KURUMSAL BİLGİ GÜVENLİĞİ YÖNETİŞİMİ VE BİLGİ GÜVENLİĞİ İÇİN İNSAN FAKTÖRÜNÜN ÖNEMİ

Eray ÇEK

113691002

İSTANBUL BİLGİ ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS PROGRAMI

Danışman: Doç. Dr. Leyla KESER BERBER

2017

KURUMSAL BİLGİ GÜVENLİĞİ YÖNETİŞİMİ VE BİLGİ GÜVENLİĞİ İÇİN İNSAN FAKTÖRÜNÜN ÖNEMİ

ENTERPRISE INFORMATION SECURITY GOVERNANCE AND IMPORTANCE OF THE HUMAN FACTOR FOR INFORMATION SECURITY

Eray ÇEK
113691002

Doç. Dr. Leyla KESER BERBER : 
(Danışman, İstanbul Bilgi Ü. Hukuk F.)

Prof. Dr. Ahmet DENKER : 
(Jüri Üyesi, İstanbul Bilgi Ü. Hukuk F.)

Yrd. Doç. Dr. Mehmet Bedii KAYA : 
(Jüri Üyesi, Yıldırım Beyazıt Ü. Hukuk F.)

Tezin Onaylandığı Tarih : 04 Mayıs 2017

Toplam Sayfa Sayısı : 106

Anahtar Kelimeler (Türkçe)	Anahtar Kelimeler (İngilizce)
1) Bilgi güvenliği yönetişimi	1) Information Security Governance
2) ISO/IEC 27001	2) ISO/IEC 27001
3) Bilgi güvenliği farkındalığı	3) Information Security Awareness
4) Risk yönetimi	4) Risk Management
5) Bilgi güvenliği politikaları	5) Information Security Policies

ÖZET

Teknoloji artık kurumlar için destek unsurları olmaktan giderek çıkmakta ve iş süreçlerinin bir parçası haline gelmektedir. Bilgi teknolojilerinin öneminin artması, bilginin korunması ve bilgi güvenliğinin önemini artırmıştır. Son 5-10 yılda ülkemizde de siber güvenlik ile ilgili daha fazla çalışma yapılmış, gerek kamunun gerekse de özel sektörün yatırımları artmıştır.

Bilgi güvenliğinin öneminin artması bilgi güvenliğinin nasıl daha etkin bir biçimde yönetilmesi gerektiğini de daha fazla tartışılır hale getirmiştir. İyi ve etkin bir bilgi güvenliği için kurumsal yönetişimin bir parçası olarak bilgi güvenliği yönetişimi kavramı kurumların hayatına dâhil olmuştur.

Çalışmanın giriş bölümünün ardından; ikinci ve üçüncü bölümde bilgi, bilgi güvenliği ve yönetişim kavramları üzerinde duruldu. Dördüncü bölümde ISO/IEC 27001 standardı açıklanarak, bilgi güvenliği yönetim sistemini detaylandırıldı. Bilgi güvenliği özünde bir risk yönetim işidir. Asıl olan bilgi güvenliği risklerinin en aza indirilmesidir. Bu nedenle de iyi bir bilgi güvenliği yönetişimi; bilgi güvenliği risklerinin yönetilmesidir. Bu nedenle beşinci bölümü bilgi güvenliği risk yönetimine ayrıldı. Altıncı bölüm uyum konusunda çünkü bilgi güvenliği sadece kurumlara bırakılmayan, kamu tarafından yasa, yönetmelik ve tebliğlerle düzenlenen bir alan.

Yedinci bölümde; bilgi güvenliği yönetişiminin neden gerekli olduğu, uygulanma yöntemleri, doğru bilgi güvenliği yönetişimin unsurlarını açıklanmaya çalışıldı. Sekizinci bölümde ise bilgi güvenliği yönetişimi için en önemli konulardan biri olan çalışanların bilgi güvenliği farkındalığı konusu anlatıldı.

Sonuç bölümünde; kurumlarda bilgi güvenliği yönetişiminin daha etkin hale getirilmesi için uygun yöntem ortaya kondu.

ABSTRACT

Technology is now out of support for the institutions and becoming a part of the business processes. The increase in the importance of information technology has increased the importance of information security and protection of information. In the last 5 to 10 years, our country has also had more work on cyber security and the investments of the public sector as well as the private sector have increased.

The increase in the importance of information security has also made it more debatable how information security should be managed more effectively. As part of corporate governance for good and effective information security, the concept of information security governance has been incorporated into the life of institutions.

Following the entrance chapter of the study; the second and third chapters focused on the concepts of information, information security and governance. In the fourth chapter, ISO / IEC 27001 standard is explained, detailing the information security management system. Information security is essentially a risk management business. The main thing is to minimize the risk of information security. For this reason, a good information security governance is managing of information security risks. For this reason, the fifth chapter is devoted to information security risk management. The sixth chapter is about compatibility because information security is not only left to institutions, but is regulated by laws, regulations and communiqués. In the seventh chapter; was explained to why information security governance is necessary, how to implement it, and the elements of accurate information security governance. In the eighth chapter, was explained information security awareness of employees, one of the most important topics for information security governance.

In the conclusion chapter; An appropriate method for making information security governance more effective in institutions has been put forward.

İçindekiler

KISALTMALAR

bkz : Bakınız

BT : Bilişim Teknolojileri

a.g.e. : Adı geçen eser

BDDK : Bankacılık Düzenleme ve Denetleme Kurulu

OTP : One Time Password (*Bir kez kullanılabilir şifre*)

CISSP : Certified Information Systems Security Professional (*Sertifikalı Bilgi Güvenliği Sistemleri Uzmanı*)

COBIT : Control Objectives for Information and Related Technologies (*Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri*)

ISACA : Information Systems Audit and Control Association

SOME : Siber Olaylara Müdahale Ekibi

ISO/IEC : International Organization for Standardization/International Electrotechnical Commision

BM : Birleşmiş Milletler

DB : Dünya Bankası

IMF : Uluslararası Para Fonu

OECD : Ekonomik Kalkınma ve İşbirliği Örgütü

BGYS : Bilgi Güvenliği Yönetim Sistemi

CISO : Chief Information Security Officer (*Bilgi Güvenliğinden Sorumlu Başkan*)

CSO : Chief Security Officer (*Güvenlikten Sorumlu Başkan*)

CEO : Chief Executive Officer (*İcra Kurulu Başkanı*)

CIO : Chief Information Officer (*BT'den Sorumlu Başkan*)

CTO : Chief Technology Officer (Teknolojiden Sorumlu Başkan)

BS : British Standart (*İngiliz Standartı*)

ATM : Automatic Teller Machine (*Otomatik Vezne Makinası*)

PIN : Personal Identification Number (*Kişisel Kimlik Numarası*)

KPI : Key Peformans Indicator (*Anahtar Performans Göstergesi*)

IOS : IPhone Operating System (*Iphone İşletim Sistemi*)

KHK : Kanun Hükmünde Kararname

BTK	: Bilgi ve Teknolojileri Kurumu
SOME	: Siber Olaylara Müdahale Ekibi
USOM	: Ulusal Siber Olaylara Müdahale

KAYNAKÇA

(tarih yok). CISSP® - Certified Information Systems Security Professional: www.isc2.org/cissp/default.aspx adresinden alındı

Aktaş, F., & Soğukpınar, İ. (2010). Bilgi Güvenliğinde Uygun Risk Analizi ve Yönetimi. *TÜRKİYE BİLİŞİM VAKFI BİLGİSAYAR BİLİMLERİ ve MÜHENDİSLİĞİ DERGİSİ 3.1 (Basılı 3)*, 41.

Bankacılık Kanunu (5411 Sayılı Kanun). (2005).

Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ . (2007).

Bankaların Destek Hizmeti Almalarına İlişkin Yönetmelik (28106 Sayılı Yönetmelik). (2011).

Bayramoğlu, S. (2005). *Yönetişim Zihniyeti: Türkiye'de Üst Kurullar ve Siyasal İktidarın Dönüşümü.* İstanbul: 5.

Canberk, G., & Sağıroğlu, Ş. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. *Politeknik Dergisi*, 165-174.

Cantürk, S. (2013, Ocak-Mart). *Bilgi Teknolojileri Yönetişimi için Yeni bir adım: COBIT 5*. KPMG Gündem: https://home.kpmg.com/content/dam/kpmg/pdf/2016/06/tr-kpmg-gundem-13-cobit-5.pdf adresinden alındı

Ersoy, E. V. (2012). *ISO/IEC 27001 Bilgi Güvenliği Standardı Tanımlar ve Örnek Uygulamalar.* Ankara: ODTÜ Yayıncılık.

Esen, M. (2015, 08 06). *Sibergah.* https://www.sibergah.com/genel/bilgi-guvenligi-nedir-ve-nasil-siniflandirilir/ adresinden alındı

Eskiyörük, D. (2007, 08 17). *BGYS - RİSK YÖNETİM SÜRECİ KILAVUZU.* Tübitak UEKAE: https://www.bilgiguvenligi.gov.tr/dokuman-yukle/bgys/...risk.../download.html adresinden alındı

Florentine, S. (2016). *Why you need a CSO/CISO?* http://www.cio.com/article/3048074/careers-staffing/why-you-need-a-cso-ciso.html adresinden alındı

Güzelsarı, S. (2003). Neo-Liberal Politikalar ve Yönetişim Modeli. *Amme İdaresi Dergisi*, 18.

