

Erişilebilirlik (Availability): Bilgiye zamanında erişim, bilgi sistemlerini kullanan kişiler tarafından büyük bir önem taşımaktadır. Bilgi sistemlerinden kendilerinden beklenen işleri belirlenen bir zamanda yapmaları istenir. Bu başarım sayesinde elektronik işe 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 faktörler de sistem sürekliliğini etkileyebilir(Fussell, 2005). Sisteme erişilebilirliğin sürekli sağlanması için fiziksel önlemler alınmalı, güvenlik duvarları, atak tespit sistemleri, antivirüs yazılımları kurulmalıdır.

Kayıt (Log) Tutma (Accountability): Elektronik ortamda gerçekleşen olayları, daha sonra analiz edilmek üzere kayıt altına almaktır(Marcinkowski- Stanton, 2003). Olay, bilgisayar sistemi ya da bilgisayar ağı üzerinde meydana gelen herhangi bir faaliyet olarak tanımlanabilir. Kullanıcının parolasını yazarak sisteme girmesi, web sayfasına bağlanması, e-posta iletişimi gibi örnekler verilebilir. Toplanan olay kayıtları üzerinde yapılacak analiz sonucunda, bilinen saldırı türlerinin izlerine rastlanırsa ve saldırı olasılığı yüksek bir aktivite tespit edilirse atak tespit sistemleri tarafından alarm mesajları üretilerek sistem yöneticileri uyarılır. Kayıt tutma saldırganların belirlenmesi içinde ayrıca bir önem arz etmektedir. Saldırı olduktan sonra kayıtlar yardımıyla iz sürülerek saldırganın kimliğinin tespit edilmesi sağlanır.

Kimlik Tespiti (Authentication): Bilgi sistemlerinden hizmet alan alıcının, iddia ettiği kişi olduğundan emin olunması (Marcinkowski- Stanton, 2003). Örneğin, izniniz olan herhangi bir ortama eriştiğinizde size sorulan şifreler, bilgisayarınızı açarken şifre girilmesi kullanıcının kimliğinin tespit edilmesinde kullanılan 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, token, biyometrik teknolojiler kimlik tespitinde kullanılan diğer teknolojilerdir.

Güvenirlik (Reliability): Bilgisayar sistemlerinden beklenen davranış ile elde edilen sonuçlar arasındaki tutarlılık durumudur (Marcinkowski- Stanton, 2003).

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).

BİLGİ AKTARIM VE PAYLAŞIMINDAKİ TEHDİTLER

Tehdit, "bir sistemin veya kurumun zarar görmesine neden olan istenmeyen bir olayın arkasındaki gizli neden" olarak tanımlanabilir(Bilişim, 2003). Her tehdidin bir kaynağı ve bu kaynağın yararlandığı sistemdeki bir "güvenlik boşluğu" vardır. *"Sistemi neye karşı korumalıyım?"* sorusuna verilecek cevap bir sisteme yönelik olan tehditlerin belirlenmesine yardımcı olacaktır. Tehditler, insan kaynaklı tehditler, fiziksel tehditler, yazılım kaynaklı tehditler, güvenlik boşlukları, eğitim ve bilinç eksikliğinden kaynaklanan tehditler olarak sınıflandırılabilir.

İnsan Kaynaklı Tehditler: İnsan kaynaklı tehditleri kendi içinde iki alt gruba ayırabiliriz:

Kötü niyet olmayan davranışlar sonucu oluşanlar: Bir kullanıcının, sistemi bilinçsiz ve bilgisizce, yeterli eğitime sahip olmadan kullanması sonucu sistemde ortaya çıkma olasılığı olan aksaklıklar.

Kötü niyetli davranışlar sonucu oluşanlar: Sisteme zarar verme amacıyla, sisteme yönelik olarak saldırganlar tarafından yapılacak tüm kötü niyetli davranışlardan kaynaklanan tehditlerdir. Bu tür tehditlerde saldırganlar tehdit kaynağı ve sistemde bulunan güvenlik boşluklarından yararlanırlar(Shephard, 2002).

