



T.C. MALİYE BAKANLIđI
Strateji Geliřtirme Bařkanlıđı

ISO 27001 STANDARDI EREVESİNDE
KURUMSAL BİLGİ GÜVENLİđİ

MESLEKİ YETERLİK TEZİ

Hazırlayan

Fulya DOđANTİMUR
Maliye Uzman Yardımcısı

Danıřman

İsmail ERASLAN
Daire Bařkanı

Ankara-2009

ÖNSÖZ

Günümüzde ticari şirketler ve kamu idareleri faaliyetlerini sürdürebilmek için yoğun bir şekilde bilgi kullanımına yönelmişlerdir. Bilginin önemi giderek artmış ve bilgi kurumun sahip olduğu varlıklar arasında çok önemli bir yere sahip hale gelmiştir. Bu nedenle de günümüzde bilginin güvenliği önemli bir konu olarak ortaya çıkmıştır.

Bu çalışmada bilgi güvenliği kavramından, kurumsal bilgi güvenliğinden ve ISO 27001 standardı ile öngörmüş olduğu Bilgi Güvenliği Yönetim Sistemi yapısına yer verilmiştir.

Çalışmanın hazırlanmasında tecrübesi ve bilgi birikimiyle bana yol gösteren, yorumlarını ve yardımlarını esirgemeyen tez danışmanım Sayın İsmail ERASLAN'a teşekkürü bir borç bilirim.

Fulya DOĞANTİMUR

Ankara-2009

ÖZET

ISO 27001 STANDARDI ÇERÇEVESİNDE KURUMSAL BİLGİ GÜVENLİĞİ

DOĞANTİMUR, Fulya

Maliye Uzman Yardımcısı

Mesleki Yeterlik Tezi

Nisan 2009, 48 sayfa

Kurumların, bilgi sistemleri süreçlerini inceleyerek tehditleri ve riskleri belirlemesi ve bu riskleri kabul edilebilir bir seviyeye indirebilmesi için alınacak karşı önlemlerin tespit edilmesi gerekmektedir. Bu çalışmada, bu yöntemlerin TS ISO/IEC 27001 Kurumsal Bilgi Güvenliği Standardı çerçevesinde bir kuruma nasıl uygulanabileceği konusunda birtakım ipuçları verilmeye çalışılmıştır.

Anahtar Kelimeler: Bilgi güvenliği, kurumsal bilgi güvenliği, bilgi güvenliği standartları, bilgi güvenliği yönetim sistemleri

ABSTRACT

ENTERPRISE INFORMATION SECURITY SYSTEMS WITHIN THE FRAMEWORK OF ISO 27001 STANDARD

DOĞANTİMUR, Fulya

Assistant Finance Expert

Proficiency Thesis

April 2009, 48 pages

Organizations have to examine their information system processes to find out threats and risks and then countermeasures against these risks must be determined to be able to reduce the risks to an acceptable level. In this article, it is aimed to provide some clues on how these methods could be applied to organizations within the framework of TS ISO/IEC 27001 Information Security Management Systems standard.

Key Words: Information security, enterprise information security, IT security, information security standards, information security management systems.

İÇİNDEKİLER

ÖNSÖZ.....	2
ÖZET.....	3
İÇİNDEKİLER.....	5
GİRİŞ.....	6
1 BİLGİ GÜVENLİĞİ VE KURUMSAL BİLGİ GÜVENLİĞİ.....	6
1.1 BİLGİ GÜVENLİĞİ KAVRAMI.....	7
1.2 BİLGİ GÜVENLİĞİNİN ÖNEMİ.....	7
1.3 KURUMSAL BİLGİ GÜVENLİĞİ.....	8
1.3.1 Kurumsal Bilgi Güvenliği İhtiyacı.....	9
1.3.2 Gerektiği Kadar Koruma İlkesi.....	10
2 ISO 27001 STANDARDI VE BİLGİ GÜVENLİĞİ YÖNETİM	
SİSTEMİ.....	11
2.1 BİLGİ GÜVENLİĞİ ÖNLEMLERİ	15
2.1.1 Kurumsal Bilgi Güvenliği Önlem Türleri.....	22
2.1.1.1 Yönetsel Önlemler	23
2.1.1.2 Teknolojik Önlemler	32
2.1.1.3 Eğitim.....	39
3 KURUMSAL BİLGİ GÜVENLİĞİ DEĞERLENDİRMESİ	42
3.1 2008 KÜRESEL Bilgi Güvenliği ANKETİ	45
4 SONUÇ.....	47
KAYNAKÇA	48

GİRİŞ

Bilgi tüm kuruluşların can damarıdır ve birçok şekilde karşımıza çıkabilmektedir. Yazıcıdan yazdırılabilir veya kağıda yazılabilir, elektronik ortamda saklanabilir, posta veya elektronik yolla iletilir, toplantı odanızdaki tahtada yazabilir, masanızdaki post-it de yazabilir, filmlerde gösterilebilir, ya da sohbet esnasında konuşulabilir. Günümüzün rekabete dayanan iş ortamında, bu tür bilgiler devamlı olarak birçok kaynağın tehdidi altındadır. Bu tehditler dahili, harici, rastlantısal veya kötü niyet şeklinde olabilir. Bilginin saklanması, iletilmesi ve alınması için yeni teknolojinin artan bir şekilde kullanılmasıyla, kendimizi artan sayıdaki tehditlere ve tehdit tiplerine tamamen açmış oluyoruz.¹

Farklılık ve rekabet avantajı sağlayan varlıklar, organizasyonlar için çok değerlidir. Birçok varlığın kaybedilmesi durumunda telafisi mümkün iken kurumların yaşam deneyimlerini de yansıtan "bilgi" para karşılığı kolaylıkla yerine konamamaktadır. Bilgiyi korumak, bilginin güvenliğini sağlamak artık bir zorunluluktur. Çünkü bilgi güvenliği, iş sürekliliğini yani aksamaların ve durmaların yaşanmamasını sağlamaktadır.

1 BİLGİ GÜVENLİĞİ VE KURUMSAL BİLGİ GÜVENLİĞİ

Bilgi, günümüzde üretim faktörü olarak değerlendirilebilmektedir. Kurumlar için vazgeçilemez, önemli bir değerdir.

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.²

Dolayısıyla, bilgi güvenliğini sadece bilgi sistemlerinin güvenliği olarak değerlendirmemek gerekmektedir. Zira bilgi sadece sistemlerde bulunmamakta çeşitli ortamlarda yer almaktadır. Bu nedenle bilgi güvenliğinin sağlanmasından

¹ <http://www.bsi-turkey.com/BilgiGuvenciligi/Genel-bakis/index.xalter>

² e-Dönüşüm Türkiye Projesi Birlikte Çalışabilirlik Esasları Rehberi Sürüm 2.0, DPT Bilgi Toplumu Dairesi, 2008

bahsederken sözü geçen bilgi kavramı sadece bilgi sistemlerinde yer alan bilgiyi ifade etmemektedir. Yani bilgi güvenliği bilgi teknolojileri ile sınırlı tutulmamalıdır.

Kurumlar için bu kadar öneme sahip ve her ortamda bulunan bir varlığın korunması, güvenliğinin sağlanması gerekmektedir.

1.1 BİLGİ GÜVENLİĞİ KAVRAMI

Bilgi güvenliği, bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanmasını anlamına gelmektedir. Gizlilik, bütünlük ve erişilebilirlik bilgi güvenliğinin temel unsurları olarak değerlendirilebilir.

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 düşünülemez. Bilginin gizliliğinin sağlanması o bilginin erişilebilirliğini engellememelidir. Aynı zamanda erişilebilen bilginin bütünlüğünün de sağlanması önemlidir. Eğer bir bilgi için sadece gizlilik sağlanıyor 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.

Bu unsurlara ek olarak bilgi güvenliği açıklanabilirlik, inkar edememe ve güvenilirlik gibi özellikleri de kapsar.

1.2 BİLGİ GÜVENLİĞİNİN ÖNEMİ

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.

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.

Söz konusu Türk katılımcılar, bilgi güvenliğinin kağıt üzerinde bir zorunluluktan ibaret olmadığını düşündüğü görülmüştür. Türkiye'deki Bilgi Güvenliği Yönetimi Sistemi'ni, ISO 27001 gibi sertifikasyon amacı gütmeyen kurduğunu belirtenlerin oranı, ankete katılanların yarısını oluşturuyor.

1.3 KURUMSAL BİLGİ GÜVENLİĞİ

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 bilgi güvenliği olarak tanımlanmaktaydı. Kurumsal bilgi güvenliği ise, kurumların bilgi varlıklarının tespit edilerek zaafiyetlerinin belirlenmesi ve istenmeyen tehdit ve tehlikelerden korunması amacıyla gerekli güvenlik analizlerinin yapılarak önlemlerinin alınması olarak düşünülebilir.³

Öncelikle bu tanımda geçen bilgi varlıkları sözcüğünün içerdiği anlam önem arz etmektedir. 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

3 Y.Vural, Ş. Sağıroğlu, Kurumsal bilgi güvenliği ve standartları üzerine bir inceleme, Gazi Üniv. Müh. Mim. Fak. Der. Cilt :23 No: 2, 2008.

masasının üzerinde bulunan bir kağıtta olabilir, bilgisayarında kayıtlı bir dosyada olabilir.

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

Yani, bilgi güvenliği sadece bir Bilgi Teknolojisi (BT) ya da yaygın söylemle Bilgi Sistemleri işi değildir; kurumun her bir çalışanın 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 yaratılmamışsa, 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.⁴

1.3.1 Kurumsal Bilgi Güvenliği İhtiyacı

Kurumsal bilgi güvenliğinin sağlanmasının önemli gerekçeleri ana hatlarıyla aşağıda belirtilmektedir. Bunlar;

-Güvenlikle ilgili tehdit ve risklerin belirlenerek etkin bir risk yönetiminin sağlanması ve kurumsal itibarın korunması.

-İş sürekliliğinin sağlanması.

-Bilgi kaynaklarına erişimin denetlenmesi.

-Personelin, yüklenicilerin ve alt yüklenicilerin güvenlik konusunda bilinç düzeyinin yükseltilmesi ve önemli güvenlik konularında bilgilendirilmesi.

-Bilgi varlıklarının gizliliğinin, bütünlüğünün ve doğruluğunun sağlanması.

4 Ş.Küçüköğlü, Uygun Güvenlik Çözümüne Yolculuk, <http://www.infosecurenet.com/macroscope/macroscope6.pdf>.

-Kurumsal bilgi varlıklarının kötü amaçlı olarak kullanma ve/veya suistimal edilmesinin engellenmesi,

-Bilgilerin güvenli bir şekilde üçüncü taraflara ve denetçilere açık olmasının sağlanması.

-Bilgi sistemlerini kullanan kişilerin, umursamazlığından, planlanmış taciz, bilinçsiz kullanım veya bilmeden yanlışlıkla suistimal etme gibi nedenlerden dolayı oluşabilecek donanım, yazılım ya da bilgisayar ağlarında meydana gelebilecek arızalara karşı korunması.⁵

Kişi ve kurumların bilgi güvenliğini sağlamadaki eksikliklerinin yanında saldırganların saldırı yapabilmeleri için ihtiyaç duydukları yazılımlara internet üzerinden kolaylıkla erişebilmeleri fazla bilgi birikimine ihtiyaç duyulmaması ve en önemlisi ise kişisel ve kurumsal bilgi varlıklarına yapılan saldırılardaki artışlar, gerek kişisel gerekse kurumsal bilgi güvenliğine daha fazla önem verilmesine yeni yaklaşımların ve standartların kurumlar bünyesinde uygulanması zorunluluğunu ortaya çıkarmıştır.⁶

1.3.2 Gerektiği Kadar Koruma İlkesi

Kurumsal bilgi güvenliğinin sağlanabilmesi için kurumun öncelikle bilgi varlıklarını tespit etmesi yani varlık envanterini çıkarması gerekmektedir. Çünkü ancak bu sayede kurum neye sahip olduğunu görecektir ve bu sahip olduğu varlıkların önemini ve karşı karşıya olduğu riskleri ve bu varlığın yok olması durumunda faaliyetlerinin ne kadar aksayacağını ya da faaliyetini yürütüp yürütemeyeceğini ortaya koyabilecektir. Daha sonra ise, neyi neye karşı ve ne ölçüde koruyacağını belirlemesi gerekmektedir. İşte bu noktada kurumun bilgi varlığı ile bu varlığı korumak için ne kadar maliyete katlanması gerektiği sorunu ortaya çıkmaktadır.

⁵ Y.Vural, Ş.Sağiroğlu, Kurumsal bilgi güvenliği: güncel gelişmeler, Bildiriler Kitabı uluslararası katılımlı bilgi güvenliği ve kriptoloji konferansı, 2007.

⁶ Y.Vural, Ş.Sağiroğlu, Kurumsal bilgi güvenliği ve standartları üzerine bir inceleme, a.g.e, s:508.

Kurum için deęeri olan varlıklar, sadece deęerleri geęerli olduęu srece korunmalı ve koruma iin harcanacak para, emek ve zaman varlıęın deęerinden fazla olmamalıdır.

Bu ilkedeki ama, korumanın anlamsız olduęu Őeyleri korumamaktır. İlkenin bir dięer amacı da, korunacak varlık hasar grdğnde, yenilemek iin yapılacak harcamadan daha fazlasını o varlıęı korumak iin harcamamaktır. Yani olasılıkla evlerde kullanılan nemli bilgilerin saklanmadıęı kiŐisel bilgisayara yz binlerce liralık bir firewall kurmak gereksizdir.