Institute, I. G. (tarih yok). *Information Security Governance, Guidance for Boards of Directors and Executive Management, 2nd Edition.* http://www.isaca.org/Knowledge-Center/Research/Documents/Information-Security-Govenance-for-Board-of-Directors-and-Executive-Management_res_Eng_0510.pdf adresinden alındı

ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Standardı. (2013).

ISO/IEC 31000 Kurumsal Risk Yönetimi Standardı. (tarih yok).

İşcan, Ö. F., & Kaygın, E. (2009). Kurumsal Yönetişim Sürecinin Gelişimi Üzerine Bir Araştırma. *Atatürk Üniversitesi Sosyal Bilimler Dergisi*, 4.

İşcan, Ö. F., & Naktiyok, A. (2005). *Dijital Çağ Örgütleri.* İstanbul: Beta Yayınları.

Karabacak, B. (2008, 03 25). *ISO/IEC 27001:2005 ve Bilgi Güvenliği Yönetişimi - Türkiye Analizi*. Tübitak UEKAE: https://www.bilgiguvenligi.gov.tr/bt-guv.-standartlari/iso-iec-27001-2005-ve-bilgi-guvenligi-yonetisimi-turkiye-analizi-2.html adresinden alındı

Karabacak, B., & Soğukpınar, İ. (2005). ISRAM: information security risk analysis method. *Computers & Security*, 147-159.

Kişisel Verilerin Korunması Kanunu (6698 Sayılı Kanun). (2016).

Korkmaz, D. (2011, 04 07). *COBIT 5.0 Geliyor*. www.innova.com.tr: http://www.innova.com.tr/haber-detay.asp?haber=50F1B496-4BF4-429C-A3F0-08E98CF37D50 adresinden alındı

Love, P., Reinhard, J., Schwab, A., & Spafford, G. (2010). *Global Technology Audit Guide(GTAG) 15, Information Security Governance.* IPPF.

Marcinkowski, S., & Stanton, J. (2003). Motivational aspects of information security policies. *IEEE International Conference*, (s. 2528).

Özavcı, F. (tarih yok). *Bilgi Güvenliği Temel Kavramlar*. http://viproy.com/files/bgtk.pdf adresinden alındı

Sobacı, M. (2007). Yönetişim kavramı ve Türkiye'de uygulanabilirliği üzerine değerlendirmeler. *Yönetim Bilimleri*, 2.

Türk Dil Kurumu Resmi Web Sayfası. (tarih yok). www.tdk.org.tr. adresinden alındı

Uçar, A. (2015). *Bankacılık Sektöründe Bilişim Suçları.* lulu.com.

Vorster, A., & Labuschagne, L. (2005). A framework for comparing different information security risk analysis methodologies. *South African Institute for Computer Scientists and Information Technologists*, 95-103.

Wikipedia. (tarih yok). *Chief Security Officer*. https://en.wikipedia.org/wiki/Chief_security_officer adresinden alındı

Yönetişim Zihniyeti: Türkiye'de Üst Kurullar ve Siyasal İktidarın Dönüşümü. (tarih yok).

ŞEKİLLER TABLOSU

§ 1. GİRİŞ

Dünya, 20. yy'ın ortalarında bilgisayarların icat edilmesinin ardından hızlı bir biçimde yeni bir çağa adım attı. 20.yy için Uzay Çağı yaklaşımı varken, artık 21. yy ile birlikte bu kavram yerini kimilerine göre Bilgi Çağı kimilerine göre Bilgi ve Teknoloji Çağı'na, yani Bilişim Çağı'na bırakacaktı.

Dünyanın Bilgi ve Teknoloji çağına dönüşmesinde hiç kuşku yok ki 90'lı yıllarda hızlı bir biçimde hayatımıza giren internet teknolojisinin önemi büyük. Kişisel bilgisayarların ve internetin yaygınlaşması, sonrasında kişisel bilgisayarların yerini mobil olan dizüstü bilgisayarlar, tabletler ve nihai olarak da akıllı telefonlara bırakmasıyla birlikte; bilgiye erişim ve bilginin önemi de büyük ölçüde artmış oldu.

Bu gelişmelere en iyi örneklerden biri olarak ise artık insanlık tarihi boyunca üretilen bilginin bugün 1,5-2 yıl gibi bir sürede üretilebilir hale gelmesi. Kuşkusuz bu sürenin daha da azalacağı öngörülebilir.

Bilginin büyük önem kazanmasıyla beraber bilgi temelli bir ekonomi modeli de ortaya çıktı ve kurumlar için bilginin güvenliğinin sağlanması hayati konulardan biri haline geldi. Bu durum kuşkusuz sadece kurumlar için değil bireyler ve devletler için de giderek daha fazla önem kazanmakta. Siber güvenlik bugün devletlerin arasındaki çekişmelerde en hassas konulardan biri durumuna gelmiştir. Siber savaşların klasik savaşların bir parçası kimi zaman ise alternatifi olması durumuyla karşı karşıyayız.

Kurumlar için de artık bilgi güvenliği geçmişte olduğundan çok daha fazla önemli hale geldi. Bilgi güvenliği, bilgi teknolojilerin de üstünde bir alan kuşkusuz fakat bilginin bugün önemli bir bölümünün bilgi sistemleri üzerinde üretiliyor, işleniyor ve saklanıyor olmasından dolayı bilgi güvenliği ile bilişim sistemlerinin güvenliği iç içe geçmiş durumda. Bu nedenle de siber güvenlik için alınan önlemler bilgi güvenliğinin bir parçası.

Çalışmamızda yukarıda bahsettiğim etkenlerden dolayı siber güvenlik konusunun da üstünde bilgi güvenliği başlığı altında, kurumlar için bu konunun etkin bir şekilde yönetilmesi için gerekli unsurları ortaya koymaya çalışacağız. Bunun için de öncelikle bilgi ve bilgi güvenliği kavramları, bilgi güvenliğinin genel prensipleri, kurumsal yönetişim ve BT yönetişimi gibi kavramları açıklayacağız. Çalışmanın devamında bilgi güvenliği yönetimi için bir model olarak ortaya konan ISO/IEC 27001 Bilgi Güvenliği Yönetim Standardı ve bu

standarda ait kontroller, bilgi güvenliğinin temelini oluşturan bilgi güvenliği risk yönetimi üzerinde duracağız.

Bilgi güvenliği yönetişimi için en önemli konulardan biri de uyum ve standartlar. Çalışmamızda özellikle Bankacılık sektöründe yer alan düzenlemelere, bunların kurumların bilgi güvenliği yönetimleri açısından etkilerine değinmeye çalışacağız. Yine bu bölümde Elektronik Haberleşme Kanunu'nun kurumlara bilgi güvenliği yönetişimi açısından neler getirdiğine, özellikle 60.madde ile BTK'ya verilen yetkileri tartışacağız. Bunun yanı sıra, kurumların tam manada bilgi güvenliğinin sağlanması için çok kritik bir öneme sahip olan ulusal güvenlik yazılımlarının önemine siber güvenlik bakış açısıyla değineceğiz.

Çalışmanın devamında bilgi güvenliği yönetişimi ile ilgili ortaya konmuş genel yaklaşımları aktarıp, bunların özellikle kurumların organizasyonlarına etkilerini, bilgi güvenliği yönetişimi için uygun organizasyon modellerini tartışacağız. Bilgi güvenliği yönetişiminin üç önemli noktası olan teknoloji, süreç ve insan faktörlerine değineceğiz fakat odaklandığımız nokta insan faktörünün kurumların bilgi güvenliği açısından önemi olacak ve bilgi güvenliği farkındalığı konusunu ayrı bir bölüm olarak ele alacağız.

Sonuç bölümünde ise etkin bir bilgi güvenliği yönetişimi oluşturabilmek için en önemli unsurun insan faktörü olduğunu ortaya koyarak, kurumların çalışanların bilgi güvenliği yönetişimine nasıl daha etkin bir şekilde katılabileceğini ilişkin bazı çıkarımlarımız olacak. Yukarıda da değindiğimiz üzere bilgi güvenliği; teknoloji, süreç ve insan faktörlerinin ancak beraber değerlendirilebilerek başarıya ulaşılabileceği bir kavram ancak kurumların en çok zorlandıkları ve en fazla zafiyete uğradıklarını düşündüğümüz insan faktörünün, diğer iki faktörden bir adım öne çıktığını öne süreceğiz.

Siber güvenlik, bilgi güvenliği olay yönetimi gibi konuları çalışmanın kapsamında yer almadı fakat buna rağmen gerekli görülen yerlerde bu konulardan da bilgi güvenliği yönetişimi açısından önemli oldukları için bahsedildi. Çalışma kurumlar için etkin bir bilgi güvenliği yönetişimi sunmayı amaçladığından dolayı çalışmanın kapsamına Bilişim sektöründe ürün geliştiricilerin ürettikleri güvenlik ürünlerinin etkinliğini ölçmeyi sağlayan ISO 15408 Ortak Kriterler Standardına yer vermedik.