Fiziksel Tehditler: Bu tür tehditler genellikle önceden tespit edilemezler, doğa olayları olmaları yüzünden genellikle engellenemez. Deprem, yangın, su baskını, sel, ani sıcaklık değişimleri, toprak kayması, çığ düşmesi bu tür tehditlere örnek olarak verilebilir. Tehdidin geliş yönüne göre de sınıflandırma yapılabilir. Buna göre *iç tehditler*, kurum içinden kuruma yönelik yapılabilecek saldırılar, *dış tehditler* ise kurum dışından kuruma yönelik olarak yapılabilecek saldırılar olarak tanımlanır. Son yıllarda yapılan araştırmalara göre güvenlik ihlallerinin % 67'si iç tehditler sonucunda ortaya çıkmaktadır(Shephard, 2002). İç tehditlerin ortaya çıkmasında kullanıcılar arasındaki yetki farklılıkları büyük rol oynamaktadır. Zorunlu olmadıkça sistemde ayrıcalıklardan kesinlikle kaçınılmalıdır.

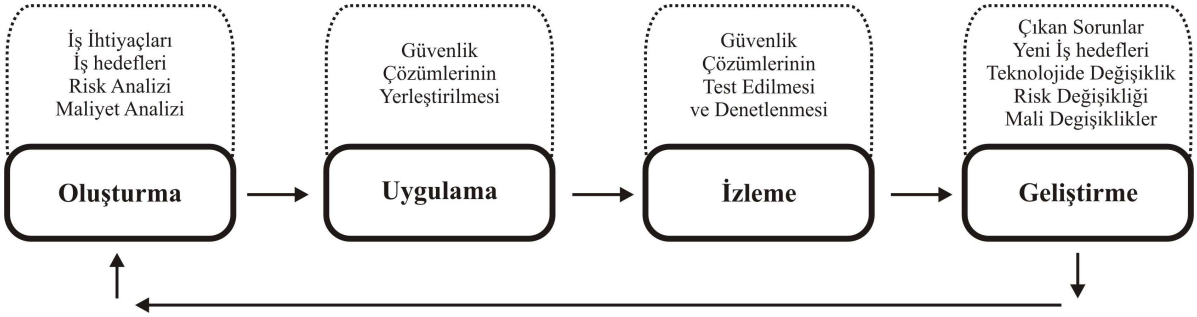
Yazılım Tehditleri: Donanımlar yazılımlar (işletim sistemi, programlar, uygulamalar) olmadan çalışamazlar. Bu yazılımların bilgisayarlarda çalışmasıyla birlikte çeşitli tehditler ortaya çıkmaktadır. Yazılımlar kötü amaçlı olarak tahrip edilebilir, değiştirilebilir, silinebilir veya kaza ile değişikliğe maruz kalabilir. Yazılımlardaki değişiklikler kolayca fark edilmezler. Örneğin, bir programı daha önceden yaptığı her şeyi yapacak ve bunun yanından saldırganın istediği ekstra işlemleri de yapacak şekilde değiştirmek mümkündür(Shephard, 2002). Bu durumda yazılımın değiştiğini fark etmek zor olabilir. Yazılımlarla birlikte gelen tehditlere örnek verilebilecek *Truva atı* (trojan horse) programı, görünürde bir işi yaparken gizlice başka işler yapılmasını sağlayan programlardır. *Virüs*, *Worm*, kötü amaçlı yazılmış programlardır. Bilgisayarlar arasında çok çabuk yayılarak etkilerini geniş alanda hissettirirler. *Arkakapı (BackDoor)*, kullanıcısından habersiz gizli giriş noktaları bulunan programlardır. Bilgiye istenmeyen kişi veya programların erişmesini sağlarlar.