Dolayısıyla, kurum tarafından bilgi gvenlięine yapılacak yatırım korunacak varlıklardan daha maliyetli olmamalıdır. Korunması iin harcanan emek ve maliyet korunacak varlıęa deęmelidir.

2 ISO 27001 STANDARDI VE BİLGİ GVENLİęİ YNETİM SİSTEMİ

İletiŐim ortamlarının yaygınlaŐması ve kullanımının artması sonucunda bilgi gvenlięinin saęlanması ihtiyaı her geen gn katlanarak artmıŐtır.

Sadece teknik nlemlerle (gvenlik duvarları, saldırı tespit sistemleri, antivirs yazılımları, Őifreleme, vb.) kurumsal bilgi gvenlięinin saęlanmasının mmkn olmadıęı grlmŐtır. Bu nedenle teknik nlemlerin tesinde, insanları, sreleri ve bilgi sistemlerini iine alan ve st ynetim tarafından desteklenen bir ynetim sisteminin gereklilięi ortaya ıkmıŐtır.

Kurum veya kuruluŐların st dzeyde bilgi gvenlięini ve iŐ sreklilięini saęlamaları iin, teknik nlemlerin yanında teknik olmayan (insan faktr, prosedrel faktrler, vb.) nlemlerin ve denetimlerin alınması, tm bu srelerin devamlılıęının saęlanması ve bilgi gvenlięi standartlarına uygun olarak ynetilebilmesi amacıyla ynetim tarafından desteklenen insanları, iŐ srelerini ve biliŐim teknolojilerini kapsayan bilgi gvenlięi standartlarına uygun olarak Bilgi Gvenlięi Ynetim Sistemi (BGYS) kurmaları gerekmektedir. Bilgi gvenlięi standartları kurumların kendi iŐ srelerini bilgi gvenlięine ynelik risklerden korumaları ve nleyici tedbirleri sistematik biimde iŐletebilmeleri ve standartların

gereğini yerine getiren kurum veya kuruluşların belgelendirilmesi amacıyla geliştirilmiştir.⁷

Bilgi varlıklarının korunabilmesi, kurumların karşılaşılabileceği risklerin en aza indirgenmesi ve iş sürekliliğinin sağlanması BGYS'nin kurumlarda üst yönetim desteğiyle hayata geçirilmesiyle mümkün olmaktadır. BGYS, ISO 27001 standardının öngördüğü bir yapıdır.

Standardın tanımına göre BGYS, “Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası” olarak tanımlanmaktadır. Kurumsal yapıyı, politikaları, planlama faaliyetlerini, sorumlulukları, uygulamaları, prosedürleri, prosesleri ve kaynakları içermektedir.

ISO 27001 Bilgi Teknolojisi-Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri-Gereksinimler standardı kurumsal bilgi güvenliğinin sağlanmasına yönelik bir standarttır. Kurumsal bilgi güvenliğinin bir kurumda nasıl uygulanabileceğini açıklayan bir dokümandır. Ayrıca, çeşitli büyüklüklerdeki kurumlara uygulanabilir bir biçimde hazırlanmıştır. Sadece sistem güvenliğinden değil bilgi güvenliğinden bahsetmektedir.

Bu standart, bir BGYS kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için bir model sağlamak üzere hazırlanmıştır. Bir kuruluş için BGYS'nin benimsenmesi stratejik bir karar olmalıdır. Bir kuruluşun BGYS tasarımı ve gerçekleştirmesi, ihtiyaçları ve amaçları, güvenlik gereksinimleri, kullanılan prosesler ve kuruluşun büyüklüğü ve yapısından etkilenir. Bunların ve destekleyici sistemlerinin zaman içinde değişmesi beklenir. Bir BGYS gerçekleştirmesinin kuruluşun ihtiyaçlarına göre ölçeklenmesi beklenir(örneğin, basit durumlar basit BGYS çözümleri gerektirir).⁸

⁷ Y.Vural, Ş.Sağiroğlu, Kurumsal bilgi güvenliği: güncel gelişmeler, a.g.e., s:196.

⁸ TS ISO/IEC 27001,Mart 2006.

Proses yaklaşımını benimsemiş bir standarttır. Girdilerden çıktı elde edimine kadar süren her faaliyet proses olarak kabul edilir.

Standard, sunulan bilgi güvenliği proses yaklaşımının, kullanıcılarını aşağıdakilerin öneminin vurgulanmasına özendirdiği belirtmiştir:

- a) İş bilgi güvenliği gereksinimlerini ve bilgi güvenliği için politika ve amaçların belirlenmesi ihtiyacını anlamak,
- b) Kuruluşun tüm iş risklerini yönetmek bağlamında kuruluşun bilgi güvenliği risklerini yönetmek için kontrolleri gerçekleştirmek ve işletmek,
- c) BGYS'nin performansı ve etkinliğini izlemek ve gözden geçirmek,
- d) Nesnel ölçmeye dayalı olarak sürekli iyileştirmek.

BGYS yaşayan bir süreç olmak zorundadır. Bu nedenle de Standard BGYS için, planla-uygula-kontrol et-önlem al (PUKÖ) döngüsünü benimsemiştir.

BGYS proseslerine uygulanan PUKÖ modeli aşamaları şu şekilde özetlenebilir:

Planlama; BGYS'nin kurulmasını ifade etmektedir. Kurumun BGYS politikası, amaçları, hedefleri, prosesleri ve prosedürlerinin oluşturulur.

Uygulama; BGYS'nin gerçekleştirilmesi ve işletilmesini yani, BGYS politikası, kontroller, prosesler ve prosedürlerin gerçekleştirilip işletilmesini ifade etmektedir.

Kontrol et; BGYS'nin izlenmesi ve gözden geçirilmesi, BGYS politikası, amaçlar ve kullanım deneyimlerine göre proses performansının değerlendirilmesi ve uygulanabilen yerlerde ölçülmesi ve sonuçların gözden geçirilmek üzere yönetime rapor edilmesini ifade etmektedir.

Önlem al; BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi, yönetimin gözden geçirme sonuçlarına dayalı olarak, düzeltici ve önleyici faaliyetlerin

gerçekleştirilerek BGYS'nin sürekliliğinin ve iyileştirilmesinin sağlanmasını ifade etmektedir.

Bu aşamalar sürekli bir biçimde birbirini izleyerek yaşayan bir sistem oluşturmaktadır.

Kurumsal bilgi güvenlik politikalarının oluşturulması, BGYS kapsamının belirlenmesi, varlıkların yönetimi, risk yönetimi, dokümantasyon oluşturma, denetim kontrollerinin seçilmesi, uygulanabilirlik beyannameleri ve yönetimin gözden geçirmesi BGYS'nin kurulum adımlarıdır.

BGYS'nin kurulması; varlık envanterinin yapılması, bu varlıklara karşı olası risk ve tehditlerin tespit edilmesi, güvenlik politikalarının oluşturulması, denetimlerin ve uygulamaların kontrolü, uygun çözümlerin geliştirilerek sistemin iyileştirilmesi gibi birbirini izleyen ve tamamlayan denetimlerin gerçekleştirilmiş olması demektir.

ISO 27001'in öngördüğü bir BGYS kurmak kurumlara birçok yarar sağlayacaktır.

BGYS kurma adımlarının izlenmesi sonucunda kurum her şeyden önce bilgi varlıklarının farkına varacaktır. Hangi varlıkları olduğunu ve bu varlıkların önemini anlayacaktır.

Risklerini belirleyip yöneterek en önemli unsur olan iş sürekliliğini sağlayabilecektir. İş sürekliliğinin sağlanması kurumun faaliyetlerine devam edebilmesi anlamına gelmektedir.

Bilgilerin korunacağından, kurumun iç ve dış paydaşlarında bir güven duygusu oluşturur, motivasyon sağlar. Daha iyi bir çalışma ortamı yaratılmasına katkı sağlar. Aynı zamanda kurum açısından prestij sağlar.

Bilgilerin bir sistematik içerisinde güvenliği sağlanmış olur. Bilgi güvenliği ihlalinin hangi nedenden kaynaklandığı daha hızlı bir şekilde belirlenir ve ne önlem alınacağı kararı etkin ve hızlı bir biçimde verilebilir.

Kurum, kuruluş ve işletmelerin belirli güvenlik standartları çerçevesinde bilgi güvenliğini sağlayarak iç ve dış tehditler karşısında zarar görmeden veya en az zararlar iş sürekliliklerini devam ettirebilmeleri için bilgi güvenliği standartlarını kendi kuruluşlarında uygulamaları artık neredeyse bir zorunluluk haline gelmiştir. Kurumların, bilgi sistemleri süreçlerini inceleyerek tehditleri ve riskleri belirlemesi ve bu riskleri kabul edilebilir bir seviyeye indirebilmesi için alınacak karşı önlemlerin tespit edilmesi gerekmektedir(Bg kurumsal bazda uygulanması).⁹

2.1 BİLGİ GÜVENLİĞİ ÖNLEMLERİ

Kurumların bilgi güvenliği açısından kendilerinin yeterli olup olmadığını Standardın Ek A bölümünde yer alan Çizelge A.1- Kontrol amaçları ve kontroller kısmındaki maddelerle denetleyebilir.

Bilgi güvenlik politikası

Amacı, bilgi güvenliği için, iş gereksinimleri ve ilgili yasa ve düzenlemelere göre yönetim yönlendirmesini ve desteğini sağlamaktır.

Kurumsal bilgi güvenlik politikası ile bilgi güvenliği konusunda yönetimin bakış açısını, onayını ve desteğini çalışanlara iletmek hedeflenmektedir. Bu doküman yönetim tarafından onaylanmalı, yayınlanmalı ve tüm çalışanlarla ilgili dış taraflara bildirilmelidir.

Güvenlik süreci, ciddi boyutta bir kültür değişimi gerektirdiği için hem birçok önemli konuda organizasyonun kural ve yasalarını hem de yönetimin ciddi yaklaşımını ve kararlılığını yansıtmaları anlamında kurumsal bilgi güvenlik politika dokümanı önemlidir. Belirli aralıklarla veya önemli değişiklikler ortaya çıktığında sürekli uygunluğunu, doğruluğunu ve etkinliğini sağlamak için gözden geçirilmelidir.

⁹ Ş.Sağiroğlu, E.Ersoy ve M.Alkan, Bilgi güvenliğinin kurumsal bazda uygulanması, Bildiriler Kitabı uluslararası katılımlı bilgi güvenliği ve kriptoloji konferansı, 2007.

Kurumun iş hedefinin ve onun bilgi güvenliğine bağlılığının tam olarak anlaşılmasını sağlar. Bu oldukça önemli bir görevdir ve üst yönetimin kesin kararını açığa vurmaktadır. Gerçek kullanıcıların ihtiyaçlarını yansıtmalıdır. Uygulanabilir, anlaşılması kolay olmalıdır ve koruma düzeyiyle üretkenliği dengelemelidir. Aşırı korumacı politikaların çalışmayı engelleyerek verimliliği düşürebileceği unutulmamalıdır. Bu nedenle politika belirlerken genel ifadeler kullanılmalıdır. Politika, personel güvenliği, fiziksel güvenlik, prosedürel ve teknik alanlar gibi bütün önemli alanları kapsamalıdır.

Kurumsal bilgi güvenlik politikası ile ilgili ilerleyen bölümlerde daha detaylı bilgi verilecektir.

Bilgi güvenliği organizasyonu

Bilgi güvenliği organizasyonu, bilgi güvenliği organizasyonel altyapısının oluşturulmasını ve yönetilmesini hedeflemektedir.

İç organizasyon ve dış taraflar olarak ele alınmalıdır. İç organizasyonda amaç, kuruluş içerisindeki bilgi güvenliğini yönetmektir. Dış taraflar olarak ele alınmasındaki amaç ise, kuruluşun dış taraflarca erişilen, işlenen, iletişim kurulan veya yönetilen bilgi ve bilgi işleme olanaklarının güvenliğini sağlamaktır.

Organizasyonda gerekli rol ve sorumluluklar belirlenmeli, tüm rollerin işbirliği içinde çalışabilmeleri için iş süreçleri oluşturulmalıdır. Bu organizasyon içinde en önemli görev, güvenlik değişim yönetiminin yapılmasıdır. Riskler, iş yapış biçimi, organizasyonel değişimler, bilgi varlıkları, iş ilişkileri, iş ortakları vb. açılardan güvenlik politikası, organizasyonu ve süreçlerine ilişkin değişim yönetimi yapılmalı ve gerekli düzenleme ile geliştirmeler hayata geçirilmelidir.

Varlık yönetimi

Yorucu ve önemli görevlerden biridir. Bilgi varlıkları, yazılım varlıkları, fiziksel varlıklar ya da diğer benzer servisler olabilen bütün bilgi teknolojileri varlıklarını yönetmeyi ifade eder.

Varlıkların sorumluluğu ve bilgi sınıflandırması olarak iki aşamada gerçekleştirilir. Varlıkların sorumluluğunda amaç, kurumsal varlıkların uygun

korunmasını sağlamak ve sürdürmektir. Bilgi sınıflandırmasında amaç, bilgi varlıklarının uygun seviyede koruma almalarını sağlamaktır.