§ 2. BÖLÜM

BİLGİ GÜVENLİĞİ

I. BİLGİ NEDİR?

Bilgi; insan aklının alabileceği gerçek, olgu ve ilkelerin tümüne verilen ad[1] olarak tanımlanmakta. Bunun yanı sıra bilgiyi; bir konu ya da iş konusunda öğrenilen ya da öğretilen şeyler[2] olarak da tanımlayabiliriz. Bilgi her yerde mevcut ancak bilginin günümüzde yaygın olarak yer aldığı ortam bilişim sistemlerinde yer aldığını söyleyebiliriz. Bilişim sistemleri bilginin; işlendiği, depolandığı, iletildiği, değiştirildiği, silindiği veya anonim hale getirildiği en önemli yer.

Bilgi'den söz etmişken bilgiyi oluşturan ve dijital bir kavram olan veri kavramından da bahsedilmesi gerekir. Çünkü bilgi; verinin işlenmiş halidir. Veri, bilgiden farklı olarak anlamlı olması gerekmeyen bir olgudur ve veriler bir araya gelerek bilgiyi oluşturmaktadır.

Verinin; İngilizce karşılığı olarak kullanılan "data", Latince "datum" kelimesinden (çoğul şekli "data" ve "vermeye cesaret etmek" fiilinin geçmiş zamanı, dolayısıyla "verilen şey") gelmektedir. Latince "data" (dedomena) kavramının M.Ö. 300 yıllarında Öklid'in bir çalışmasında geçtiği bildirilmektedir (17). Dilimizde de "verilen şey" anlamında, "veri" olarak kullanılmaktadır. Bilişim teknolojisi açısından veri, bir durum hakkında, birbiriyle bağlantısı henüz kurulmamış bilinenler veya kısaca, sayısal ortamlarda bulunan ve taşınan sinyaller ve/veya bit dizeleri olarak tanımlanabilir.[3]

II. BİLGİ GÜVENLİĞİ NEDİR?

Bir varlık türü olarak bilginin izinsiz veya yetkisiz bir biçimde erişim, kullanım, değiştirilme, ifşa edilme, ortadan kaldırılma, el değiştirme ve hasar verilmesini önlemek olarak tanımlanır ve "gizlilik", "bütünlük" ve "erişilebilirlik" olarak isimlendirilen üç temel unsurdan

[1] www.tdk.org.tr
[2] www.tdk.org.tr
[3] Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme Canberk, Gürol-Şeref Sağıroğlu

meydana gelir. Bu üç temel güvenlik öğesinden herhangi biri zarar görürse **güvenlik zafiyeti** oluşur.[4]

Bilgi karşımıza çok çeşitli ve farklı yerlerde ortaya çıkmaktadır. Bilginin yer aldığı ortamlara örnek vermemiz gerekirse; sunucular, kişisel ve dizüstü bilgisayarlar, tabletler, akıllı telefonlar, veri tabanı gibi elektronik ortamlar, elektronik posta, taşınabilir diskler, CD/DVD ROM'lar, kâğıt vb. olarak sayılabilir.

Bilginin üç hali olduğunu burada ifade etmemiz gerekir. Bunlar;

- Durağan bilgi
- Hareket halindeki bilgi
- Kullanımdaki bilgi

III. BİLGİ GÜVENLİĞİ PRENSİPLERİ

A- GİZLİLİK

Gizlilik kavramı; bilginin sadece yetkisi olan kişiler tarafından erişmesi, yetkisiz kişilerin eline geçmemesi ve yetkisiz kişiler tarafından görülememesidir. Bilgiyi bir veri tabanında sakladığımızda veya bir yere göndermek istediğimizde bu bilginin sadece istediğimiz kişi veya grup tarafından görülmesi istenir. Gizliliği sağlamada kullanılan en önemli teknoloji olarak ise şifreleme teknolojisini söyleyebiliriz.

B- BÜTÜNLÜK

Bütünlük; bilginin yetkisiz kişiler tarafından değiştirilememesi, tam ve eksiksiz olmasıdır. Bilginin yine saklandığı veri tabanında veya iletim halindeyken yetkisi olmayan herhangi bir kişi tarafından değiştirilmesini, tahrip edilmesini veya silinmesi istenmez. Bütünlüğün korunmasında kullanılan teknolojiler arasında elektronik imza, açık anahtar altyapısı gibi kavramlar sayılabilir.

[4] https://www.sibergah.com/genel/bilgi-guvenligi-nedir-ve-nasil-siniflandirilir/

C- ERİŞİLEBİLİRLİK

Bilginin yetkisi olan kişiler tarafından, gerektiği zaman ulaşılabilir olması bilgi güvenliğinin erişilebilirlik prensibidir.

Bilgi güvenliğinin yukarıda bahsettiğimiz üç temel prensibi dışında başka bir takım prensipleri de vardır. Ancak belirttiğimiz gibi bilgi güvenliğini esas oluşturan üç temel prensip; gizlilik, bütünlük ve erişilebilirliktir. Aşağıda üç temel prensip dışında yer alan diğer prensiplerden bahsedeceğiz.

D- LOGLAMA

İngilizce Accountability kavramının karşılığı olarak dilimize hesap verilebilirlik olarak çevirebileceğimiz, log kayıtlarının bütünlüğünden bahsedilmesi gerekir. Log tutma, elektronik ortamda yapılan işlemlere ait kayıtların tutulmasıdır. Log kayıtlarının tutarlılığı inkâr edilemezlik, hesap verilebilirlik prensibinin sağlıklı olarak sürdürülmesi için çok önemlidir. Log kayıtlarının tutulması meydana gelecek bilgi güvenli ihlallerinin tespit edilmesinde, önlenmesinde, yasal soruşturmalarda karşımıza çıkan bir prensiptir.

E- KİMLİK DOĞRULAMA

Bilgi güvenliği prensiplerinden bir başkası da İngilizcesi Authentication olan ve kimlik doğrulama kavramıdır. Bilgi sistemlerinden hizmet alan kişinin, uygulamanın ya da bir web servisinin gerçekten o kişi, uygulama ya da web servisi olduğunun tespiti gerekmektedir. Kimlik doğrulama olmaksızın bir bilgi güvenliği düşünmek olanaksızdır. Şifre, OTP, biyometrik kimrik doğrulama gibi çeşitli kimlik doğrulama yöntemleri bulunmaktadır.

F- İNKÂR EDİLEMEZLİK

İnkâr edilemezlik de bir başka prensiptir. İnkâr edilemezlik prensibinin log kayıtlarının tutulması prensibiyle de birlikte değerlendirmek mümkündür. İnkâr edilemezliğin sağlanması için bütünlüğü korunmuş, tutarlı bir log kayıtlarının tutulması mekanizması gerekmektedir.

G- GÜVENİLİRLİK

Güvenilirlik bahsedeceğimiz son prensiptir. Bilişim sisteminden beklenen sonucun üretilmesi ve elde edilen sonuçlar ile beklenen sonuçların tutarlılık durumudur. [5]

IV. BİLGİ GÜVENLİĞİ DOMAİNLERİ

ISC^2 bilgi güvenliği alanında faaliyet gösteren ve tüm dünyada kabul gören, sertifikaları dünyanın en gözde güvenlik sertifikalarının başında gelen bir kuruluş. ISC^2 'nin CISSP (Certified Information Systems Security Professional) sertifikasına göre bilgi güvenliği aşağıda belirtilen 8 domaine ayrılmıştır. [6]

Aşağıda kısaca değineceğimiz bu domainler bilgi güvenliğinin sağlanmasında hangi başlıkların önemli olduğunu ve gruplandırılması açısından önemli bir örnektir.

A- GÜVENLİK VE RİSK YÖNETİMİ

Bu domainde; bilgi güvenliğinin genel kavramları, iş etki analizi, bilgi güvenliği farkındalığı, risk yönetimi, iş sürekliliği, uyum ve düzenlemeler gibi kavramlar bu domainin parçasıdır. Bilgi güvenliğinin yönetişim kısmı CISSP için tam da bu domaindir. Bilgi güvenliği yönetişimi genel prensiplerine daha çok bu domainde bahsedilir.

[5] Marcinkowski, S.J., Stanton, J.M. 2003. Motivational aspects of information security policies. Systems, Man and Cybernetics, IEEE International Conference on, 3: 2528s.
[6] https://www.isc2.org/cissp/default.aspx

B- VARLIK GÜVENLİĞİ

Bilgi güvenliğinin en önemli konularından biri bilginin sınıflandırılması ve etiketlenmesi konusudur. Bu domainde varlıkların ve yine bir varlık türü olan bilginin toplanması, saklanması, sınıflandırılması, etiketlenmesi işlemlerinden yola çıkılarak bir bilgi yaşam döngüsünü tanımlar.

C- GÜVENLİK MÜHENDİSLİĞİ

Bilgi güvenliğinin sağlanmasında teknik konulara daha çok yer verilen bir domaindir. Kriptoloji, güvenlik mimarisi ve tasarımı, fiziksel güvenlik gibi konular bu domain altında incelenmektedir.