Korunmasızlık (Vulnerability): Yazılım veya donanımdan kaynaklanan zafiyetleri güvenlik boşluğu olarak tanımlayabiliriz. Bir güvenlik boşluğu sayesinde saldırgan, sistemdeki bilgisayarlara veya bilgisayar ağı üzerindeki kaynaklara yetkisiz olarak erişebilir(Shephard, 2002).

Eğitim ve Bilinç: Bir kurumun bilişim güvenliği açısından karşı karşıya bulunduğu riskleri azaltmada kullanılması gereken ana yöntemlerden biri eğitimdir. Bilgi sistemlerini kullanan kullanıcıların, bilgi güvenliği konusunda eğitimlerle bilinçlendirilmesi, onların bir güvenlik boşluğu olmasını ve kurum açısından risk oluşturacak bir etken olmaları olasılığını en aza indirecektir(Moffett, 1990).

Güvenlik Politikaları

Bilgi güvenliği politikası, organizasyonlarda uygulanacak olan bilgi güvenliğinin sağlanması için gerekli olan önlemlerin alınmasını sağlayan kurumsal etkinliklerdir(Karaarslan, 2003). Güvenlik politikaları kurumun üst düzey yönetimi tarafından desteklenmeli ve çalışanlar tarafından benimsenmelidir. Güvenlik politikası uygulanabilir, kullanıcı tarafından anlaşılır, yapılabilir ve güvenlik yöneticileri tarafından kolay yönetilebilir olmalıdır. Bilgi güvenliği politikaları her organizasyon için farklılık gösterse de, tipik olarak çalışanın sorumluluklarını, kontrol mekanizmalarını, amaç ve hedefleri içeren genel ifadelerden oluşur. Politikalar organizasyona özgü özel kanunlar olarak da düşünülmekle birlikte, her organizasyon içinde genel olarak Şekil 1.'de ifade edilen süreç işlemektedir.



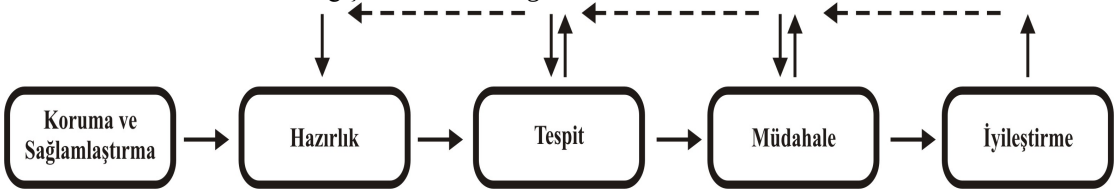
Şekil 1. Güvenlik Politikası Döngüsü

Yöneticiler arasında yapılan bir araştırmaya göre, kurumlarında güvenlik teknolojisinin kullanılmakta olduğunu bildirenlerin oranı %70 olarak tespit edilmesine rağmen, yalnızca %38'nin yazılı bir güvenlik politikasına sahip oldukları belirlenmiştir (Bilişim, 2003).

GÜVENLİK YAŞAM DÖNGÜSÜ

Bilgi güvenliği kavramlarının etkinliğini yitirmemesi konuyu devamlılığı olan yaşayan bir süreç olarak ele almakla mümkün olacaktır. Tehditlerin sürekli olarak yenilenmesi ve çeşitlilik kazanması, kullanılan altyapıların sık aralıklarla güncellenerek, iyileştirilerek değişikliklere uğraması ve yazılım sistemlerindeki sürekli değişimler, herhangi bir zamanda güvenli kabul edilebilecek bir sistemin belirli bir süre sonra da güvenli kalacağını garanti edemez (Donaldson, 1996). Bu nedenle, güvenlik çalışmaları tüm dünyada kabul gören "yaşam döngüsü" ile modellenmektedir. Bilgi güvenliği yönetiminde kabul görmüş yaklaşımlardan biri olan CERT (Computer Emergency Response Team) tarafından önerilen güvenlik yaşam döngüsü, Şekil 2'de gösterilen, aşağıdaki adımları içermektedir (Pfleeger, 1997).