Varlık envanter dokümanı oluşturulmalı, varlıkların şu an buldukları yer bilgisi tutulmalı, tüm varlıklar için değer ve önemini yansıtan (gizlilik vb.) bir etiketleme yöntemi düşünülmeli ve bu varlıkların nasıl ele alınacağına ilişkin süreçler belirlenmelidir. Örneğin çok gizli bilgilerin kopyalanması, saklanması, elektronik posta ile gönderiminin nasıl olması gerektiğine vb. ilişkin prosedürler belirlenmeli ve sahiplikleri ile sorumlulukları belli kişilere verilmelidir.

İnsan kaynakları güvenliği

İnsan hataları ve ihmalleri bir çok hırsızlığın, dolandırıcılığın ya da imkanları kötü kullanmanın kaynağıdır.

Kurum çalışanlarının görevlerine güvenlik ile ilgili rol ve sorumlulukları tanımlanmalıdır. Bu rol ve sorumluluklar değişim yönetiminin bir gereği olarak düzenli bir biçimde revize edilmelidir.

Dikkatli ve iyi eğitilmiş çalışanlar olası güvenlik ihlallerini engelleyebilir. Bu nedenle, çalışanların bilgi güvenliği konusunda bilinçlendirilmesi, bu hususta farkındalık yaratılması ve eğitimlerin düzenlenmesi gereklidir.

İstihdam öncesi, çalışma esnasında ve istihdamın sonlandırılması veya değiştirilmesi aşamalarının her birinde farklı önlemler alınmalıdır. İstihdam öncesi güvenliğin amacı, çalışanlar, yükleniciler ve üçüncü taraf kullanıcıların kendi sorumluluklarını anlamalarını ve düşünüldükleri roller için uygun olmalarını sağlamak ve hırsızlık, sahtecilik ya da olanakların yanlış kullanımı risklerini azaltmaktır. Çalışma esnasında güvenliğin amacı, tüm çalışanlar, yükleniciler ve üçüncü taraf kullanıcıların bilgi güvenliğine ilişkin tehditler ve kaygıların ve kendi sorumluluklarının farkında olmalarını ve normal çalışmaları sırasında kurumsal güvenlik politikasını desteklemek ve insan hatası riskini azaltmak üzere donatılmalarını sağlamaktır. İstihdamın sonlandırılması veya değiştirilmesi esnasında güvenlik amacı, çalışanlar, yükleniciler ve üçüncü taraf kullanıcıların düzenli bir şekilde kuruluştan ayrılmalarını veya istihdamın değiştirilmesini sağlamaktır.

Fiziksel ve çevresel güvenlik

İşletme alanlarına ve bilgiye yetkisiz erişimi, hasarı ve müdahaleyi engellemek için tasarlanan güvenli fiziksel çevre genellikle her güvenlik planının başlangıç noktasıdır.

Güvenli alanlar ve teçhizat güvenliği olarak ele alınmalıdır. Güvenli alanlar kavramındaki güvenlik amacı, kuruluş binalarına, ünitelerine ve bilgilerine yetki dışı fiziksel erişimi, hasarı ve müdahaleyi engellemektir. Teçhizat güvenliği amacı, varlıkların kaybını, hasarını, çalınmasını ya da tehlikeye girmesini ve kuruluşun faaliyetlerinin kesintiye uğramasını engellemektedir.

Bu fiziksel güvenlik çerçevesi, fiziksel giriş kontrolü, yangından elektromanyetik radyasyona kadar dağılan riskleri minimize edecek koruma araçlarını sağlama, güç kaynaklarına ve bilgi kablolarına yeterli güvenliği sağlama gibi bazı aktiviteleri kapsar. Etkin maliyetli tasarım ve sürekli izleme, yeterli fiziksel güvenlik kontrolünü korumak için iki anahtar durumdur.

Haberleşme ve işletim yönetimi

Bütün haberleşme ve işletim yönetimi ve faaliyeti için uygun bir biçimde belgelenmiş prosedürler tespit edilmelidir. Bu ayrıntılı işletim yönergelerini ve olay cevap prosedürlerini içerir.

Operasyonel prosedürler ve sorumluluklar, üçüncü taraf hizmet sağlama yönetimi, sistem planlama ve kabul, kötü niyetli ve mobil koda karşı koruma, yedekleme, ağ güvenliği yönetimi, ortam işleme, bilgi değişimi, elektronik ticaret hizmetleri ve izleme bölümlerini içerir. Operasyonel prosedürler ve sorumluluklar, bilgi işleme olanaklarının doğru ve güvenli işletimini sağlamayı amaçlayan bir uygulamadır. Üçüncü taraf hizmet sağlama yönetiminin amacı, üçüncü taraf hizmet sağlama anlaşmalarıyla uyumlu olarak uygun bilgi güvenliği ve hizmet dağıtım seviyesini gerçekleştirmek ve sürdürmektir. Sistem planlama ve kabulün amacı, sistem başarısızlıkları riskini en aza indirmektir. Kötü niyetli ve mobil koda karşı korumada amaç, yazılım ve bilginin bütünlüğünü korumaktır. Yedekleme ise bilgi ve bilgi işleme olanaklarının bütünlüğünü ve kullanılabilirliğini sağlamayı amaçlamaktadır. Ağ güvenliği yönetiminde amaç, ağdaki bilginin ve destekleyici altyapının korunmasını sağlamaktır. Ortam işleme, varlıkların yetkisiz ifşa edilmesi, değiştirilmesi, kaldırılması veya yok edilmesini ve iş faaliyetlerinin kesintiye

uğramasını önlemeyi amaçlamaktadır. Bilgi değişiminin kontrolü, bir kuruluş içindeki ve herhangi bir dış varlık ile değiştirilen bilgi ve yazılımın güvenliğini sağlamayı amaçlamaktadır. Elektronik ticaret hizmetlerinde amaç, hizmetlerin güvenliğini ve bunların güvenli kullanımını sağlamaktır. İzleme, yetkisiz bilgi işleme faaliyetlerini algılamayı amaçlar.

Bilginin ve yazılımın dış kaynaklar arasında değişimi kontrol edilmelidir ve ilgili yasalarla uyumlu olmalıdır. Uygun bilgi ve yazılım değişim anlaşmaları olmalıdır, geçişteki araçlar güvenli olmalıdır ve yetkisiz ulaşımlara, yanlış kullanımlara ve bozulmalara karşı korunmalıdır.

Network yönetimi bilgisayar network güvenliğine ulaşmak ve korumak için bir takım kontrolleri gerektirir. Kamu networku üzerinden geçen bilginin gizliliğini ve bütünlüğünü korumak için özel kontroller yerleştirilmelidir. Özel kontroller ayrıca network servislerinin ulaşılabilirliği için de gerekebilir.

Elektronik ticaret, internet gibi kamu networku üzerinden elektronik bilgi değiş tokuşunu, elektronik mail ve online kayıtları içerir. Elektronik ticaret, hileli aktivitelere, sözleşme uyuşmazlıklarına ve bilginin açığa vurulmasına ya da değişikliğine sebep olabilecek birçok network tehdidine karşı korunmasıdır. Elektronik ticaretin bu gibi tehditlerden korunması için kontroller uygulanmalıdır.

Erişim kontrolü

Erişim kontrolü için iş gereksinimi, kullanıcı erişim yönetimi, kullanıcı sorumlulukları, ağ erişim kontrolü, işletim sistemi erişim kontrolü, uygulama ve bilgi erişim kontrolü ve mobil bilgi işleme ve uzaktan çalışma aşamalarından oluşur. İş gereksinimi aşaması, bilgiye erişimi kontrol etmek amaçlıdır. Kullanıcı erişim yönetiminde, bilgi sistemlerine yetkili kullanıcı erişimini sağlamak ve yetkisiz erişimi önlemek amaçlanmaktadır. Kullanıcı sorumlulukları, yetkisiz kullanıcı erişimini ile bilgi ve bilgi işleme olanaklarının tehlikeye atılmasını ya da çalınmasını önlemek amacıyla belirlenmelidir. Ağ erişim kontrolünde amaç, ağ bağlantılı hizmetlere yetkisiz erişimi önlemektir. İşletim sistemi erişim kontrolü, işletim sistemine yetkisiz erişimi önlenmek amaçlıdır. Uygulama ve bilgi erişim kontrolü, uygulama sistemlerinde tutulan bilgilere yetkisiz erişimi önlemektedir. Mobil bilgi

işleme ve uzaktan çalışma kontrolü, mobil bilgi işleme ve uzaktan çalışma hizmetlerini kullanırken de bilgi güvenliğini sağlamak amacıyla yapılmalıdır.

İş ve güvenlik gereklilikleri doğrultusunda, bilgiye erişim kontrol altında tutulmalıdır. Sadece gerekli olan personele, gerektiği kadar erişim yetkisi sağlanmalı, erişim kontrolü kuralları ve süreçleri belirlenmelidir.

Kullanıcılar erişim hakları ile bu konuda kendi sorumluluk ve yükümlülükleri hakkında bilgilendirilmiş ve bilinçlendirilmiş olmalıdır.

Ağ servislerine yetkisiz erişimler, tüm organizasyonu etkileyecek risklerdir. Kullanıcılara sadece, kendi işlerinin devamı için gerekli olacak doğrudan ağ bağlantısı sağlanmalı, kullanıcı terminalinden bilgisayar servisine kadar tüm ağ servisi kontrol altında olmalıdır. Gerektiğinde iletişim, ayrılmış hatlar üzerinden sağlanabilmeli, belli kullanıcılar için menü ve alt menüler kısıtlanmalı, ağ erişimi sınırlandırılabilmesi, dış bağlantılar için kullanıcı doğrulama çözümleri kullanılmalı ve gerekli durumda bağlantı süresi kısıtlanabilmelidir.

Bilgi sistemleri edinim, geliştirme ve bakımı

Yazılım alım, geliştirme ve bakım süreçlerinde güvenlik ihmal edilmemelidir.

Geliştirilen bilgi sistemleri iş uygulamalarının, tüm güvenlik ihtiyaçlarının karşılamasını ve organizasyon güvenlik politikalarını destekleyecek şekilde planlanıp tasarlanmasını garantilemek üzere, güvenlik ihtiyaçları tanımlanmalı ve belgelenmelidir. Uygulama sistemi verilerinin kaybını, yetkisiz değişimini ve kötüye kullanımını önlemek üzere, gerekli kontroller uygulama içine yerleştirilmeli, kullanıcı ve işlem kayıt bilgilerinin uygulama tarafından tutulması sağlanmalıdır. Veri girişinde hataya neden olabilecek, güvenlik açığı oluşturabilecek konular düşünülerek kontroller konulmalı, gerekli kodlama yapılmalı ve test edilmelidir. Gerektiğinde mesaj doğrulama teknikleri, kriptografik çözümler uygulanmalıdır.

Bilgi sistemlerinin güvenlik gereksinimleri, uygulamalarda doğru işleme, kriptografik kontroller, sistem dosyalarının güvenliği, geliştirme ve destekleme proseslerinde güvenlik ve teknik açıklık yönetimi adımlarından oluşmaktadır. Bilgi sistemlerinin güvenlik gereksinimleri belirlenerek güvenliğin bilgi sistemlerinin dahili bir parçası olması sağlanmalıdır. Uygulamalarda doğru işleme sağlanarak

uygulamalardaki bilginin hataları, kaybı, yetkisiz deęiştirilmesi ve kötüye kullanımı önlenmelidir. Kriptografik kontroller, bilginin gizliliğini, aslına uygunluęunu ya da bütünlüğünü kriptografik yöntemlerle koruma amacıyla yapılır. Sistem dosyalarının güvenlięi sağlanmalıdır. Geliştirme ve destekleme proseslerinde güvenlik, uygulama sistem yazılımı ve bilgisayarın güvenlięini sağlamayı ifade etmektedir. Teknik açıklık yönetimi yapılarak teknik açıklıkların istismarından kaynaklanan riskler azaltılır.

Bilgi güvenlik ihlal olayı yönetimi, bilgi güvenlięi olayları ve zayıflıklarının rapor edilmesi ile bilgi güvenlięi ihlal olayları ve iyileştirmelerin yönetilmesi adımlarını içerir. Bilgi güvenlięi olayları ve zayıflıkları, bilgi sistemleri ile ilişkili bilgi güvenlięi olayları ve zayıflıkları, zamanında düzeltici önlemlerin alınabilmesi için rapor edilir. Bilgi güvenlięi ihlal olaylarına tutarlı ve etkili bir yaklaşımın uygulanmasını sağlamak için bilgi güvenlięi ihlal olayları ve iyileştirmelerinin yönetimi yapılmalıdır.

İş süreklilięi yönetimi

Güvenlik sürecinin en önemli kavramlarından biri iş süreklilięi yönetimidir. Büyük çaplı sistem çökmeleri, arızalar ya da doğal felaketler gibi durumlarda, kritik işlerin devamını sağlayabilmek üzere gerekli önlemler alınmalıdır. Bu konuda önlem ve çözümlere karar vermek üzere, öncelikle iş süreklilik ve etki analizi yapılmalıdır. Belirlenen risklerin gerçekleşmesi durumunda, işin belli seviyede devamı için yapılacaklar, sorumluluklar, iletişim bilgileri, operasyon detayları, acil durumu ortadan kaldırmak üzere yapılması gerekenler belirlenmelidir. Yapılan acil durum planları düzenli aralıklarla test edilmeli ve doğrulanmalıdır; test sonuçlarına göre gerektiğinde yeniden düzenlenmelidir.