D- İLETİŞİM VE AĞ GÜVENLİĞİ

Bilgi güvenliği kuşkusuz en önemli konularının başında ağ güvenliği gelmektedir. Bilginin üç halinden bahsetmiştik. Bunlardan biri "hareket halindeki bilgi" kavramıydı. Hareket halindeki veri de iletişim ve ağ güvenliğinin konusudur. Bu domainde ağ güvenliği için yapılması gereken genel prensiplere ve kontrollere yer verilmektedir.

E- KİMLİK VE ERİŞİM YÖNETİMİ

CISSP'ye göre en kritik ve en geniş incelenen konulardan biri tıpkı iletişim ve ağ güvenliği gibi kimlik ve erişim yönetimidir. Bilgi güvenliği ihlallerine en sık rastlanan konu erişim yönetimiyle ilgilidir. Bilgi güvenliğinin gizlilik başta olmak üzere üç temel prensibinin sağlanması için de kimlik doğrulama ve yetkilendirme konusu olmazsa olmaz bir konudur. Bu domainde kimlik ve erişim yönetimi detaylı olarak incelenmektedir.

F- GÜVENLİK DEĞERLENDİRME VE TESTİ

Bilgi güvenliği ihlallerinin artması ve siber saldırıları günümüzde bilgi güvenliği olay yönetimi başlığının önemini artırmıştır. Bu domain içerisinde; zafiyet tarama, sızma testi, log ve ihlal yönetimi, kod ve log gözden geçirme konuları işlenmektedir. Ülkemizde de bilgi güvenliği olay yönetimi yasal olarak düzenlenmektedir. Bu konuya örnek olarak verebileceğimiz, BDDK'nın bir düzenlemesi olan ve tüm bankaların bünyelerinde oluşturmalarını bekledikleri SOME (Siber Olaylara Müdahale Ekibi) ekipleri bulunmaktadır.

G- GÜVENLİK OPERASYONLARI

Güvenliğin bir de operasyonel boyutu vardır. *Disastery Recovery*, yedekleme gibi konuları da içeren bir domaindir.

H- YAZILIM GELİŞTİRME GÜVENLİĞİ

Bilgi güvenliğinin en hassas konularından biri olan yazılım güvenliği bu domainle incelenmiştir. Güvenlik zafiyetlerinin ve bunun bağlantılı olarak da bilgi güvenliği ihlallerinin önemli bölümü yazılım geliştirme süreçlerinde yaşanan eksiklerden kaynaklandığı için artık günümüzde yazılım geliştirme güvenliği ayrı bir domain olarak ele alınma noktasına gelmiştir.

§ 3. BÖLÜM

YÖNETİŞİM

I. YÖNETİŞİM NEDİR?

Türkçe'ye "yönetişim" olarak çevireceğimiz Governance kavramı yeni bir yönetim modelidir. İngilizce "government" kelimesinin karşılığı olan yönetim ile "governance" kelimesinin dilimizdeki karşılığı olan yönetişim kavramları birçok yerde birbirine karıştırılmakta ve iç içe geçmektedir. Fakat bu iki kavramın karıştırılması hem dilimize çevrilirken kullanılan yönetim ve yönetişim kelimelerinin benzerliği hem de gerçek de ihtiva ettikleri anlamların birbirine yakın olmasıdır. Yönetim(Government) kavramı hükümet etme, idare etme bağlamında kullanılmakta, hiyerarşik nitelikte bir yönetim modelini öne çıkarmaktadır. Yönetişim(Governance) kavramı ise yönetim sürecinde rol oynayan aktörler ve örgütler arasında etkileşimini ve yönetim faaliyetlerine katılmasını ifade etmek üzere kullanılmaktadır.

Yönetişim kavramını anlamak için yönetim kavramından da bahsetmek gerekecektir. Bu noktada COBIT 5'in yönetim ve yönetişim arasındaki farkına da değinmeye çalışacağız.

"*Yönetişim kavramı özellikle 1990'lı yıllardan sonra kamu yönetimi literatürüne girmiş ve uluslararası örgütler (BM, DB, IMF, OECD) tarafından yayımlanan raporlarda sıkça kullanımından sonra akademik araştırma ve tartışmaların odak noktalarından biri olmuştur. Ancak, yönetişim kavramı üzerine yapılan söz konusu yoğun çalışmalara rağmen, kavramın herkes tarafından üzerine uzlaşı sağlanmış tek bir tanımı söz konusu değildir."*[7]

"Yönetişim kavramının tek bir tanımının olmamasının nedeni, yönetişim kavramının hukuktan siyasete, kamu yönetiminden işletmeye ve uluslar arası ilişkilere kadar bir çok disiplinle ilgili olması ve yerel, ulusal ve global mekânsal ölçeklerde uygulama alanı bulmasıdır."[8]

[7] Mehmet Zahid Sobacı, Yönetişim kavramı ve Türkiye'de uygulanabilirliği üzerine değerlendirmeler (Yönetim Bilimleri Dergisi), s.2.
[8] Sonay Bayramoğlu, Yönetişim Zihniyeti: Türkiye'de Üst Kurullar ve Siyasal İktidarın Dönüşümü, (İstanbul: İletişim Yayınları, 2005), s. 35; Selime Güzelsarı, 'Neo-Liberal Politikalar ve Yönetişim Modeli', Amme İdaresi Dergisi, 36 (2), Haziran 2003, s. 18.

II. KURUMSAL YÖNETİŞİM

Değişen ve giderek zorlaşan rekabetçi ortamda kurumlar için çok çeşitli farklı sorunlar ortaya çıkmaktadır. Zorlaşan koşullar, kurumların büyümeleri sonucu ortaya çıkan hantallaşma da yönetim anlayışında bazı değişikliklerin olması gerekliliğini ortaya koymuştur. Geçmişte işletmeleri yöneten kişiler aynı zamanda işletmenin sahibi iken bu durum giderek profesyonel kadrolar tarafından işletmelerin yönetilmesi sürecine doğru gitmiştir.

Kurumsallaşma sürecini tamamlayan işletmeler için günümüzde klasik yönetim anlayışından giderek yönetişim anlayışına doğru bir geçiş söz konusudur. Kurumsal yönetişim, bir anlamda yönetim faaliyetlerinin bir ekip tarafından yerine getirilmesidir. Kurumsal yönetişim, örgütün vizyon, misyon, strateji, yapı, kültür ve liderlik biçimi gibi örgütsel beyne ve bedene ait unsurların kim tarafından belirleneceği ve düzenleneceği sorularına cevap arayan bir yönetim tekniği olarak görülebilir.[9]

A- KURUMSAL YÖNETİŞİMİN İLKELERİ

Kurumsal yönetişim anlayışı için şeffaflık (transparency), hesap verebilirlik (accountability), sorumluluk (responsibility) ve adaletlilik (fairness) tüm dünyada kurumsal yönetişim ilkeleri olarak kabul edilmiştir.[10]

1. Şeffaflık

Şeffaflık ilkesi *"Ticari sır niteliğinde olan bilgiler hariç olmak üzere, şirket ile ilgili bilgilerin zamanında, tam, doğru ve açık bir şekilde kamuya duyurulmasını ifade eder."*[11]

[9] Ömer Faruk İşcan, Atılhan Naktiyok, Dijital Çağ Örgütleri (İstanbul: Beta Yayınları, 2005)
[10] Ömer Faruk İşcan, Erdoğan Kayğın, Kurumsal Yönetişim Sürecinin Gelişimi Üzerine Bir Araştırma (Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 2009), s.4.
[11] a.g.e.

2. Hesap verebilirlik

Yönetim kurulu üyelerinin pay sahiplerine karşı hesap verme durumudur.[12]

3. Sorumluluk

Şirket yönetiminin şirket adına yapmış olduğu faaliyetlerin mevzuata, esas sözleşmeye, şirket içi düzenlemelere uygunluğunun ve bunun denetlenmesidir.[13]

4. Adaletlilik

Kurumsal yönetişimde adaletlilik kavramı; yönetimin tüm faaliyetlerinde ortaklarına, paydaşlarına ve tüm diğer menfaat sahiplerine karşı eşit ve adalet içinde davranması durumu olarak ifade edilir.

İşcan ve Kayğın'a göre bu ilkelerin amacı:

- *Menfaat sahiplerinin karşılıklı hak ve yükümlülüklerinin belirlenmesi,*
- *Şirket yönetiminde şeffaflığın sağlanması,*
- *Şirket yönetimine güvenin artırılması,*
- *Şirket performansını artırarak, istikrarlı büyüme ve yüksek karlılık sağlanmasıdır.*[14]

III. BİLGİ TEKNOLOJİLERİ YÖNETİŞİMİ

Bilgi teknolojilerinin günümüzde çok yaygın olarak kullanılmasıyla birlikte BT Yönetişimi de daha önemli hale gelmiştir. Geçmişte Bilişim Teknolojileri, kurumlar için sadece bir araç, destek unsuru olarak görülürken bu durum günümüzde BT'nin kurumların iş süreçlerinin ayrılmaz bir parçası haline gelmiştir. Bilişim teknolojilerinin çok önemli bir unsur haline

[12] a.g.e.
[13] a.g.e.
[14] a.g.e.

gelmesiyle birlikte BT'nin süreçleri, yönetim modelinin nasıl olması gerektiği gibi konular çok daha fazla konuşulmaya başlandı. BT Yönetişimi anlayışı da bu şekilde ortaya çıktı ve kurumlara BT'nin nasıl çok daha etkin olarak yönetilebileceğini gösterdi.