Sağlamlaştırma (Hardening)
Hazırlık (Preparing)
Saldırı Tespiti (Detection)
Müdahale (Respond)
İyileştirme (Improving)



Şekil 2. CERT Güvenlik Yaşam Döngüsü

Sağlamlaştırma aşamasında, bilgisayar ağının ve tüm bilgi sistemlerinin güvenliğini artırmaya yönelik faaliyetler gerçekleştirilir ve bilinen tehditlere karşı önlemler alınır (Ruiu, 2006).

Hazırlık aşamasında, bilinmeyen tehditlerin tespit edilip müdahale edilebilmesi için gerekli hazırlıklar gerçekleştirilir, ağın ve tüm sistemlerin karakteristik özellikleri belirlenir.

Tespit aşamasında, ağ ve sistemler üzerindeki yetkisiz ya da şüpheli olaylar hazırlık aşamasından yararlanılarak tespit edilir ve şüpheli durumlar değerlendirilir.

Müdahale aşamasında, bir önceki aşamada tespit edilen şüpheli durumlar detaylı olarak incelenir ve çözümlenir.

İyileştirme aşamasında ise, önceki aşamalarda karşılaşılan sorunlar ve tecrübeler ışığında Güvenlik Politikası gözden geçirilir ve geliştirilir.

Bu adımların tekrarlı bir biçimde gerçekleştirilmesi sayesinde, sürekli olarak potansiyel sorunlar tespit edilebilir ve zamanında önlem alınarak sistem güvenliği azami seviyede korunmaya çalışılır (Bishop, 2000).

Güvenlik Denetimleri: Güvenlik denetimi, bir kurumun güvenlik altyapısının, güvenlik politikasının, yönergelerinin ve personelinin ayrıntılı bir biçimde ele alınması, zayıf yönlerin tespiti ve bu zayıflıkların giderilmesi için öneriler sunulmasıdır (Okamoto-Tanaka, 1989). Bir denetim sırasında sorgulanabilecek konulara aşağıdaki örnekler verilebilir

Hangi veriler "yalnızca okunur", hangileri "yazılabilir"?

Önemli verileri kim(ler)/ ne(ler) değiştirebilir?

Sistem erişimini ve kaynak kullanımını ne(ler) engelleyebilir?

Sistem üzerindeki değişiklikler nasıl yapılmaktadır?

Sisteme erişim yolları nelerdir?

Fiziksel güvenlikler yeterli midir?

Sistemdeki değişiklikler kayıt (Log) altına alınıyor mu?

Sistemde aksaklık çıktığında, bunun nedenleri ortaya çıkarılabiliyor mu?

BİLGİ GÜVENLİĞİ YÖNETİM STANDARTLARI

Bilgi güvenliğinin sağlanması, teknik bir problem olmanın yanı sıra, yönetimsel bir problemdir. Bilgi güvenliği yönetimini sağlayabilmek için dünyada çeşitli

standartlar kullanılmaktadır. Bu standartlar, 1993 yılında BS 7799 olarak duyurulan İngiliz standardı, 1999 yılında uluslararası bir standart olarak kayda geçen Ortak Kriterler (Common Criteria), 2000 yılında ise BS 7799 standartlarının ilk bölümü esas alınarak yayınlanan ve 2005 yılında revize edilen ISO/IEC 17799:2005 ve ISO 27001 standartlarıdır (Guan vd., 2003)- (Duan- Wu, 1999).

Tüm dünyada ISMS (Information Security Management System) olarak adlandırılan ve daha birçok bilgi teknoloji standartlarıyla desteklenen bu yeni yönetim sistemi standartlarında, bilişim teknolojilerinin güvenliği ile ilgili kriterler ile bu sistemlerin yeterliliği ve denetimlerini ilgilendiren konu başlıkları altında ele alınarak sorgulama ve detay kontrolleri yapılmaktadır (Duan- Wu, 1999).