Uyum

Bilgi sistemleri tasarımı, operasyonu, kullanımı ve yönetimi birtakım kanuni, düzenleyici veya sözleşmeye dayalı yaptırımlara tabi olabilir. Bu başlık altında, bu yaptırımların ve ilgili güvenlik gerekliliklerinin ihlalinin önlenmesi hedeflenmelidir. Örneğin fikri haklara ilişkin yasalarla uyum için ilgili süreçler, kural ve politikalar belirlenmeli ve belgelenmelidir. Yasal gereklilik nedeniyle belirli süreyle saklanması gereken kayıtlar kayıp, imha ve sahtecilik risklerine karşı uygun şekilde korunmalıdır.

Yasal gereksinimlerle uyum, güvenlik politikaları ve standartlarla uyum ve teknik uyum ve bilgi sistemleri denetim hususlarını ifade eder. Yasal gereksinimlerle uyum, her türlü hukuka, yasal, düzenleyici ya da sözleşmeye tabi yükümlülüklerle ve her türlü güvenlik gereksinimlerine ilişkin ihlalleri önlemeyi ifade etmektedir. Güvenlik politikaları ve standartlarla uyum ve teknik uyum, sistemlerin kurumsal güvenlik politikaları ve standartlarıyla uyumunu sağlamayı amaçlar. Bilgi sistemleri denetim hususları, bilgi sistemleri denetim prosesinin etkinliğini artırıp müdahaleleri azaltmak için belirlenir.

2.1.1 Kurumsal Bilgi Güvenliği Önlem Türleri

Kurumsal bilgi güvenliği, bilginin üretildiği, işlendiği ve saklandığı her ortamda sağlanmak zorundadır. Bunun için mevcut yazılımlar, donanımlar, ortamlar ve insan kaynakları dikkate alınmalıdır.

Yukarıda, Standard çerçevesinde kurumsal bilgi güvenliğinin sağlanması için önlemler alınması gereken alanlar ve önlem türlerinden bahsedildi.

Bilgi güvenliğine yönelik olarak bahsi geçen önlemleri genel olarak 3 başlık altında toplamak mümkündür:

1. Yönetimsel önlemler
2. Teknolojik önlemler
3. Eğitim

Kurumsal bilgi güvenliği yönetim, teknoloji ve eğitim üçgeninde devamlılık gerektiren ve bu üç unsur arasında tamamlayıcılık olmadığı sürece etkin bir güvenlikten bahsedebilmenin mümkün olmayacağı yönetilmesi zorunlu olan canlı bir süreçtir.

Bu üç önlem türünün her biri, başarıya ulaşmak için diğer iki önlem türü ile tam ve eksiksiz çalışmalıdır. Bu üç önlem türü birbirileri ile ayrılmaz ve sıkı bağlarla sahiptir. Bir kurumun bilgi güvenliği bu üç önlem türünün birlikte çalışmasıyla sağlanabilmektedir.

2.1.1.1 Yönetmel Önemler

Yalnız teknolojik önlemlerle (anti-virüs, "firewall" 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 bireysel olarak ve kurum bazında bir güvenlik politikası oluşturmak, bunu yazılı olarak dokümanete etmek ve çalışanlarına, iş ortaklarına, paydaşlarına aktarmak zorundadır. 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, çalışanlarını bilgilendirmeli ve Bilgi Güvenliği sistemi, iş ortaklarını (müşteri, tedarikçi, taşeron, ortak firma vb.) da kapsamalıdır.¹⁰

Yönetmel Önemler, güvenlik yönetimi ile ilgili bir dizi kuralın ortaya koyulması ve uygulanması şeklinde özetlenebilir. Hemen her konuda olduğu gibi, bilgi güvenliğinin yönetiminde de başarı; iyi bir planlama ve üst düzey politikaların doğru ve tutarlı bir şekilde belirlenmesi ile elde edilebilir. Bunun ardından, belirlenenlerin yazıya dökülmesi, yani prosedür, yönerge ve talimatlar gibi dokümanların oluşturulması gelmelidir.¹¹

Üst yönetimin desteği olmadan, kurumsal tabanda bir işi gerçekleştirmek hayli zordur. Bu nedenle üst yönetim ile güvenlik yönetimi arasında açık bir iletişim kanalı kurulmalı ve her iki yönde de kusursuz bir bilgi akışı sağlanmalıdır. Bu sayede, yürütülen güvenlik yönetim programı üst yönetimden ihtiyacı olan desteği alır, üst yönetim de gerektiğinde devreye girerek gerekli stratejik kararları verir.¹²

Yönetmel önlemler kapsamında yapılması gereken temel işlemler şunlardır:

1. Risk yönetimi

¹⁰ A. ONUR, Kurumsal Bilgi Güvenliği'ne Bakış, http://www.bilgiyonetimi.org/cm/pages/mkl_gos.php?nt=474.

¹¹ Bilişim Güvenliği Sürüm 1.1, Pro-G Bilişim Güvenliği ve Araştırma Ltd., 2003

¹² Bilişim Güvenliği, a.g.e., s. 14

2. Güvenlik politikaları
3. Standartlar, yönergeler ve prosedürler
4. Güvenlik denetimleri

2.1.1.1.1 Risk yönetimi

Risk, sözlük anlamı olarak zarara uğrama tehlikesidir; öngörülebilir tehlikeleri ifade eder. Risk Yönetimi ise bir kurumun ya da kuruluşun çalışabilirliğini, ticari müesseseler içinse öncelikle karlılığını olumsuz yönde etkileyebilecek risk faktörlerinin belirlenmesi, ölçülmesi ve en alt düzeye indirilmesi sürecidir¹³.

Bir sistemin nasıl korunacağına karar vermeden önce, onu hangi tehlikelere karşı korumak gerektiği bilinmelidir. Coğrafyanın karakteristiğinden, teknik hatalara, intikam almak isteyen eski çalışanlardan "hacker"lara kadar tüm riskler göz önünde tutulmalıdır¹⁴.

Doğrudan ve dolaylı maliyetler dikkate alınmadığında, bir kurum için, kağıt üstünde "çok güvenli" bir güvenlik altyapısı kurmak kolaydır. Ancak kurumun hedefi, kendisi için "yeterli, etkin ve yönetilebilir" bir güvenlik altyapısını oluşturmak olmalıdır. Bu yeterlilik düzeyini belirlemede risk analizi önemli bir role sahiptir. Risk analizi yardımıyla kurumlar, karşı karşıya buldukları riskleri öncelik sırasına koyabilir ve her bir riske karşı alınacak önlemlerin ve tedbirlerin getireceği maliyetleri değerlendirebilirler¹⁵.

Risk yönetimi riskin tümüyle engellenmesi değil, sorunlara sistematik ve dikkatli bir şekilde yaklaşılması ve almaya karar verilen risklerin dikkatli yönetimi yoluyla gereksiz kayıpların engellenmesidir. Başarılı bir risk yönetimi için, kurumun

¹³ Bilişim Teknolojilerinde Risk Yönetimi, TBD Kamu –BİB Kamu Bilişim Platformu VIII.

¹⁴ Uygun Güvenlik Çözümüne Yolculuk, a.g.e.

¹⁵ "Bilişim Güvenliği", a.g.e., s. 13

varlıklarına ve hedeflerine yönelik riskleri belirlemek, analiz etmek, kontrol altında tutmak ve izlemek gereklidir¹⁶.

Burada önemle üzerinde durulması gereken konu etkinliktir. Risklerin ortadan kaldırılması veya azaltılması için kontrollerin oluşturulması gereklidir, ancak çok fazla kontrol sebebiyle iş yapılamaz duruma gelinmesi de kurumlar için bir risk faktörü olabilmektedir. Risk yönetimi prosedürleri oluşturulurken getiriler ve etkinlik iyi değerlendirilmelidir¹⁷.

Risk analizi, risklerin gerçekleşme olasılıklarının, gerçekleşmeleri durumunda yol açacakları kayıpların doğru bir şekilde belirlenmesi ve buna göre uygun tedbirlerin devreye sokulmasıdır. Risk analizinin üç temel amacı vardır:

- Risklerin belirlenmesi
- Tehditlerin potansiyel etkisinin belirlenmesi
- Riskin gerçekleşmesi durumunda getireceği zararlar, bu riskten korunmak için seçilecek tedbir arasında ekonomik bir denge kurulması¹⁸.

Risk değerlendirmesi çalışmasında aşağıdaki esaslar göz önünde bulundurulmalıdır:

- a) Bilgi varlıklarının (ekipman, yazılım vb.) ya da iş varlıklarının ve aktivitelerinin tanımı ve değerinin tespit edilmesi;
- b) Bu varlıklara karşı, içeriden veya dışarıdan gelebilecek tehditlerin belirlenmesi;
- c) Bu tehditlerin oluşma olasılığının belirlenmesi;

¹⁶ Bilişim Teknolojilerinde Risk Yönetimi, a.g.e.

¹⁷ Bilişim Teknolojilerinde Risk Yönetimi, a.g.e.

¹⁸ Bilişim Teknolojilerinde Risk Yönetimi, a.g.e.

- d) Bu tehditlerin kurumdaki etkilerinin belirlenmesi;
- e) Tehditlerin engellenmesi veya kabul edilebilir bir seviyeye indirilmesi için gerekli ek kontrollerin belirlenmesi;
- f) Ek kontrollerin uygulanması için aksiyonların planlanması.

Risklerin yukarıda belirtildiği şekilde tanımlanması ve önceliğinin belirlenmesi yanı sıra; bu risklerin azaltılması ya da ortadan kaldırılmasına yönelik kontrol ve çözüm alternatifleri; maliyet, uygulanabilirlik ve yararlılık ilkeleri doğrultusunda değerlendirilmeli, gerekli önlemler planlanarak uygulanmalıdır¹⁹.

2.1.1.1.2 Güvenlik Politikaları

Kurumsal bilgi güvenliği politikası, kurum ve kuruluşlarda bilgi güvenliğinin sağlanması için tüm bilgi güvenlik faaliyetlerini kapsayan ve yönlendiren talimatlar olup tüm çalışanların ve ortak çalışma içerisinde bulunan diğer kurum ve kuruluşların uymaları gereken kuralları içeren kabul edilebilir güvenlik seviyesinin tanımlanmasına yardım eden resmi bir belge niteliğindedir.

BGYS çerçevesinde oluşturulacak güvenlik politikalarına üst yönetim ve tüm çalışanların destek vermesi ve tavizsiz bir şekilde uyması, işbirliğinde bulunulan kişi ve kurumlarında bu politikalara uyma zorunluluğunun getirilmesi kurumsal bilgi güvenliğinin sağlanmasında önemli bir faktördür.

İyi bir bilgi güvenlik politikası, öncelikle uygulanabilir olmalıdır. Politika kullanıcıların ve sistem yöneticilerinin eldeki olanaklarla uyabilecekleri kurallar ve ilkelerden oluşmalıdır. Politika yeterli düzeyde yaptırım gücüne sahip olmalıdır. Alınan güvenlik önlemleri ve politikayı uygulayan yetkililer yaptırımları uygulayabilecek güçle donatılmalıdır. Politika kapsamında herkesin sorumluluk ve yetkileri açıkça tanımlanmalıdır. Kullanıcılar, sistem yöneticileri ve diğer ilgililerin sisteme ilişkin sorumlulukları ve yetkileri kuşku ve çelişkilere yer bırakmayacak biçimde açıklanmalıdır. Gerekli durumlarda istisnalar ve alternatif uygulamalar

¹⁹ Bilişim Sistemleri Güvenliği El Kitabı, Türkiye Bilişim Derneği, Sürüm 1.0, Mayıs 2006, s. 24-25

açıklanmalıdır. Güvenlik politikasının kapsamı da nitelikleri kadar önemlidir.²⁰ Kurumun sahip olduğu bilgi varlıkları ve ihtiyaçları doğrultusunda kapsam belirlenmelidir. Bilgi varlıklarının tamamı kapsam dahilinde olabileceği gibi belirli ortamlarda saklanan bilgi varlıkları da belli bir yerleşim birimindeki bilgi varlıkları da kapsamı oluşturabilir.

Güvenlik politikaları kurumun üst düzey yönetimi tarafından desteklenmeli ve çalışanlar tarafından benimsenmelidir. Güvenlik politikası kullanıcılar tarafından uygulanabilir ve anlaşılabilir, güvenlik yöneticileri tarafından yönetilebilir olmalıdır. Bilgi güvenliği politikaları her kuruluş için farklılık gösterse de, genellikle çalışanın sorumluluklarını, güvenlik denetim araçlarını, amaç ve hedeflerini kurumsal bilgi varlıklarının yönetimini, korunmasını, dağıtımını ve önemli işlevlerin korunmasını düzenleyen kurallar ve uygulamaların açıklandığı genel ifadelerdir. Yönetimin, kurumsal bilgi güvenliği hakkında aldığı ayrıntılı kararları da içerir²¹.