BT Yönetişiminin temel görevi iş hedefleriyle uyumlu bir şekilde BT faaliyetlerinin gerçekleştirilmesi, kurumun stratejileri ve vizyonu doğrultusunda konumlanmış, uyumlu hale gelmiş bir BT yapısının oluşturulmasıdır.

BT Yönetişimi kurumun hedef, vizyon ve stratejileriyle uyumlu BT faaliyetlerinin oluşturulmasında, sektörde işlerliği ve güvenilirliği kanıtlanmış en iyi yöntemlerin, tekniklerin uygulanmasını öngörür.

Günümüzde BT yönetişimi ile ilgili en kapsamlı çerçeve COBIT'dir. Özellikle COBIT 5.0 BT Yönetişimi için örnek bir model sunmaktadır. Burada COBIT'den bahsederek BT Yönetişim anlayışının genel hatlarını ortaya koymuş olacağız.

A- COBIT

COBIT, günümüzde Bilişim Teknolojileri Yönetişimi ile ilgili en kapsamlı metodu ortaya koyan en önemli çerçevedir. COBIT, ISACA tarafından yayınlanmıştır. ISACA; 1969 yılında kurulmuş olup, kar amacı gütmeyen bir organizasyondur. 180 ülkede 100.000'den fazla üyesi bulunan, iş ve BT liderlerinin bilgi ve teknolojiden sağladıkları faydayı artırmaları ve bunlara ilişkin riskleri yönetme konusunda destek sağlamak için oluşturulmuştur.

COBIT; Bilgi ve ilgili teknolojiler için kontrol hedefleri anlamına gelmektedir. 1996 yılında ISACA tarafından oluşturulmuştur. COBIT'in günümüzde en yeni sürümü 5.0 sürümüdür. COBIT'in ülkemizde ise yaygın olarak kullanılmasında önemli kilometre taşlarından birisi BDDK tarafından Bankacılık Bilgi Sistemlerini denetlemek için kullanmasıdır. Bankacılık Bilgi Sistemlerinin denetlenmesi için COBIT'in bir önceki sürümü olan COBIT 4.1 sürümü halen aktif olarak kullanılmaktadır.

COBIT, BT süreçlerini iş hedefleriyle uyumlu bir şekilde organize edilebilmesi için en iyi uygulama kontrollerini sunmaktadır. COBIT 4.1 sürümü dört ana kısımdan oluşmaktadır.

- Planlama ve Organizasyon
- Tedarik ve Uygulama

- Teslimat ve Destek
- İzleme ve Değerlendirme

COBIT 5'in önceki COBIT sürümüne göre en önemli farklı yönetişime çok daha fazla odaklanmış olmasıdır. Yeni sürüm, bu yaklaşım temel alınarak şekillendirilmiş. Bu yaklaşımın sunmakta olduğu model, etkili bir yönetişim yapısının kurulabilmesi için sormamız gereken sorulara ve bu soruların birbirleriyle olan etkileşimlerine dikkat çekiyor. Bu sorular ile ilgili servisin ne için, kim tarafından, nerede ve nasıl gerçekleştirildiği konularında detaylı bilgi sahibi oluna bilinmesi amaçlanmış. Bu yaklaşımın sunmuş olduğu model kapsamı içinde, yeni sürüm ile değişikliğe uğramış ve yeni oluşturulmuş olan "süreç modeli" ile "bilgi referans modeli" kullanılıyor.[15]

Haziran 2012'de yayımlanan COBIT 5'ten temel yenilik; yönetim ve yönetişim kavramlarının birbirinden ayrılarak farklı süreçler halinde ele alınmasıdır. Yeni süreç modelinde kurumsal yönetişim ve BT yönetişimini bütünleşik bir şekilde ele almayı sağlayan yeni bir süreç modeli ortaya konulmaktadır. Bu bağlamda COBIT 5 "yönetişim" ve "yönetim" terimlerine aşağıdaki şekilde bir bakış getiriyor.

Yönetişim, işletme hedeflerinin belirlenmesinde paydaşların ihtiyaçlarının, durumlarının ve tercih haklarının değerlendirilmesini sağlar; önceliklendirme ve karar üretme yoluyla yönlendirir; üzerinde anlaşılmış yön ve hedeflere uyum ve performansı izler. Yönetim, işletme hedeflerine ulaşmak için yönetişim tarafından saptanmış yön ile uyumlu olarak planlama, inşa etme, işleme ve izleme faaliyetlerini gerçekleştirir.[16]

COBIT 5 süreç referans modeli dördü yönetim, bir tanesi de yönetişim olmak üzere beş domain içermekte ve beş domainde toplam 37 süreç yer almaktadır.

Kurumsal BT Yönetişimi

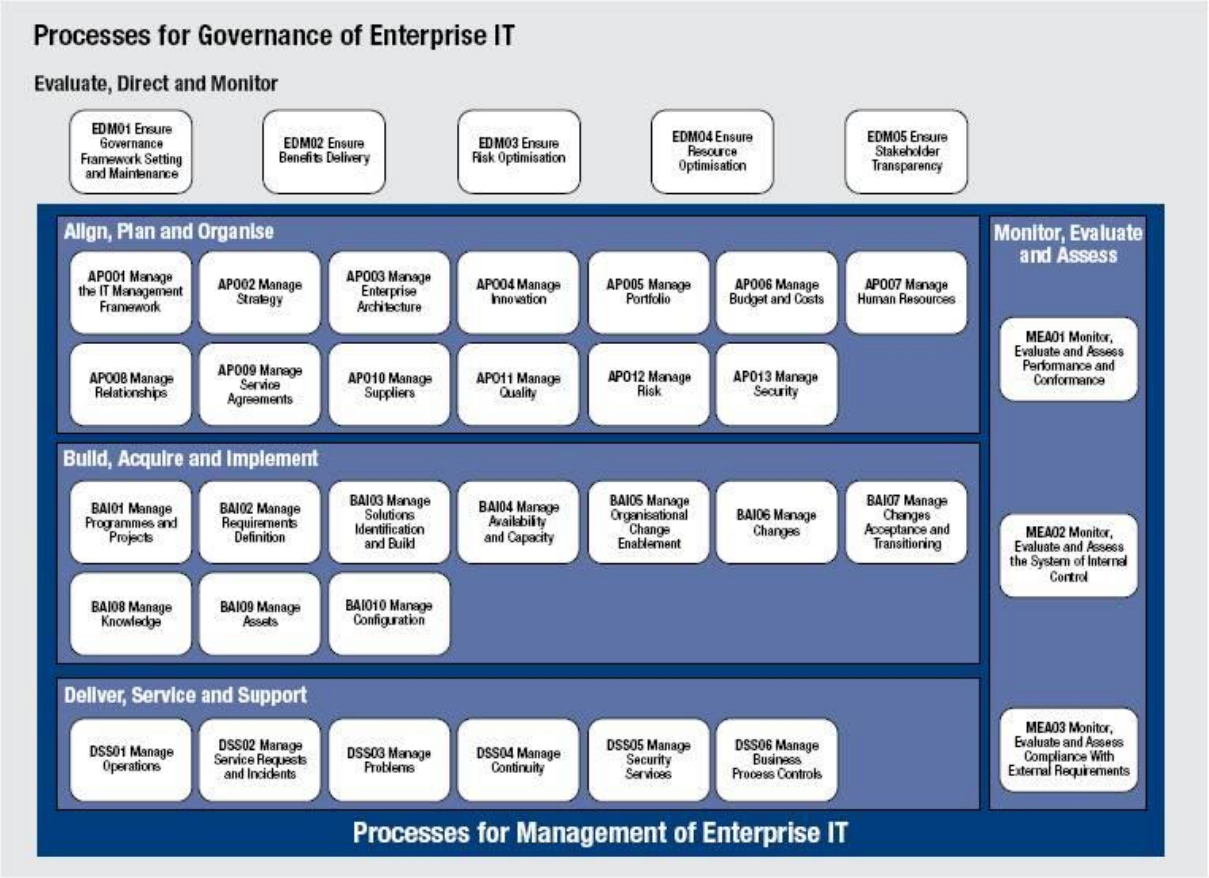
- Ölçme, Yönetme ve İzleme (Evaluate, Direct and Monitor -EDM) – 5 süreç

Kurumsal BT Yönetimi

- Align, Plan and Organise (APO) – 13 süreç
- Build, Acquire and Implement (BAI) – 10 süreç