Bilgi güvenliği yönetim sistemlerinin uygulanmasından sorumlu olan bilgi güvenlik yöneticilerinin karşılaştıkları en büyük problem, bilgi güvenliğinin sağlanması amacıyla alınan önlemlerin kesin hatlarıyla uygulamaya dökülememesidir. Bunun en önde gelen nedenlerinden biri bilgi güvenlik sistemlerinin kurumsal kültürle çelişmesidir. Bu çelişkinin en önde gelen nedeni insan faktörüdür. Öyle ki; insanoğlu doğası gereği engellemelere karşı her zaman direnç göstermiştir. Bu direncin aşılabilmesi için güvenlik ile kullanışlılık arasındaki hassas dengenin kurulabilmesi gereklidir.

Kurumsal kültür çelişkisinin ikinci faktörü ortak çalışma yapan kurumlar arasında görülmektedir. Bu çelişkinin giderilebilmesi kurumlar arası güvenlik kültür farklılığının ortadan kaldırılması ile oluşabilir. Bunu oluşturmak için kurumlar arası güvenlik kültür farklarını en aza indirgeyecek etkin bilgi güvenliği yönetim modeline ihtiyaç duyulmaktadır. Bu çalışmada bu ihtiyaçtan yola çıkılarak örnek kurumlar arası Bilgi Güvenlik Modeli oluşturulmuştur.

BİLGİ GÜVENLİĞİ YÖNETİM MODELİ

Öncelikle bilgi güvenlik yönetimi gerçekleştirilebilmesi için kurumsal bilgi varlıklarının envanteri çıkarılır. Bunlar önem derecelerine göre sınıflandırılarak varlık yönetimi yapılır.

Bilgi varlılarının güvenliğini tehdit eden unsurlar belirlenip sınıflandırılarak kurumsal tehlike matrisi oluşturulur.

Tehlike değeri x gerçekleşme olasılığı= tehlike matrisidir.

Tehlike matrisi baz alınarak riskler tespit edilerek risk değerlendirmesi ve analizlerinin yapılmasıdır. Risk analizi sonucunda elde edilen değerler riskler karşısında alınması gereken önlemleri belirler. Bu önlemler şu şekildedir.

1) Risk kabul edilir: Bu durumda yapılacak herhangi bir şey yoktur.

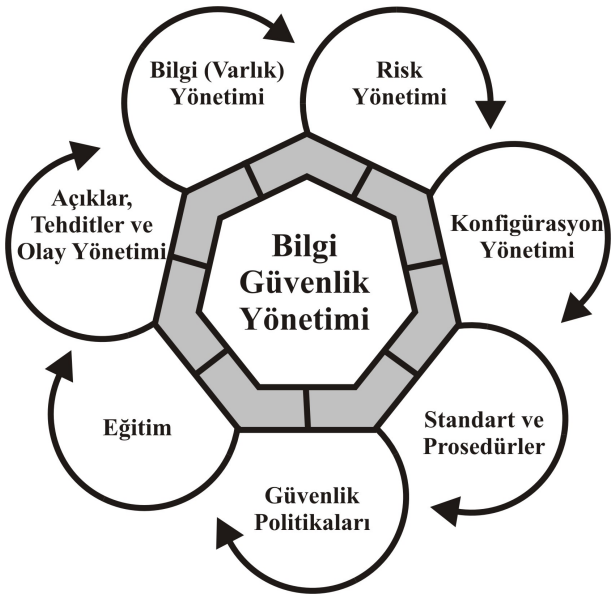
2) Riskin en aza indirgenmesi: Gereken yatırımlar maliyet etken bir yapıda yapılmalıdır.

3) Risk transferi: Risk maliyet etken yapıda bir yapıda uzman bir güvence kuruluşuna aktarılır.

Risk analizi sonucunda ortaya çıkan risk haritası esas alınarak güvenlik politikaları hazırlanır.

Bilgi güvenliği yönetim standartlarıyla, kurumsal bilgi güvenliği yönetim sisteminin çatısı oluşturulur.