Güvenlik politikası kısımları²²

Bölüm Adı	İçeriği
Genel Açıklama	Politikayla ilgili gerekçeler ve buna bağlı risklerin tanımlamasını kapsar.
Amaç	Politikanın yazılmasındaki amaç ve neden böyle bir politikaya ihtiyaç duyulduğunu açıklar.
Kapsam	Politikaya uyması gereken çalışan grupları (ilgili bir grup veya kurumun tamamı) ve bilgi varlıklarını belirler.
Politika	Uygulanması ve uyulması gereken kuralları veya politikaları içerir.
Cezai Yaptırımlar	Politika ihlallerinde uygulanacak cezai yaptırımları açıklar.

²⁰ D.Akkurt, Bilgi işlem sistemleri için bilgi güvenlik politikası, 2002. <http://www.akkurt.com/kurumsalpolitikalar.html>

²¹ Kurumsal Bilgi Güvenliği: Güncel Gelişmeler, a.g.e.,s: 193.

²² Kurumsal bilgi güvenliği ve standartları üzerine bir inceleme, , a.g.e.,s: 510

Tanımlar	Teknik terimler ile açık olmayan ifadeler listelenerek açıklanır.
Düzeltilme Tarihi	Politika içerisinde yapılan değişiklikler, tarihler ve sebepleri yer alır.

Kurumsal Bilgi Güvenlik Politikası Çeşitleri

Kurumsal bilgi güvenlik politikaları kurumların hassasiyetleri doğrultusunda farklılıklar gösterebilir. Bilgi güvenliğinin temel unsurlarından hangisi kurum için daha önemli durumda ise o unsura önem verilerek politika hazırlanabilir. Kurumsal bilgi güvenliği politikası kuruma özgü olmalıdır ve kurumun ihtiyaçlarına yönelik olmalıdır.

Gizlilik politikası: Elimizde bir miktar bilgi olsun ve bir grup insan bu bilgiye ulaşabilsin, bu bilgi bu grubun dışındakiler için gizli bilgidir. Gizlilik açısından, güvenlik politikası yetkisi olmayanlara bilgi sızmasının ne zaman söz konusu olduğunu tanımlar.²³

Bütünlük politikası: Elimizde bir miktar bilgi olsun ve bir grup bu bilginin bütünlüğüne güvensin, o zaman bu bilgi bu gruba göre bütünlüğü olan bilgidir. Burada söz konusu bir kaynak da olabilir, o zaman o kaynağa güvenen grup için, o kaynak bütünlüğe sahiptir. Bütünlük açısından, güvenlik politikası bilginin hangi durumda, hangi yolla ve/veya kimler tarafından değiştirebileceğini tanımlar. Buna bütünlük politikası denir.

Kullanılabilirlik politikası: Elimizde bir miktar bilgi olsun ve bir grup bu bilgiyi kullanabilsin, o zaman bu bilginin bu grup tarafından kullanılabilir olduğu söylenir. Kullanılabilirlik açısından, güvenlik politikası hangi servislerin ne şartlar altında söz konusu kullanıcılar tarafından kullanılabileceğini tanımlar. Buna kullanılabilirlik politikası denir.

Askeri-yönetimsel güvenlik politikası: Bu çeşit politikalarda ilk amaç gizlilik. Güvenilirlik ve erişilebilirlik de önemlidir ancak birinci planda gizlilik

²³ M. Bishop, Computer Security-Art and Science, Adison –Wesley Professional, 2002.

gelir. Diğer ikisinin üstesinden gelinebilir ancak gizliliğin delinmesinin sonuçları çok ağır olur.

Ticari güvenlik politikası: Bu çeşit politikalarda ilk amaç güvenilirliktir. Bunun isminin ticari olmasının nedeni, ticari uygulamalarda amaç verilerin değiştirilmesini engellemektir.

Politika dokümanları, kuralların farklı ve yanlış anlaşılmasını önlemek, ilgilileri eğitmek, muhtemel sorunları önceden tespit edebilmek, kriz durumlarında hızlı hareket edebilmek gibi faydalar sağlar. Yasal boşlukların olduğu durumlarda, kuruluşun saldırganlardan korunabilmesi için, politika dokümanları, yasal destek oluşturur.

Uygulanacak olan yasal ve ahlaki mahremiyet koşulları açıklanmalıdır. Elektronik mesajların ve dosyaların okunması, kullanıcı işlemlerinin kaydedilmesi gibi kullanıcıların davranışlarının izlenmesine dönük işlemlerin hangi koşullarda yapılacağı ve bu işlemler yapılırken kullanıcının kişisel haklarının nasıl korunacağı açıklanmalıdır.²⁴

Güvenlik politikaları, güvenli bir sistemin nasıl olması gerektiğini tanımlar. Güvenlik politikaları oluşturulurken sisteme gelebilecek bütün tehditler göz önünde bulundurulmalıdır. Ayrıca, güvenlik tehditleri zamanla değiştiğinden, güvenlik politikaları da devamlı kontrol edilip güncellenmelidir. Güvenlik politikalarının etkin olarak kullanılabilmesi için kullanıcıları da güvenlik politikaları konusunda bilgilendirmek gerekmektedir.

Politikalar içerisinde; gerekçelerin ve risklerin tanımlandığı, kapsadığı bilgi varlıkları ve politikadan sorumlu olan çalışanların ve gruplarının belirlendiği, uygulanması ve yapılması gereken kuralların, ihlal edildiğinde uygulanacak cezai yaptırımların, teknik terimlerin tanımlarının ve düzeltme tarihçesinin yer aldığı 7 bölümden oluşmalıdır.²⁵

²⁴ Bilgi işlem sistemleri için bilgi güvenlik politikası, a.g.e.

²⁵ Kurumsal bilgi güvenliği güncel gelişmeler, a.g.e., s:193.

2.1.1.1.3 Standart, yönerge ve prosedürler

Tehditlerin sürekli olarak yenilenmesi, kullanılan yazılım veya donanımlarda meydana gelen güvenlik açıklarının takibi, insan faktörünün kontrolü gibi süreçlerin takip edilebilmesi ve üst seviyede bilgi güvenliğinin sağlanması için bilgi güvenliği sürecinin yönetilmesi için bilgi güvenliği standartları kullanılmalıdır²⁶

Yönergeler, kurumsal bir standardın belli bir uygulamada kullanılmasında güçlük çekildiğinde, yol gösterici bir takım öneriler içerecek şekilde hazırlanırlar. Standartlar, gerçek hayatta ve uygulamada karşılaşılabilecek bütün durumları ele alamayabilir. Bu durumda bir yönerge yardımı ile standartta yeterince açık olmayan "gri alanlar" açıklığa kavuşturulur.²⁷

Yönergeler;

- kanunların karşısında olmamalıdır,
- kurum özellikleri dikkate alınarak geliştirilmelidir,
- ilişkilendirilip bir bütün haline getirilmelidir,
- zaman içinde değişiklik gerektirir,
- uygulanabilirse başarılı olur(tuğkan tuğlular).²⁸

Prosedürler, belli bir işi gerçekleştirmeye yardımcı olmak amacıyla hazırlanmış olan ve atılacak adımları ayrıntılı olarak içeren dokümanlardır.

Prosedür, yönerge ve standartları, tek bir büyük dokümanın içine sıkıştırmak yerine, modüler bir şekilde hazırlamak, kullanım kolaylığı ve esneklik açısından daha verimli bir çalışma sağlayacaktır. Çünkü bu türlerden her birinin kullanım alanı

²⁶ Kurumsal bilgi güvenliği güncel gelişmeler, a.g.e., s:194.

²⁷ Bilişim Güvenliği, a.g.e., s. 27.

²⁸ T.TUĞLULAR, Üniversitelerde Bilgi Güvenliği Politikaları, http://www.ulakbim.gov.tr/dokumanlar/guvenlik/Tugkan_Tuglular.pdf

ve kullanacak kişiler farklılık gösterir bu şekilde dokümanların kullanıcılarına dağıtılması ve gerektiğinde güncellenmeleri kolaylaşmış olur.²⁹

2.1.1.1.4 Güvenlik Denetimleri

Bilgi güvenlik denetimi, maliyete ve bir güvenlik olayının diğer bütün zararlarına uğramaksızın kurumun bilgi güvenliğini belirlemesi için en iyi yollardan biridir.³⁰

Güvenlik denetimleri, sürekli devam eden etkin güvenlik politikalarının tanımlanması ve korunması sürecinin parçasıdır.

Güvenlik denetimlerinin cevaplaması gereken anahtar sorular vardır:

- Şifreleri kırmak zor mu?
- Paylaşılan verilere kimin eriştiğini kontrol etmek için ağ cihazları üzerinde yer alan erişim kontrol listeleri var mı?
- Veriye kimin eriştiğini kaydeden denetleme günlükleri var mı?
- Denetim günlükleri yeniden gözden geçiriliyor mu?
- İşletim sistemleri için güvenlik ayarları endüstri güvenlik uygulamalarına uygun kabul edildi mi?
- Her bir sistem için bütün gereksiz uygulamalar ve bilgisayar hizmetleri elimine edildi mi?
- Bu işletim sistemleri ve ticari uygulamalar var olan seviyeyle uyuyor mu?
- Yedekleme ortamları nasıl saklanıyor? Kim ona erişebiliyor? Güncelleniyor mu?

²⁹ Bilişim Güvenliği, a.g.e., s. 27-28.

³⁰B.Hayes, Conducting a Security Audit: An Introductory Overview, 2003, www.securityfocus.com.

Bunlar bir güvenlik denetiminde değerlendirilebilecek değerlendirilmesi gereken soru türlerinden yalnızca birkaçıdır. Dürüstçe ve dikkatlice bu soruların cevaplanmasıyla kurum gerçekçi olarak önemli bilgilerinin güvenliğinin nasıl olduğunu değerlendirebilir.³¹

Bilgi güvenliği bilgi teknolojilerinden daha fazlasını içerir-sistemi kullanan insanlar da dikkatsizce güvenlik boşlukları açabilir. Bir güvenlik denetimi bilgi teknolojileri altyapısı ve ekip davranışları içinde problemleri ortaya çıkarmayı ve dikkat çekmeyi amaçlar. Her denetim sonuç olarak bütün olası riskleri belirlemeye çalışmalıdır.³²

2.1.1.2 Teknolojik Önlemler

Bilgi güvenliğine ilişkin kurumsal bir politika oluşturmanın temel koşullarından birisi, bilgi ve iletişim teknolojilerinde gözlenen gelişmelerin bilinmesidir. Bu noktada, söz konusu teknolojik gelişmelerin ne olduğunu ve ne yönde olacağını doğru anlamak ve içeriğini doğru belirlemek son derece önemlidir.

Kurumsal bilgi güvenliğinin önemli bir kısmı elektronik ortamdaki bilgilerin saklanması içermektedir. Elektronik ortamdaki bilgilerin korunması için teknolojik önlemlerin alınması gerekmektedir.

2.1.1.2.1 Kriptoloji

Kriptoloji (şifre bilimi); haberleşen iki veya daha fazla tarafın bilgi alışverişinin güvenli olarak gerçekleşmesini sağlayan tekniklerin ve uygulamaların bütünüdür. Kişiler arası veya kamu kurumları arasındaki iletişimde uygulanabilecek bir yöntemdir.

Kriptografi, belgelerin şifrelenmesi ve şifrenin çözülmesi için kullanılan yöntemlere verilen addır. Bilgi güvenliğinin sağlanması için başkası tarafından dinlenme, bilginin değiştirilmesi, kimlik taklidi gibi tehditlerin engellenmesinde

³¹ Conducting a Security Audit: An Introductory Overview, a.g.e.

³² J. Kapp, How to conduct a security audit, <http://www.techsupportalert.com/pdf/t04123.pdf>

kullanılabilecek temel araç kriptografidir. Kriptografinin önemli konuları, güvenilirlik, bütünlük, kimlik doğrulama gibi bilgi güvenliği konularındır.

Şifreleme (Encryption), Veriyi bir anahtarla şifrelemeye verilen addır. Hedef, veriyi, gerekli anahtar olmadan çözülebilmesi imkansız mümkün olduğunca yakın şekilde kodlamaktır. Şifre Çözme ise (Decryption) şifrelenmiş veriyi çözüp eski haline getirme işlemidir. Kriptolojide en çok kullanılan kelimelerden olan anahtar ise bir metni şifrelemekte veya açmakta kullanılan veri parçasına (sayı, kelime veya herhangi bir sayısal veri parçası) verilen isimdir.³³

Şifreleme algoritmaları anahtar kullanma yöntemlerine göre genel olarak iki kategoriye ayrılmaktadır; simetrik (veya gizli-anahtar) ve asimetrik (veya açık-anahtar) algoritmaları.

Asimetrik kriptografi; şifreleme ve şifre çözme işlemleri farklı anahtarlarla yapılmaktadır. Asimetrik kriptografi de taraflar aynı şifreleme algoritmasını kullanmaktadırlar.

Simetrik kriptografi; şifreleme ve şifre çözme işlemleri aynı anahtarlarla yapılmaktadır. Taraflar aynı şifreleme algoritmaları kullanır, algoritmalar birbirine uyumludur ve tek anahtar kullanılır.

Simetrik kriptografide, şifreleme ve çözme işlemleri için aynı anahtar veya çözme anahtarı şifreleme anahtarından kolayca türetilen anahtar kullanılırken, asimetrik kriptografi şifreleme ve çözme için farklı anahtar kullanırlar ve çözme anahtarı şifreleme anahtarından elde edilemez.