[15] COBIT 5.0 Geliyor, http://www.innova.com.tr/haber-detay.asp?haber=50F1B496-4BF4-429C-A3F0-08E98CF37D50
[16] Bilgi Teknolojileri Yönetişimi için Yeni Bir Adım: COBIT 5, https://home.kpmg.com/content/dam/kpmg/pdf/2016/06/tr-kpmg-gundem-13-cobit-5.pdf

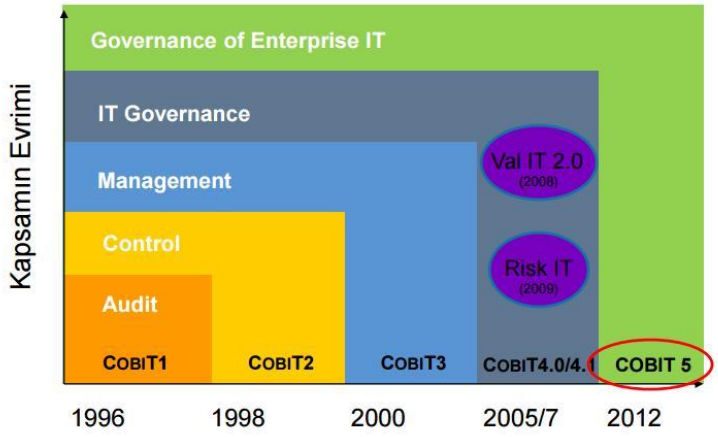
- Deliver, Service and Support (DSS) – 6 süreç
- Monitor, Evaluate and Assess (MEA) - 3 süreç



Şekil 1- Kurumsal BT Yönetişim Süreçleri[17]

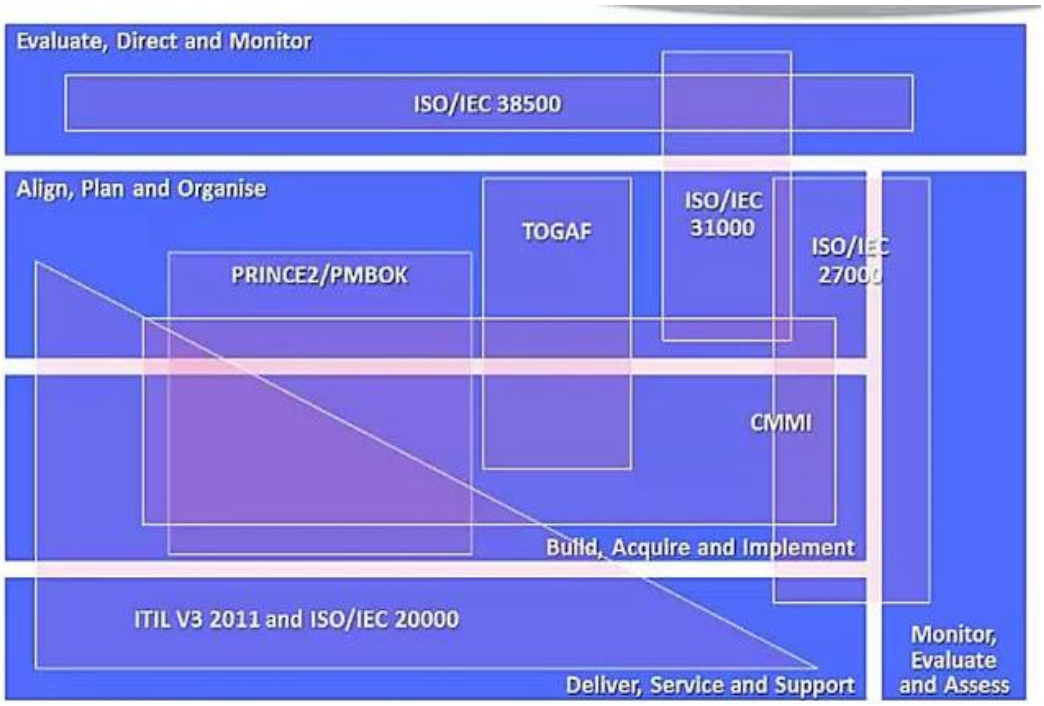
Aşağıda COBIT'in geçmişten bugüne kadar olan geçirdiği değişim yer almaktadır. COBIT 1996 yılında ortaya konulduğu dönemde bir denetim modeli sunarken bugün Kurumsal BT Yönetişimi olarak karşımıza çıkmaktadır.

[17] COBIT 5



Şekil 2- COBIT'in Evrimi

COBIT 5'in diğer standart ve çerçevelerle olan ilişkisini gösteren aşağıdaki şekil de bize COBIT 5'in tüm bu standart ve çerçeveleri tek bir çatı altında buluşturan bir yönetişim modeli olarak karşımıza çıkarıyor.



Şekil 3- COBIT 5 ile Diğer Standartların Ortak Noktaları

§ 4. BÖLÜM

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

I. BİLGİ GÜVENLİĞİ VE RİSK YÖNETİMİ İLİŞKİSİ

Kurumlarda bilgi güvenliğinin sağlanmasının en temel şartlarından biri güvenlik risk analizleridir. Güvenlik risk analizi; kurumun yaşayabileceği muhtemel güvenlik risklerini ortaya koyarak, kurumun önceliklerinin belirlenmesi ve tehditlerin ortaya konularak bu risklerin ortadan kaldırılması bilgi güvenliğinin sağlanması açısından oldukça kritiktir.

Güvenlik risk analizi ve risk yönetimi kavramlarını açıklamadan önce güvenlik risk analizi temelli bir bilgi güvenliği sistemi yönetim modeli kavramından ve ISO 27001 BGYS standardından bahsetmemiz gerekiyor.

II. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ NEDİR?

Bilgi Güvenliği Yönetim Sistemi; bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak üzere sistemli, kuralları konulmuş, planlı, yönetilebilir, sürdürülebilir, dokümante edilmiş, yönetimce kabul edilmiş ve desteklenmiş, uluslararası güvenlik standartlarının temel alındığı faaliyetler bütününe denmektedir. [18]

Kurumlarda bilgi güvenliğinin sağlanması sadece teknoloji ile mümkün değildir. Teknolojik çözümlerin yeterli olacağı algısı tamamen yanlış bir algıdır. Bilgi güvenliği; teknoloji, süreç ve insan faktörlerinin beraber değerlendirilmesi gereken ve bu üç faktöre göre oluşturulması gereken bir kavramdır. Bilgi güvenliği yönetim sistemi bu noktada teknoloji-süreç-insan faktörlerine göre oluşturulmuş bir sistemdir.

[18] Eren Veysel Ersoy, ISO/IEC 27001 Bilgi Güvenliği Standardı Tanımlar ve Örnek Uygulamalar (ODTÜ Yayıncılık, 2012, s.8)

BGYS, sadece BT bölümlerinin sorumluluğunda olan bir sistem değildir. BGYS; tüm kurum çalışanlarının katılımını gerektiren, yönetimin desteğinin alan ve oluşturulan güvenlik politikalarına tüm kurumun uyması gerektiren bir sistemdir.

A- BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİNİN FAYDALARI

Bir kurumda bilgi güvenliği yönetim sisteminin sağladığı çok sayıda ve kritik yarar vardır. Burada bunlardan bahsetmemiz gerekir.

- BGYS, kuruma yönelik bilgi güvenliği tehditlerinin ve risklerinin belirlenerek, etkin ve iyi bir risk yönetim anlayışının ortaya konmasını sağlar.
- Güvenlik standartlarına, düzenlemelere, yasa ve yönetmeliklere uyum sağlanması
- Kurumun itibarının korunması
- Rekabette kuruma güvenlik açısından geride kalmaması
- İş sürekliliğinin sağlanması
- Kurumu tehdit eden risklerin sürekli değerlendirilmesi
- Bilgi kaynaklarına yapılan erişimlerin kontrolü ve denetimi
- Bilgi güvenliliğinin temel prensipleri olan; gizlilik, bütünlük ve erişilebilirlik perspektifli bir modelin sağlanması
- Denetim izlerinin oluşturulması ve kontrol edilmesi, böylece hesap verilebilirlik ilkesinin sağlanması
- Bilgi sistemleri varlıklarının ve süreçlerin belirlenmesi
- Çalışanların, tedarikçilerin ve üst düzey yönetimin bilgi güvenliği konusunda farkındalık seviyesinin eğitimler ve farklı yöntemlerle artırılması
- Bilgi varlıklarının bütünlüğünün korunması

III. ISO/IEC 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

Bilgi Güvenliği Yönetim Standartlarının günümüzde en çok kabul edileni ise ISO/IEC tarafından yayınlanan 27000 ailesidir. ISO/IEC 27001 standardı bir İngiliz standardı olarak ortaya çıkmıştır. BS-7799, ISO/IEC 27001'in ilk halidir.

ISO/IEC 27001 standardının tarihsel gelişimine bakıldığında; 1993 yılında BSI(British Standarts Institution) tarafından başlatıldığını görüyoruz. İlk olarak BS 7799-1 olarak yine aynı yıl içerisinde yayınlandı. 1995 yılında ise bir İngiliz standardı olarak kabul edildiğini görüyoruz. 1998 yılında ise standardın ikinci sürümü olan BS 7799-2 yayınlandı. 2000 yılına gelindiğinde ise ISO (The International Organization for Standardization) ve IEC (The Electrotechnical Commission) kuruluşları ortak bir çalışma grubu oluşturdular ve BS 7799-1 standardını temel alarak ISO/IEC 17799 standardını geliştirdiler.