Tüm bu yukarıda sayılan modüllerin en zayıf halkasını oluşturan insan faktörünün negatif etkisini en aza indirgemek için güvenlik farkındalık eğitimlerinin ayırım gözetilmeksizin tüm kurum çalışanlarına verilmesi gereklidir.



Şekil 3. Bilgi güvenliği yönetimi modeli.

Bu çalışma kapsamında ortaya konulan bilgi güvenliği yönetim sistemi bu modüller arasındaki bilgi geçişlerinin etkin bir şekilde yapılmasını sağlamaktır.

SONUÇ

Bu araştırma sonucunda bilgi güvenliğinin yönetilmesi için çok geniş bilgi ve teknoloji birikimi gerektiği, ancak teknolojinin tek başına bilgi güvenliğinin yönetimi için yeterli olmadığı ortaya konmaya çalışılmıştır. Bunun yanında iyi tasarlanmış güvenlik politikaları, hatasız yapılandırılmış bilgi güvenlik sistemleri, güvenlik açıklarının ve tehditlerinin etkili yönetimi, standardize edilmiş etkili süreçler, risk ve maliyet analizi, bilginin etkin bir şekilde yönetimi, bilgili ve iyi eğitimli bilgi güvenliği yöneticilerinin olması gerektiğine dair kazanımlar elde edilmiştir. Tüm bu araştırmalar ve parametreler göz önüne alınarak Şekil 3 ile ifade edilen bilgi güvenlik yönetim modeli oluşturulmuştur. Ortaya konan bilgi güvenlik yönetim modeli kurumsal seviyede kullanım alanı olan yapı baz alınarak geliştirilmeye çalışılmıştır.

KAYNAKLAR

Anonim. 2003. Bilişim Güvenliği Kitapçığı. ProG Bilişim Güvenliği ve Araştırma Ltd, 7s. http://www.pro-g.com.tr/whitepapers/bilisim-guvenligi-v1.pdf (01.07.2008).

Bishop, M. 2000. Education in information security. Concurrency, IEEE , 8: 4- 5

Campbell, S. 2003. Supporting digital signatures in mobile environments. Enabling Technologies: Infrastructure for Collaborative Enterprises. Proceedings. Twelfth IEEE International Workshops, 238s.

Donaldson, M.G. 1996. Evaluation of IT security products, devices and systems. Information Security - Is It Safe?., IEE Colloquium, 3s.

Duan, H., Wu, J. 1999. Security management for large computer networks. Communications, APCC/OECC '99. Fifth Asia-Pacific Conference on. and Fourth Optoelectronics and Communications Conference, Volume 2, 1210s.

Fussell, R.S. 2005. Protecting information security availability via self-adapting intelligent agents. Military Communications Conference, IEEE, 2977s.

Guan, B., Lo, C., Wang, P., Hwang, J. 2003. Evaluation of information security related risks of an organization: the application of the multicriteria decision-making method. Security Technology, Proceedings. IEEE 37th Annual International Carnahan Conference on, 170s.

Karaarslan E., Teke A., Şengonca H. 2003. Bilgisayar Ağlarında Güvenlik Politikalarının Uygulanması. Akademik Bilişim, Çukurova Üniversitesi, 1s.

Marcinkowski, S.J., Stanton, J.M. 2003. Motivational aspects of information security policies. Systems, Man and Cybernetics, IEEE International Conference on, 3: 2528s.

Moffett, J. 1990. Network security management. Security and Networks, IEE Colloquium on , 4- 6

Okamoto, E., Tanaka, K., 1989, Identity-based information security management system for personal computer Networks. Selected Areas in Communications, IEEE Journal on, 7: 2, 292s.

Pfleeger, C.P. 1997. The fundamentals of information security. Software, IEEE ,14 (1,14)

Ruiu, D. 2006. Learning from information security history, Security & Privacy Magazine, IEEE, 4:1, 78s.

Shephard, B. 2002. Information security-who cares?. Power System Management and Control, Fifth International Conference on (Conf. Publ. No. 488), 126s.