Genel hatları ile asimetrik ve simetrik kriptografinin güçlü ve zayıf yanlarını şu şekilde özetleyebiliriz.³⁴

³³ O.FINDIK, T.AKSOY, Bilgi güvenliğinin sağlanmasında kullanılan yöntemler ve bunların etkin kullanımı, Akademik Bilişim 2003 konferansı, Çukurova Üniversitesi, 2003.

³⁴ <http://www.kriptoloji.net/>

Asimetrik Kriptografi

Kuvvetli Yönleri

Hazırlanan algoritmaya bağlı kaba kuvvete dirençlidir.

Zayıf Yönleri

Şifrelerin uzunluğundan kaynaklanan algoritmaların yavaş çalışması.

Kriptografinin ana ilkeleri olarak Anahtar uzunlukları bazen sorun saydığımız; bütünlük, kimlik doğrulama çıkarabiliyor olması. ve inkar edememezlik güvenli bir şekilde hizmeti sağlanabilir.

Anahtarı kullanıcı belirleyebilir.

Simetrik Kriptografi

Kuvvetli Yönleri

Algoritmalar olabildiğince hızlıdır.

Zayıf Yönleri

Güvenli anahtar dağıtımı zordur.

Donanımla birlikte kullanılması.

Kapasite sorunu vardır.

Güvenlidir.

Kimlik doğrulama ve bütünlük ilkeleri hizmetlerini güvenli bir şekilde gerçekleştirmek zordur.

Kriptoanaliz ise; kriptografi sistemleri tarafından ortaya konan bir şifreleme sistemini inceleyerek zayıf ve kuvvetli yönlerini ortaya koymayı amaçlayan bilim dalıdır.

2.1.1.2.2 Firewall

Internet, güvensiz bir ağıdır. İnterneti güvensiz yapan paylaşımın fazlalığı ve insanın doğal yok etme içgüdüsüdür.

Ağ güvenliği ile ilintili teknolojilere göz atıldığında, bu alanda en yaygın uygulaması bulunan teknolojinin güvenlik duvarları (firewall) olduğunu öne sürmek mümkün olacaktır. Firewall İngilizceden ateş duvarı olarak çevrilebilir. Aslında itfaiyecilerin kullandığı bir tabir olan Firewall kelimesinin nereden geldiğini anlatmak ne işe yaradığını daha iyi özetleyecektir. Binalarda yangın çıkması

durumunda yanan bir odadaki alevlerin diğerk odalara sıçramaması için özel oda duvarları yapılmıştır. Bu duvarlar ateşten etkilenmez ve ateşin yayılmasını büyük ölçüde önler. Bu duvarlara itfaiyecilerin verdiği isim ise Firewall'dır.³⁵

Güvenlik duvarı ağ güvenlik sisteminin önemli bir parçasıdır. Bir güvenlik duvarı ağ ile Internet gibi herkesin kullanımına açık ağ arasında güvenlik sağlar. Bu iki ağ arasındaki tüm trafik güvenlik duvarı tarafından incelenmektedir.

Güvenlik duvarı bilgisayarınızın kapısında duran bir güvenlik görevlisine benzer. Kimlerin ya da hangi yazılımların bilgisayarınıza giriş yapabileceklerini denetler. Başlangıçta bilgisayarınızın internet bağlantısı da dahil bütün giriş çıkışı engeller, yazılımları kullandıkça, hangi yazılımlara ne kadar erişim hakkı vereceğini sorar.

Güvenlik duvarından sadece izin verilen trafik geçebileceğinden Internet ile özel ağ arasındaki haberleşmenin serbestlik seviyesini kontrol etmede kullanabilir. Güvenlik duvarınızı ayarlarken nelerin yasaklanacağını belirleyebilir ve geri kalan her şeye izin verebilirsiniz. Bu ufak bir ağ için esnek ve uygundur. Fakat büyük bir ağı bu şekilde korumak zordur. Alternatif olarak, güvenlik duvarınızda hangi servislere izin verileceğini belirleyip diğerk her şeyi bloklayabilirsiniz. Bu kullanıcılarına sınırlama getirirse de bu metot daha güvenlidir.

Bir güvenlik duvarının etkili olabilmesi için sızılmasına izin vermemelidir. Ağı veri kaynaklı (zararsız görünüp intranetinize girdikten sonra sisteminize içerden saldıran) saldırılardan koruyamaz. Bu sebeple, kriptolama ve çalışanların eğitilmesi gibi güvenlik önlemleri ile birlikte kullanılmalıdır.

Güvenlik duvarları sadece intranet ile Internet arasındaki haberleşmede kullanılmaz. Aynı zamanda intranet içerisindeki trafiği kontrol etmede ve izlemeye de kullanılabilir. Eğer kurumda tüm dahili bilgilere erişmemesi gereken kişiler varsa ağ güvenlik alanlarına bölünebilir. Eğer sadece bir güvenlik duvarınız varsa ve bir saldırgan onu geçmeyi başarırsa ağdaki tüm bilgilere erişebilir. Fakat dahili güvenlik duvarlarınız varsa sadece bir bölümüne erişebilir.

³⁵ Bilgi güvenliğinin sağlanmasında kullanılan yöntemler ve bunların etkin kullanımı, a.g.e., s:1-2.

2.1.1.2.3 Yedekleme

Yedekleme, en genel anlamıyla, bir bilgisayar sistemini işlevsel kılan temel birimlerin, üzerinde çalışan yazılımların ve depolanan verilerin, arıza, hata, hasar durumlarında çalışmaların kesintiye uğramasını ve / veya verilerin geri dönülemez biçiminde kaybolmasını engellemek amacıyla birden fazla kopya halinde bulundurulmasını sağlayan işlemler bütünüdür.

Yedekler düzenli olarak kontrol edilmeli ve kayıt ortamı sürekli olarak değiştirilmelidir. Yedeklerin fiziksel güvenliği sağlanmalıdır. Kayıt ortamı doğru seçilmeli. Birden fazla farklı ortamda yedekler tutulmalıdır.

Sağlıklı bir yedekleme yönteminde, çeşitli elemanların doğru biçimde seçilmesi ve bir arada uyumlu çalışır hale getirilmesi gereklidir. Bu elemanlar şu şekilde sıralanabilir:

1. **Kaynak:** Yedeklemesi yapılacak verinin, normal işletim sırasında tutulduğu ortam, yedekleme sistemi için kaynak oluşturacak ortamdır.
2. **Yedekleme Donanımı:** Verinin kopyalarını oluşturmak üzere kullanılacak donanım bu başlıkta seçilmelidir. Standart depolama cihazları dışında, özel amaçlı yedekleme donanımları da kullanılabilir.
3. **Yedekleme Yazılımı:** Yedekleme işlemini yürütmek üzere, yedekleme ve kurtarma işlemlerini bir arada yapmayı sağlayan yazılımlar kullanılmaktadır.
4. **Yedekleme Ortamı:** Kopyalanan verinin saklanacağı ortam da yapılacak işleme önemli kısıtlamalar getirmektedir. Bu nedenle yapılacak seçimde ortam seçimi de önem kazanmaktadır.

Yedekleme yöntemi: yazılımlar, farklı yöntemlerle yedekleme yapılmasına imkan verir. Yaygın üç yöntem şöyle sıralanabilir:

1. **Tam (full) yedek:** Bu yöntem, seçilen kaynağın tüm içeriğini yedekler. En güvenilir yöntemdir, ancak zaman ve kapasite ihtiyacı yüksektir. Diğer yöntemler kullanılmadan önce, en az bir kez tam yedek alınmalıdır.

2. **Adımlı (incremental) yedek:** Bu tip yedeklemede, sadece son yedekten bu yana yedeklenmemiş olduğu tespit edilen dosyalar yedeklenir. Kurtarma sırasında önce bu tam yedek, sonra sırasıyla tüm adımlı yedekler kurtarılmalıdır. Bu nedenle güvenilirlik düşer.
3. **Fark (differential) yedek:** Bu tip yedeklemede, son tam yedekten bu yana yedeklenmemiş olduğu tespit edilen dosyalar yedeklenir. Kurtarma sırasında önce tam yedek, sonra son fark yedeği kurtarılmalıdır. Güvenirlik orta düzeydedir.

2.1.1.2.4 Saldırı tespit sistemleri

Günümüzde artan bilgisayar korsanlığı ve internet üzerinden gelen saldırılar, savunma sistemlerinin de gelişmesinde büyük bir rol oynamaktadır.

Uzman olmayan kişiler tarafından kullanılan savunma sistemleri, sisteme zararlı aktivitelerin yapılmasına sebep olmaktadır. Savunma stratejisi belirlemek için, öncelikle saldırgan profilleri ve saldırı çeşitleri tespit edilmelidir. Bu noktada Saldırı Tespit Sistemleri (STS) devreye girmektedir.

STS, internet veya yerel alan ağından gelebilecek ve ağdaki sistemlere zarar verebilecek, çeşitli paket ve verilerden oluşabilen saldırıları farketmek üzere tasarlanmış bir sistemdir. Atak nereden gelirse gelsin önlemini almak üzere üretilmiş bir çözüm olarak, kurum içinden herhangi birisi ya da dışarıdan bir kişi veya kuruluş sisteme girdiği anda bu durumu fark etmekte ve kişinin nereden geldiği ve nereye bağlandığı sorularına ilişkin raporlamalar yapmaktadır. Ayrıca belirlenilen kurallar çerçevesinde gelen saldırıları tespit ederek kısa mesaj servisi (SMS-Short Message Service), e-posta, sistem kaydı ve veritabanı gibi uyarı ve kayıt çıktıları sağlayabilir ve gerekirse Güvenlik Duvarı'na saldırı olduğuna dair uyarı sinyalleri yollayabilir.³⁶

Saldırı Tespit Sistemleri, küçük ve orta boy ağlarda ateşduvarının (firewall) önüne ve arkasına olmak üzere iki noktada konumlandırılmaktadır. Büyük ağlarda ise, sistemin yapısına göre, gerek görülen her noktaya, Saldırı Tespit Sistemi sensörleri konulmaktadır. Ateş duvarımızın önünde konumlandırılması dolayısı ile,

³⁶ Bilişim Sistemleri Güvenliği El Kitabı, a.g.e., s:38.

hiçbir filtrelemeye maruz kalmadan tüm paketleri inceleyebilen sistemimiz, internet ortamında şirketimizin ağına gelen tüm saldırıları ve saldırgan profillerini rahatça ortaya koyabilmektedir. Saldırı tiplerine ve saldırıların hedeflerine bakarak, önlemler almamız kolaylaşmaktadır. Ateşduvarının arkasında, yerel ağımızın içinde bulunan Saldırı Tespit Sistemini konumlandırmak, ilki kadar kolay olmamaktadır. Günümüzde Saldırı Tespit Sistemlerinin problemleri, saldırı olmayan aktiviteleri bazen saldırı olarak algılaması (false-negative) ve saldırı olan aktiviteleri ise bazen saldırı olarak algılamaması (false-positive) olayıdır. Bu yüzden, Saldırı Tespit Sistemlerini uygulanmasında insan faktörü ve bilgi çok önemlidir. Bazı Saldırı Tespit Sistemleri otomatik olarak müdahale etmeye olanak sağlamaktadır. Yani, saldırı kaydı sistemde tespit edilir edilmez, insan faktörü olmadan tepki vermek veya gerekli cihazlarda konfigürasyon değişiklikleri yapmaya olanak sağlar.

Saldırı tespit sistemlerini Gordeev şu şekilde sınıflamaktadır:

1. Analiz yaklaşımı
2. Bilgi tabanlı sınıflandırma
3. Tepki tabanlı yaklaşım
4. Analiz zamanı yaklaşımı
5. Mimari.

Analiz Yaklaşımı: Yanlış kullanım tespiti ve anormallik tespiti olarak ikiye ayrılır. Yanlış kullanım tespitinde desenler ve bilinen atakların imzası saldırıları tanımak için uygun bir formda saldırı tespit sistemine verilir. Anormallik tespitinde ise normal davranış profillerine göre sapmalar bulunmaya çalışılır.

Bilgi Tabanlı Sınıflandırma: Uygulama tabanlı, host tabanlı ve ağ tabanlı olmak üzere üçe ayrılır. Uygulama tabanlı, uygulama katmanında bilgi toplar ve saldırıları tespit eder. Host tabanlı, bir host üzerindeki aktivite bilgilerini toplar. Ağ tabanlı ise ağ trafiğini analiz eder.

Tepki Tabanlı Yaklaşım: Aktif ve pasif saldırı tespitini olarak ikiye ayrılır. Eğer bir saldırı tespit sisteminin verdiği cevaplar otomatik ise o sistem aktif bir sistemdir. Eğer sadece uyarı veriyorsa pasiftir.

Analiz Zamanı Yaklaşımı: Gerçek zamanlı ve aralıklı olarak ele alınabilir. Bir saldırı tespit sistemi bilgi kaynaklarından sürekli olarak bilgi ediniyorsa bu gerçek zamanlı bir saldırı tespit sistemidir. Bu bir atağın ilerlemesini izlemeye yardımcı olur. Periyodik veya zaman aralıklı saldırı tespit sisteminde ise bilgi belli aralıklarla edinilir, sistem kesikli olarak çalışır.

Mimari: Merkezleştirilmiş ve dağıtılmış bir mimari söz konusu olabilir. Merkezleştirme ya bir monolitik modül olarak ya da birbiri ile haberleşen STS fonksiyonlarını yerine getiren bir miktar monolitik modülden oluşur. Dağıtılmış STS ise her biri bir işe atanmış varlıklardan oluşur, dağıtım fiziksel olmayıp fonksiyoneldir.