Bu standart içerisinde bilişim güvenliği ile ilgili olarak bazı kuralları ortaya koymuş ve 10 bölümde toplam 127 kontrol maddesi yer almıştır. Bu kontrol maddeleri kurumlarda bilgi güvenliğinin sağlanması için uygulanması gereken kuralların oluşturulmasını sağlamaktadır. ISO/IEC 17799 standardı 2005 yılından ise ISO/IEC 27001:2005 sürümü olarak yayınlanmıştır. Ülkemizde ise TSE tarafından çevirisi yapılarak TS ISO/IEC 27001:2005 olarak bir Türk standardı olarak kabul edilmiştir. 2013 yılında ise ISO/IEC 27001'in son sürümü yayınlanmış ve bu standart da TS ISO/IEC 27001:2013 olarak kabul edilmiştir.

ISO/IEC 27001 standardı özü itibariyle kurumlarda bilgi güvenliği yönetim sisteminin kurulması ve bu yönetim sisteminin oluşturulması için kontrol maddelerinin verilmesidir. Burada belirtilen kontrol maddeleri nasıl olması gerektiği sorusuna detaya girmeden yanıt vermektedir. Kurumlarda bunun nasıl sağlanacağıyla ilgili detayı ise vermemektedir. Bu kurumların kendi verecekleri kararlardır.

A- ISO/IEC 27001 STANDARDININ TEMEL ÖZELLİKLERİ

ISO/IEC 27001 standardının üç temel özelliği vardır. Aşağıda kısaca onlardan bahsedeceğiz.

1. Ölçülebilirlik

ISO/IEC 27001 standardı ölçülebilen, üçüncü taraflarla değerlendirilebilen bir standarttır. Bilgi güvenliği varlıklarının veya süreçlerinin değerlendirilmesine ve bunlarla ilgili risklerin ölçülebilmesini sağlamaktadır. Bu konuyu risk analizi kavramını detaylandırırken değerlendireceğiz.

2. Tekrarlanabilirlik

BGYS çok sayıda kontrol içermektedir ve bu kontrollere bağlı olarak istenildiği kadar tekrar edilebilme şansını sahiptir. İlerde bahsedeceğimiz PUKÖ (Planla-Uygula-Kontrol Et-Önlem Al) döngüsü sürekli tekrar edilebilir.

3. Ölçeklenebilme

BGYS, istenildiğinde kurumun belli bazı bölümü veya bölümleri için oluşturulabilir, daha sonra gerekirse farklı diğer bölümlere veya kurumun tamamına yansıtılabilir. Kapsam ile ilgili olarak istenildiği zaman değişikliğe gidilme şansı tanır. Ek denetimler ilave edilebilir veya azaltılabilir. Bu da ISO/IEC 27001'in ölçeklenebilir olma özelliğidir.

B- ISO/IEC 27001 PUKÖ YAKLAŞIMI

ISO/IEC 27001 standardının temel özelliklerinden bahsederken PUKÖ döngüsüyle ilgili kısa bir bilgi vermiştik. ISO/IEC 27001 standardı; kurumlarda bilgi güvenliği yönetim sisteminin kurulmasında kısaca PUKÖ döngüsü adı verilen; "Planla-Uygula-Kontrol Et-Önlem Al" yöntemini esas almaktadır.

1. Planla

BGYS'nin kurulması, kurumun ihtiyaçlarının ve hedeflerinin ortaya konması, kapsamının belirlenmesi süreci Planla adımında gerçekleştirilmektedir. Bunun yanı sıra bilgi güvenliği

politikalarının oluşturulması, ilgili süreçlerin ve prosedürlerin belirlenmesi burada gerçekleştirilir.

2. Uygula

Bilgi güvenliği yönetim sisteminin oluşturulması bu adımda gerçekleştirilir. Güvenlik politikalarının, süreçlerin ve prosedürlerin işletilmesi, denetimlerin gerçekleştirilmesi sağlanmaktadır.

3. Kontrol Et

Bilgi güvenliği yönetim sistemi oluşturulduktan sonra sürekli izlenmeli ve gözden geçirilmelidir. Güvenlik politikalarının ve bu politikalara göre alınan önlemlerin işlerliğinin tespit edilmesi, denetimler ve kontroller yoluyla eksiklerin ortaya çıkarılması gerekmektedir.

4. Önlem Al

Gözden geçirme çalışmaları, denetimler ve kontrollerde ortaya çıkan eksiklerin giderilmesi, bilgi güvenliği yönetim sisteminin sürekli geliştirilmesi, zayıflıkların giderilmesi bu adımda gerçekleştirilmektedir.

C- ISO/IEC 27001 BGYS ANA MADDELER VE KONTROLLER

ISO/IEC 27001:2013 sürümü 14 ana maddede 114 kontrol maddesi vermektedir. 2005 sürümünden farklı olarak ana madde sayısı 3 artırılmış, kontrol maddesi sayısı ise 16 adet azaltılmıştır. Biz burada ISO/IEC 27001:2013 sürümünde yer alan ana maddelere ve kontrollere değineceğiz.[19]

[19] ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Standardı

1. Bilgi Güvenliği Politikaları (Madde A.5)

Bilgi güvenliği politikaları ana maddesinin tek alt maddesi vardır ve iki adet kontrol içerir. Kurumda BGYS kapsamında bilgi güvenliği politikalarının oluşturulması ve yönetimin desteğinin sağlanması amaçlanmaktadır. Kurumda bilgi güvenliği politikaları tüm çalışanlara duyurulmalı, yönetimin desteği açıkça ifade edilmeli ve tüm çalışanlar bilgi güvenliği politikalarına uymalı ve farkındalık sağlanmalıdır.

a) Bilgi güvenliği için yönetim yönlendirmesi (Madde A.5.1)

Bu maddenin amacı; iş gereksinimleri, ilgili yasa ve düzenlemelere uygun bilgi güvenliği için yönetim yönlendirmesi ve desteği sağlamaktır. İki adet kontrol içerir.

aa) Bilgi güvenliği politikaları (Madde A.5.1.1)

Bilgi güvenliği ile ilgili politikalar oluşturulmalı, üst yönetim tarafından onaylanmalı, yayınlanmalı, tüm çalışanlar ve ilgili diğer taraflara duyurulmalıdır.

bb) Bilgi güvenliği için politikaların gözden geçirilmesi (Madde A.5.1.2)

Kurumun bilgi güvenliği politikaları, belirli aralıklarda veya gerektiği zamanlarda; ihtiyaçlar doğrultusunda etkinliğini sağlamak amacıyla gözden geçirilmelidir.

2. Bilgi Güvenliği Organizasyonu (Madde A.6)

Bilgi güvenliği organizasyonu ana maddesi iki alt ana madde ve yedi kontrol içermektedir. Bu maddenin temel amacı kurumda bilgi güvenliğini yönetecek bir grubun oluşturulmasıdır. ISO/IEC 27001 genelde burada bir forum, komite, komisyon benzeri yapının oluşturulmasını

önerir. Bu maddeden anlaşılması gereken sadece bilgi güvenliğini teknoloji ve süreç bakımından yönetecek bir bölümün olması anlaşılmamalıdır. Kuşkusuz BT güvenliğini yönetecek bir ekip olmalıdır fakat bu yeterli görülmez ve yönetimin desteğinde, bilgi güvenliği politikalarını hayata geçirecek bir komitenin varlığını işaret etmektedir. Bu konu tam da bilgi güvenliği yönetişimi kavramının kendisidir ve bilgi güvenliği yönetişimi kavramını incelerken bu kısmı detaylandıracağız.

a) İç organizasyon (Madde A.6.1)

Bu maddede amaç; kurumda bilgi güvenliğini yönetmek, başlatmak ve kontrol etmek amacına yönelik yönetim oluşturulması gerekmektedir. Beş tane kontrol içerir.

aa) Bilgi güvenliği rol ve sorumluluklar (Madde A.6.1.1)

Tüm bilgi güvenliği sorumlulukları tanımlanmalı ve atanmalıdır.

bb) Görevlerin ayrılması (Madde A.6.1.2)

Kurumun varlıklarının yetkisiz veya farkında olmadan zarar verme ihtimalini en aza indirmek için, görev ve sorumluluk alanları birbirinden ayrılmalıdır.

cc) Otoriterle iletişim (Madde A.6.1.3)

İlgili otoritelerle uygun iletişim kurulmalıdır.