2.1.1.3 Eğitim

Bilgi güvenliğinin sağlanmasında ne kadar önlem alınmış olsa da insan faktörü göz ardı edilirse hiçbir önlem sonuç vermeyecektir. Çünkü bilgi güvenliği bilinci ve farkındalığı olmayan insanlar bu güvenlik sürecini aksatacaktır.

Bilginin korunmasına çalışıldığı günden bu yana insanlar, güvenlik sürecinin en zayıf tarafını oluşturmuşlardır. Birçok teknik ve yönetsel güvenlik kontrolleri uygulansa dahi bu kontroller saldırganlar tarafından en zayıf halka olan insan kullanılarak çeşitli yöntemlerle kolaylıkla aşılabilmektedir. "Gücünüz en zayıf halkanız kadardır" ilkesi bilgi güvenliği içinde geçerlidir.

Yapılan araştırmalar göstermiştir ki bilgi güvenliği ihlali olayları genellikle kurum çalışanları tarafından yapılmıştır. Bunlardan çoğu bilinçsiz davranışların sonucudur. Nadir de olsa kötü niyetli çalışanların bilgiyi dışarıya sızdırması, kötü amaçlı kullanımı veya yok etmesi de söz konusudur.

Kurumsal bilgi güvenliğinin sağlanmasında insan faktörü önemli bir yere sahiptir. Yeterli bilinç, farkındalık ve eğitim düzeyine sahip olmayan kurum çalışanları ile kurumsal bilgi sistemleri üzerinde yetkileri olan ve yerel saldırgan

olarak adlandırılan iyi niyetli olmayan üst derecede bilgiye sahip olan çalışanlar kurumsal bilgi güvenliğini tehdit eden faktörlerdir.

Bu nedenle günümüzde saldırganlar teknolojik olmayan ve engellenmesi daha zor olan sosyal yöntemleri tercih etmektedirler. İnsan faktörünü kullanmak teknik yöntemlere göre daha tehlikeli sonuçların oluşmasını sağlayan önemli ve güncel bir saldırı aracıdır. Bu saldırı türünü kullanan saldırganlar, sosyal mühendis olarak adlandırılmaktadır. Sosyal mühendislik insan doğasında varolan başkalarına güvenme ve yardım etme eğiliminin başka şekilde elde edilmesi zor olan şeylerin ele geçirilmesi amacı ile kullanılmasıdır. Sosyal mühendislerin amaçları, bilgiye erişim yetkisi olan kullanıcılar aracılığıyla güvenlik teknolojilerinin atlatılmasını (by-pass) sağlamaktır. İnsanlar başkalarının maksatlı olarak kendilerini tuzağa düşürmeyecekleri veya kullanmayacaklarını düşünme eğiliminde olsalar da bu yöntem en sık kullanılan saldırı yöntemlerindedir. Bu yöntem kolay ve hızlı olduğu için saldırganlar tarafından tercih edilmektedir. En yaygın sosyal mühendislik yöntemleri başka birisiymiş gibi davranma, kompliman, aciliyet ve yetkilendirme alınmış duygusu yaratmadır. Bu nedenlerle kullanıcıların sosyal mühendisliğe karşı korunmasını hedefleyen bir eğitim stratejisi izlenmelidir. bilgi güvenliği hususunda çalışanlara eğitim verilerek, yeterli bilince ve bilgiye sahip olması ile bu zaafiyet giderilebilmektedir.

Bilgi güvenliğini sağlamak için en önemli unsur olan insan faktörünün bilgi güvenliği konusunda eğitimi şarttır. Bu eğitim, kurumun hayati fonksiyonlarını yerine getirebilmesini sağlayan bilginin, nasıl korunacağını, neden korunması gerektiğini öğretmelidir. Çalışanlar hatalı davranışlarının kurum bilgi güvenliği üzerinde yaratabileceği etkiyi anlamalıdır.

Eğitimin temel hedefi, çalışanları kurumsal bilgi güvenliği hususundaki görev ve sorumlulukları hakkında bilinçlendirmektir. Ayrıca, güvenlik ve güvenlik kontrollerinin önemi hakkında kolektif bir bilinç oluşturulması amaçlanmaktadır. Kurumdaki tüm personelin bilgi güvenliğinin yarar ve öneminin farkına varması ve bu hususta bilinçlendirilmesini sağlanmaktadır. Çalışanların bilgiyi ve bilgi kaynaklarını koruma konusunda üzerlerine düşen sorumlulukları anlaması kritik öneme sahiptir.

Bilgi güvenliđi ve bu husustaki eđitimler alıřanlar tarafından eski kye yeni adet getirilmesi olarak algılanabilmektedir. Kullanıcılara gre, kurum gvenlik nlemleri olmaksızın gayet iyi alıřmaktadır ve yeni gvenlik nlemleri hayatı zorlařtırıcı gereksiz deđiřikliklerdir. nk alışkanlıkların deđiřmesi sz konusudur. Ancak kullanıcı odaklı eđitimlerle bu bakıř aısı deđiřtirilebilir.

Bilgi güvenliđi bilgi iřlem iři olarak algılandığından, alıřanlar gvenlik Bilgi Teknolojilerinin problemi olduđuna kendisi ile ilgili olmadığına inanmakta ve bu konuda bir sorumluluđu olmadığını dřnmektedir. Oysa bilgi güvenliđi sadece Bilgi Teknolojilerinin ve bilgi iřlem biriminde alıřanların deđil tm personelin sorumluluđudur.

Eđitimler herkese aynı biimde ve aynı ierikte verildiđinde istenilen sonucu vermemektedir. Eđitim verilmeden nce eđitim gereksinimi belirlenip sınıflandırma yapılıp her sınıfa zg bir anlatım biimi ve ierik belirlendiđinde daha etkin bir sonu elde edilmektedir.

Yeni teknolojinin kuruma katılması genellikle kullanıcı davranıřlarının deđiřmesi veya yeni bir bakıř aısına sahip olmasını gerektirir. Ancak, teknoloji bazen eđitimden hızlı veya bađımsız olarak ilerlemektedir. Dolayısıyla, eđitimsiz olarak yeni teknolojinin kullanıma alınması sz konusu olursa bilgi gvenliđinde bir zaafiyet oluřacaktır.

Bu noktadan hareketle eđitimin bir kereye zg bir faaliyet olmaması gerektiđi anlařılmaktadır. Ancak ilk bařtaki ilgi ve heyecanın kaybedilmemesi gerekmektedir. Aksi halde eđitimlerde bilgi gvenliđi de bir angarya olarak grlecektir. İletiřime ncelik verilerek, eđitim alan insanların ihtiyaları ve beklentileri dođrultusunda dzenli ve tutarlı programlar oluřturulması ve ilerletilmesi suretiyle ilgi canlı tutulabilmektedir.

Ancak unutulmaması gereken husus, eđitim ile ancak iyi niyetli ve bilinsiz kullanıcıların bilgi gvenliđi ihlalini gerekleřtirmesinin nne geilebileceđidir. Eđitim, kt niyetli alıřanlara karřı alınacak nlemler arasında yer almamaktadır.

İnsana bağı güvenlik riski hiçbir zaman tamamen yok edilemese de iyi planlanmış bir eğitim programıyla riskin kabul edilebilir bir seviyeye indirilmesi sağlanabilmektedir.

3 KURUMSAL BİLGİ GÜVENLİĞİ DEĞERLENDİRMESİ

Bilgi varlıklarından yazışmaların güvenliği ile ilgili olarak arşiv güvenliğinden bahsedilebilir. 16/05/1988 tarihli ve 19816 sayılı Devlet Arşiv Hizmetleri Hakkında Yönetmelik ile “Türk Devlet ve Millet hayatını ilgilendiren ve en son işlem tarihi üzerinden otuz yıl geçmiş veya üzerinden onbeş yıl geçtikten sonra kesin sonuca bağlanmış olup, birinci maddede belirtilen kuruluşların işlemleri sonucunda teşekkül eden ve onlar tarafından muhafazası gereken, Türk Milletinin geleceğine tarihi, siyasî, sosyal, hukukî ve teknik değer olarak intikal etmesi gereken belgeler ve Devlet hakları ile milletlerarası hakları belgelemeye, korumaya, bunlarla ilgili işlem ve münasebetler bakımından tarihî, hukukî, idarî, askeri, iktisadî, dinî, ilmî edebî estetik, kültürel biyografik, jeneolojik ve teknik herhangi bir konuyu aydınlatmaya, düzenlemeye, tespite yarayan, ayrıca ait olduğu devrin ahlâk, örf ve âdetlerini veya çeşitli sosyal özelliklerini belirten her türlü yazılı evrak, defter, resim, plan, harita, proje, mühür, damga, fotoğraf, film, ses ve görüntü bandı, baskı ve benzeri belgeleri ve malzemeyi” koruma, yararlanma, devir ve yoketme kuralları belirlenmiştir.

Yazılı ortamdaki belgelerin gizliliği ve bütünlüğü bu yasal düzenlemeler ile belirlenmiş olmakla birlikte erişilebilirlik anlamında yetersizdir.

Belgelerin içerdiği bilgilere erişebilirlik çok mümkün değildir. Belgeler kapalı bir ortamda muhafaza edilirken ilgili kişilerin bu belgelerdeki bilgilere ulaşması için oraya gitmeleri ve standart bir dosya sınıflandırmasına sahip olmayan bu belgeler arasından uzun zaman alan bir arama yapması gerekmektedir.

Benzeri başka durumlarda söz konusudur. Bu kapsamda bilgi toplumuna geçiş süreci hız kazanarak bilgilerin elektronik ortama aktarılması suretiyle erişilebilirlik de sağlanmıştır. Bilgilerin elektronik ortama aktarılması yani bilginin ortam değiştirmesi sonucunda ise gizlilik ve bütünlük kavramlarının tekrar ele alınması gerekmiştir.

5070 sayılı Elektronik İmza Kanunu ile yazışmaların elektronik ortamda yapılmasında elektronik imza kullanılması gerekliliği belirtilmiştir.

5070 sayılı Elektronik İmza Kanunu'nda yer alan şekliyle elektronik imza; başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi tanımlar. Elektronik imza; bir bilginin üçüncü tarafların erişimine kapalı bir ortamda, bütünlüğü bozulmadan (bilgiyi ileten tarafın oluşturduğu orijinal haliyle) ve tarafların kimlikleri doğrulanarak iletildiğini elektronik veya benzeri araçlarla garanti eden harf, karakter veya sembollerden oluşur.

2003/48 sayılı Başbakanlık Genelgesi ile yürürlüğe giren e-Dönüşüm Türkiye Projesinin 4.1.1.' inci maddesinde Bilgi Güvenliği Yönetim Sisteminin (BGYS) tüm kurumlarda kurulmasının hedeflendiği belirtilmektedir.

05/08/2005 tarihli ve 25897 sayılı Resmi Gazete'de yayımlanan, 2005/20 sayılı Başbakanlık Genelgesi ile çıkarılan Birlikte Çalışabilirlik Esasları Rehberinde elektronik ortamda sunulan hizmetlerde başarı, güven ortamının sağlanmasına bağlı olduğu vurgulanmıştır. Bu da, güvenlikle ilgili politika ve düzenlemelerin geliştirilmesini gerektirir.

2006/38 sayılı Yüksek Planlama Kurulu Kararı'yla onaylanan ve 28/07/2006 tarihli ve 26242 sayılı Resmi Gazete'de yayımlanan Bilgi Toplumu Stratejisi Belgesinde stratejik öncelikler arasında yer alan bilgi güvenliğinin ülke genelinde ve kamu kurumlarında bilgi sistemleri ile elektronik iletişim ve ağ bağlantılarında güvenliğin sağlanması ve sürdürülmesi için gerekli organizasyonel düzenlemelerin gerçekleştirileceğinden bahsedilmektedir. Ayrıca, bilgi güvenliğinin sağlanması için yasal düzenlemelerin yapılacağı da vurgulanmaktadır.

Devlet Planlama Teşkilatı (DPT) tarafından hazırlanan "Bilgi Toplumu Stratejisi"nin 88. maddesini "Ulusal Bilgi Sistemleri Güvenlik Programı" oluşturmaktadır. Bu işin sorumluluğu ise TÜBİTAK-UEKAE'ye (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü) verilmiştir. Programın en önemli hedefi başta kamu idareleri olmak üzere ülkemizin bilgi sistem güvenliği ile ilgili bilgi ihtiyacını karşılamaktır. Diğer hedefi ise kamu bilgi sistemlerinin güvenliğinin sağlanması ile ilgili etkin önlemler alınmasında öncü olmaktır. Program 2007 Ocak itibarıyla

başlamış olup 2010 yılı sonunda bitecektir. Bu programın altında birçok proje yer alıyor. Bu projeleri şöyle sıralayabiliriz:

- Pilot olarak seçilen 4 kamu kurumuna ISO 27001'e uygun bilgi güvenliği yönetim sistemi oluşturma konusunda danışmanlık veriliyor.

- Program kapsamında TÜBİTAK-UEKAE bünyesinde kurulan Bilgisayar Olaylarına Müdahale Koordinasyon Merkezi hem bilgisayar olay müdahale ekibi kurma konusunda kamu kurumlarına danışmanlık veriyor hem de güvenlik olayları ile ilgili ulusal anlamda koordinasyon görevini yürütüyor.

- Kamu kurum ve kuruluşlarında çalışan bilgi sistem uzmanlarının bilgi sistem güvenliğinin değişik alanları ile ilgili bilgi eksikliğini gidermek amacıyla program kapsamında 13 farklı alanda eğitimler düzenleniyor. Linux/Unix Güvenliği, Microsoft Sistemler Güvenliği, Veritabanı Güvenliği, Web Uygulamaları Güvenliği, Kablosuz Ağ Güvenliği, Bilgi Güvenliği Yönetim Sistemi, İş Sürekliliği/Felaket Kurtarım verilen eğitimler arasında yer alıyor.

- Ülkemizde bilgi güvenliği alanında bilgi sahibi her türlü kurum veya kişinin katkıda bulunmasına imkan sağlandığı, bilgi güvenliği konularında oluşturulan birçok rehber doküman, makale, güncel açıklık bilgilerinin yer aldığı bilgi güvenliği kapısı www.bilgiguvenligi.gov.tr adresinde Mart 2008'de yayına başladı.

- Sistem güvenliğinin sağlanması ile ilgili detaylı rehber dokümanların hazırlandığı bilgi sistemleri güvenliği dokümantasyon projesi gerçekleştiriliyor.

Bilgi güvenliğinin önemi giderek artmasına ülke güvenliği açısından önem arz etmesine rağmen konu ile ilgili yeterli yasal düzenleme henüz yapılamamıştır. Kişisel verilerin korunmasına hala tasarı aşamasında olup kanunlaşmamıştır.

20 Temmuz 2008 tarihli Resmi Gazete'de yayınlanan Elektronik Haberleşme Güvenli Yönetmeliği sonucunda Telekomikasyon Kurumu tarafından yetkilendirme çerçevesinde elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme şebekesi sağlayan ve alt yapısını işleten sermaye şirketlerinin, bir yıllık süre içerisinde TS ISO/IEC 27001 veya ISO/IEC 27001 standardlarına uyumluluğu yükümlülük haline gelmiştir.

5651 sayılı “İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun” 23 Mayıs 2007 tarihinde 26530 sayılı Resmi Gazete’de yayımlanarak yürürlüğe girmiştir.

5651 Sayılı Kanunda belirtilen hususlar;

- Telekomünikasyon Kurumu tarafından hazırlanan 24.10.2007 tarihli “Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik”,
- Başbakanlık tarafından hazırlanan 01.11.2007 tarihli “İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik” ve
- Başbakanlık tarafından hazırlanan 30.11.2007 tarihli “İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik”

ile ayrıntılı olarak düzenlenmiştir. Söz konusu mevzuat düzenlemeleri içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usulleri düzenlemek amacını taşımaktadır. 5651 Sayılı kanun ve ilgili yönetmelikler çerçevesinde içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıları gibi tanımlamalar yapılmıştır. Daha ziyade özel sektör ve özellikle ticari amaçlı toplu kullanım sağlayıcılar olan internet kafelere yönelik düzenlemeler olduğu kanısı yaygın olmasına karşın, yapılan tanımlamalar ve sorumluluklar çerçevesinde kamu kurum ve kuruluşlarının da uymaları gereken önemli yükümlülükler bulunmaktadır. Bu yükümlülükler, idari işlemlerin yanında bilgi güvenliğini de ilgilendiren teknik hususlarda alınması gereken tedbirleri kapsamaktadır.

3.1 2008 KÜRESEL BİLGİ GÜVENLİĞİ ANKETİ

“2008 Küresel Bilgi Güvenliği Anketi” sonuçlarına göre; araştırmaya katılan şirketlerin sadece yarısı, bilgi güvenliğine dönük yatırımlara ağırlık verdiğini belirtmiştir. Ancak, Türkiye’den ankete katılanların yüzde 73’ü bu yönde yatırımlarını artırdığını ifade etmiştir. Güvenlik zaaflarının daha büyük tehditler

yaratabileceğine inanan Türk firmaları, yine de mevcut yapılan yatırımın yeterli olmadığı görüşünde birleşmiştir. Aynı zamanda, Türkiye’de “bütçe azlığı” nın önemli bir sorun olduğu da ortaya koyulmuştur.

Anketin ortaya koyduğu sonuçlardan biri de, Türk şirketlerinin çoğunlukla ‘bilgi güvenliği’ olgusunu salt ‘teknoloji’ sorunu olarak ele aldıkları yönünde. Genel amaçlı bilgi sistemlerinin kurulumunda bilgi güvenliği birimleri süreçlere büyük oranda dahil olurken, insan kaynakları sistemlerinin kurulumunda katılımın yarı yarıya azaldığı görülmektedir. Bu oran dünyada yüzde 69 iken, Türkiye’de yüzde 53 olarak gerçekleşmiştir. Bu verilerin, pek çok firmada insan kaynakları yazılım uygulamalarının bilgi güvenliği riskleri taşıdığına bir işaret olduğu ifade edilmiştir.

Araştırmanın dünya ve Türkiye bulgularında göze çarpan diğer bir konu da ‘risk yönetimi’nin bilgi güvenliği stratejilerinde kısıtlı bir rol oynaması. Anket katılımcılarının dünya çapında yüzde 28’i ve Türk yöneticilerin yüzde 31’i, bilgi güvenliği ve risk yönetimi’ sorumlularının bir araya gelmediğini vurguluyor.

Dünya genelinde iş sürekliliği planlaması’nı öncelikle bilgi teknolojileri yönetiminin sorumluluk alanı olarak değerlendirenlerin oranı yüzde 41 iken, Türkiye ortalaması yüzde 67 olarak ortaya çıkıyor. Yine genel risk yönetimi çerçevesinde ele alınmayan iş sürekliliği planlamasının başarısının bu nedenle sınırlı olduğu görülüyor. Ankete katılan şirketlerin çoğunluğunun kriz yönetimi için komuta odalarının hazır olmadığını ifade ederken, Türk şirketlerinin yalnızca yüzde 31’inin bu konuda hazırlıklı olduğu vurgulanıyor. İş sürekliliği planlarını sınanan firma sayısı, dünyada yüzde 26 iken, Türkiye’de yüzde 18 oranını aşamıyor.

Dünyaya bakıldığında ankete katılan şirketlerin yüzde 45’inin bilgi güvenliği çalışmalarını üçüncü partilere devretmeye başladıkları görülüyor. Oysa yine rapor gösteriyor ki, üçüncü parti firmalarıyla yapılan çalışmalarda yaşanan veri ve bilgi kaybı olayları artıyor. Tedarikçilerden söz konusu raporu talep eden şirketlerin dünya ortalamasının üçte biri civarında olduğu görülüyor.

4 SONUÇ

Bilgi güvenliğinin önemi gün geçtikçe artmakta ve bilgi güvenliği daha karmaşık bir hal almaktadır.

Kurumsal bilgi güvenliğinin sağlanmasında aşağıdaki hususlara da dikkat edilmesi önerilmektedir.

- Kurumsal bilgi güvenliğini sağlamanın dinamik bir süreç olduğu ve süreklilik arz ettiği,
- Kurumsal bilgi güvenliğinin sadece teknolojiyle sağlanır yaklaşımından uzaklaşarak insan-eğitim-teknoloji üçgeninde yeni bir yaklaşımla sağlanması gerektiği,
- Uluslararası standartlara uygun olarak yapılması ve uygulanması gerektiği,
- Standartlar yüksek seviyede bir güvenliği garanti etse de bazen standartlarında yetersiz kalabileceği,
- Kurumsal bilgi güvenliği seviyesinin güncel durumunun belirlenmesi amacıyla iç ve dış ortamlardan zaman zaman bağımsız uzman kuruluşlar tarafından denetlenmesi gerektiği,
- Kurumsal bilgi güvenliğinin yönetilmesinin zorunlu bir süreç olduğu ve her zaman iyileştirmelere ihtiyaç duyulduğu ve
- En zayıf halka kadar güvende olunacağı varsayımıyla hareket edilerek gerekli önlemlerin alınması gerektiği

bilinmeli ve uygulanmalıdır.

KAYNAKÇA

AKKURT D., Bilgi işlem sistemleri için bilgi güvenlik politikası, 2002.
<http://www.ak-kurt.com/kurumsalpolitikalar.html>

BİSHOP M., Computer Security-Art and Science, Adison –Wesley
Professionel, 2002.

CALDER A., Implementing Information Security based on
ISO27001/ISO17799-A management guide, Van Haren publishing, 2006.

ÇAĞLAYAN U., Bilgi güvenliği:dünyadaki eğilimler, Ulaknet Sistem
Yönetimi konferansı-Güvenlik, Ankara, 2003.

FINDIK O., AKSOY T., Bilgi güvenliğinin sağlanmasında kullanılan
yöntemler ve bunların etkin kullanımı, Akademik Bilişim 2003 konferansı, Çukurova
Üniversitesi, 2003.

HAYES B., Conducting a Security Audit: An Introductory Overview, 2003,
www.securityfocus.com.

HELLMAN G., From logs to logic,
<http://www.arcsight.com/articles/From%20Logs%20to%20Logic.pdf>.

KAPP J., How to conduct a security audit,
<http://www.techsupportalert.com/pdf/t04123.pdf>

KODAZ H., RSA Şifreleme algoritmasının uygulaması, Konya, 2003.

KÜÇÜKOĞLU Ş., Uygun Güvenlik Çözümüne Yolculuk,
<http://www.infosecurenet.com/macroscope/macroscope6.pdf>.

MUKUND B., ISO 17799 Papers: BS 7799,
<http://17799.denialinfo.com/biju.htm#top>.

ONUR A., Kurumsal Bilgi Güvenliği'ne Bakış,
http://www.bilgiyonetimi.org/cm/pages/mkl_gos.php?nt=474.

ÖZAVCI F., Bilgi güvenliği-Temel kavramlar, 2002, <http://seminer.linux.org.tr/seminer-notlari/bilgiguvenligi-temelkavramlar.ppt>.

ÖZGİT A., DAYIOĞLU B., Bilişim Güvenliğinde Yaşam Döngüsü ve Derinlik, http://www.ulakbim.gov.tr/dokumanlar/guvenlik/Attila_Ozgit.ppt.

SAĞIROĞLU Ş., ERSOY E. ve ALKAN M., Bilgi güvenliğinin kurumsal bazda uygulanması, Bildiriler Kitabı uluslararası katılımlı bilgi güvenliği ve kriptoloji konferansı, 2007.

SMİTH S., JAMİESON R., Determining key factorsin e-gövernment information system security, www.ism-journal.com, 2006.

TAKCI H., SOĞUKPINAR İ., Saldırı tespitinde en yakın k komşu uygulaması, NET-TR03. Türkiyede Internet Konferansları VIII, 2002.

Bilgi sistemlerinin güvenliğine ilişkin OECD rehber ilkeleri-Güvenlik kültürüne doğru, <http://www.oecd.org/dataoecd/42/59/32493366.PDF>.

TUĞLULAR T., Üniversitelerde Bilgi Güvenliği Politikaları http://www.ulakbim.gov.tr/dokumanlar/guvenlik/Tugkan_Tuglular.pdf

VURAL Y., SAĞIROĞLU Ş., Kurumsal bilgi güvenliği ve standartları üzerine bir inceleme, Gazi Üniv. Müh. Mim. Fak. Der. Cilt :23 No: 2, 2008.

VURAL Y., SAĞIROĞLU Ş., Kurumsal bilgi güvenliği: güncel gelişmeler, Bildiriler Kitabı uluslararası katılımlı bilgi güvenliği ve kriptoloji konferansı, 2007.

Bilgi Toplumu Strateji Belgesi 2006-2010, Devlet Planlama Teşkilatı Bilgi Toplumu Dairesi.

Bilişim Güvenliği, Sürüm 1.1, Pro-G Bilişim Güvenliği ve Araştırma Ltd., 2003.

Bilişim Teknolojilerinde Risk Yönetimi, TBD Kamu –BİB Kamu Bilişim Platformu VIII.

Bilişim Sistemleri Güvenliği El Kitabı, Türkiye Bilişim Derneği, Sürüm 1.0, Mayıs 2006.

e-Dönüşüm Türkiye Projesi Birlikte Çalışabilirlik Esasları Rehberi Sürüm 2.0, DPT Bilgi Toplumu Dairesi, 2008

TS ISO/IEC 27001, Mart 2006.

Devlet Arşiv Hizmetleri Hakkında Yönetmelik.

Elektronik İmza Kanunu.

İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun.

2008 Küresel Bilgi Güvenliği Anketi,
[http://www.ey.com/Global/assets.nsf/International/TSRS_Global_Information_Security_Survey_2008/\\$file/TSRS_Global_Information_Security_Survey_2008.pdf](http://www.ey.com/Global/assets.nsf/International/TSRS_Global_Information_Security_Survey_2008/$file/TSRS_Global_Information_Security_Survey_2008.pdf)

<http://www.bilgiguvenligi.org.tr>

<http://bilisimsurasi.org.tr/>

<http://www.bsi-turkey.com/BilgiGuvenligi/Genel-bakis/index.xalter>.

<http://www.kriptoloji.net/>

<http://bthukuku.bilgi.edu.tr/>

<http://www.tbd.org.tr/>

<http://www.uekae.tubitak.gov.tr/>