çç) Özel ilgi gruplarıyla iletişim (Madde A.6.1.4)

Özel ilgi grupları veya diğer uzman güvenlik örgütleri ve profesyonel kurumlar, dernekler ile uygun bir iletişim sistemi geliştirilmelidir.

dd) Proje yönetiminde bilgi güvenliği (Madde A.6.1.5)

Bilgi güvenliğine; kurum içerisindeki her türlü projede, proje yönetimi içerisinde yer verilmelidir.

b) Mobil cihazlar ve uzaktan çalışma (Madde A.6.2)

Bu maddenin temel amacı uzaktan çalışma ve mobil cihaz kullanımındaki güvenliği sağlamaktır. İki adet kontrol maddesi içermektedir.

aa) Mobil cihaz politikası

Mobil cihazların kullanımın yaygınlaşmasıyla birlikte ISO/IEC'nun 2013 sürümünde eklenmiş bir kontrol maddesidir. Mobil cihazlardan kaynaklanabilecek bilgi güvenliği risklerinin en aza indirilmesi içi bir politika oluşturulması ve gerekli güvenlik önlemlerinin alınması gerekmektedir.

bb) Uzaktan çalışma

Çalışanların kurum ağına ve bilgiye; uzaktan erişmelerini güvenli bir biçimde sağlamak için uygun bir politika oluşturulmalı ve gerekli güvenlik önlemleri alınmalıdır.

3. İnsan Kaynakları Güvenliği (Madde A.7)

BGYS'nin sadece BT bölümlerinin sorumluluğu altında olmadığından tüm kurumun katılımıyla gerçekleştirilmesi gerektiğinden yukarıda bahsetmiştik. Bunun en iyi örneklerinden biri olan bu ana madde insan kaynakları güvenliğinin sağlanmasına yönelik oluşturulmuştur. Çalışanların bilgi güvenliği farkındalıklarının artırılmasından istihdam ve tarama faaliyetlerine kadar geniş bir yelpazede kontrol maddeleri sunulur. Üç alt madde ve altı kontrolden oluşmaktadır.

a) İstihdam öncesi (Madde A.7.1)

Çalışanların istihdam edilmesi öncesinde; bilgi güvenliği açısından uygun çalışanlar olup olmadıklarının tespit edilmesi ve düşünüldükleri göreve uygunluklarının anlaşılması için gerekli süreçler tasarlanmalıdır.

aa) Tarama (Madde A.7.1.1)

Tüm işe alım adayları, yükleniciler ve üçüncü taraf kullanıcılar için ilgili yasa, düzenleme ve etiğe göre ve iş gereksinimleri, erişilecek bilginin sınıflandırması ve alınan risklerle orantılı olarak geçmiş doğrulama kontrolleri gerçekleştirilmelidir.

bb) İstihdam koşulları (Madde A.7.1.2)

Çalışanlar, alt yükleniciler ve dış kaynak taraf kullanıcılar yapılan sözleşmeler gereğince kendilerinin ve kurumun bilgi güvenliği rol ve sorumluluklarını belirten kendi işe alım sözleşmelerini imzalamalıdırlar.

b) Çalışma esnasında (Madde A.7.2)

Kurum çalışanları ve diğer paydaşların(dış kaynak çalışanlar gibi) bilgi güvenliği sorumluluklarının bilincinde olmaları ve bunun gereğine uygun olarak davranmaları bu maddeyle amaçlanmaktadır.

aa) Yönetimin sorumlulukları (Madde A.7.2.1)

Yönetim; tüm çalışanlar ve dış kaynaklardan, kurumun politika ve prosedürlerine uygun bir biçimde bilgi güvenliği politikalarına uymalarını ve uygulamalarını istemesi gerekir. Bunun yanı sıra kendileri de sorumlulukları yerine getirmelidirler.

bb) Bilgi güvenliği farkındalığı, eğitimi ve öğretimi (Madde A.7.2.2)

Kurumdaki tüm çalışanlar ve dış kaynakları, kendi iş süreçleri ile ilgili olarak, kurumsal politika ve prosedürler hakkında bilgi güvenliği farkındalık eğitimi almalı ve bu eğitimler düzenli aralıklarla güncellenmelidir.

cc) Disiplin süreci (Madde A.7.2.3)

Bilgi güvenliği ihlal olaylarına karışan bir çalışanla ilgili bir disiplin süreci oluşturulmalıdır. Bu süreç resmi ve tüm çalışanlara bildirilmiş olmalıdır.

c) İstihdamın sonlandırılması ve değiştirilmesi (Madde A.7.3)

İstihdamın değiştirilmesi ve sonlandırılması sürecinde, kurumun çıkarlarını korumak amacına yönelik olarak gerekli süreçler oluşturulmalıdır.

aa) İstihdamın sonlandırma veya değiştirilme sorumlulukları (Madde A.7.3.1)

İstihdamın sonlandırılması veya değiştirilmesinden sonra geçerliliğini koruyan bilgi güvenliği sorumlulukları ve yükümlülükleri; tanımlanmış, çalışanlara ve yüklenicilere bildirilmiş ve uygulamaya zorlanmış olmalıdır.

4. Varlık Yönetimi (Madde A.8)

Üç alt madde ve on adet kontrolden oluşan bir ana maddedir. Kurumlarda bilgi güvenliğinin sağlanması için en önemli maddelerden biri kuruma ait bilgi güvenliği varlıkların belirlenmesi ve bunlara ait bir envanterin yönetimidir. Oldukça güç bir süreç olarak karşımıza çıkmaktadır. Burada bahsedilen bilgi güvenliği varlıkları arasında sunucular, veri tabanları, uygulamalar, kurumsal bilgisayarlar, akıllı cihazlar gibi çok sayıda bilgi varlığı sayılabilir.

a) Varlıkların sorumluluğu (Madde A.8.1)

Bu maddenin temel amacı; kurumsal bilgi varlıklarının belirlenmesi buna uygun olarak sorumlulukların tanımlanması şeklinde ifade edilebilir.

aa) Varlıkların envanteri (Madde A.8.1)

Bilgi ve bilgi işleme araçları ile ilişkili varlıklar tanımlanmalı ve bu varlıklara ait bir varlık envanter sistemi kurulmalı ve düzenli olarak güncellemelidir.

bb) Varlıkların sahipliği (Madde A.8.2)

Envanterdeki bilgi varlıkları sahiplenilmiş olmalıdır.

cc) Varlıkların kabul edilebilir kullanımı (Madde A.8.3)

Bilginin, bilgi ve bilgi işleme araçları ile ilişkilendirilmiş bilgi varlıklarının kabul edilebilir kullanım kuralları, tanımlanmış, dokümante edilmiş ve uygulanmış olmalıdır.

çç) Varlıkların iadesi (Madde A.8.4)

Tüm çalışanlar ve dış taraf kullanıcılar, istihdam, sözleşme veya anlaşmaları sona erdiğinde, kendi sahipliğinde olan kuruma ait tüm varlıkları iade etmelidir.

b) Bilgi sınıflandırması (Madde A.8.2)

Bu maddenin amacı; bilgiye, kuruluştaki önemi ile uygun bir koruma seviyesi sağlamaktır. Bilgi sınıflandırması, bilgi güvenliği yönetim sisteminin kurulmasında ve bilgi güvenliğinin sağlanmasında en temel ve önemli adımların başında gelmektedir.

aa) Bilginin sınıflandırılması (Madde A.8.2.1)

Bilgi; yetkisiz ifşa (açıklama) ve değiştirme söz konusu olduğunda, yasal gereksinimler, değer, kritiklik ve hassaslık kriterleri ile sınıflandırılmış olmalıdır.

bb) Bilginin etiketlenmesi (Madde A.8.2.2)

Kurumun bilgi sınıflandırma düzenine (yöntemine) uygun olarak, bilginin etiketlenmesi için prosedürler geliştirilmiş ve uygulanmış olmalıdır.

cc) Varlıkların işlenmesi (Madde A.8.2.3)

Kurumun bilgi sınıflandırma düzenine (yöntemine) uygun olarak, varlıkların işlenmesi için prosedürler geliştirilmiş ve uygulanmış olmalıdır.

c) Medya (Ortam) işleme (Madde A.8.3)

Bu maddenin amacı; ortamda (medyada) depolanmış bilginin; yetkisiz ifşasını, değiştirilmesini, kaldırılmasını veya yok edilmesini önlemektir.

aa) Taşınabilir ortam yönetimi (Madde A.8.3.1)

Kuruluşun bilgi sınıflandırma düzenine (yöntemine) uygun olarak, taşınabilir ortam yönetimi için prosedürler uygulanmış olmalıdır.

bb) Ortamın yok edilmesi (Madde A.8.3.2)

İhtiyaç ortadan kalktığında, kurumun resmi prosedürleri kullanılarak ortam güvenli bir şekilde yok edilmesi gerekmektedir.

cc) Fiziksel ortam transferi (Madde A.8.3.3)

Bilgi içeren ortamlar, taşıma sırasında, yetkisiz ve kötü kullanıma ve bozulmalara karşı korunmalıdır.

5. Erişim Kontrolü (Madde A.9)

Bilgi ve bilgi sistemlerine yapılan erişimlerin rol ve görev tanımlarına uygun olacak şekilde, güçlü ve güvenli kimlik doğrulama teknikleri kullanılarak yapılması ve erişimlerin kısıtlanması ile ilgili maddedir. Bilgi güvenliğinin en temel özelliklerinin başında erişim kontrolü gelmektedir. Dört alt madde ve 14 adet kontrol içermektedir.

a) Erişim kontrolü için iş gereksinimleri (Madde A.9.1)

Bilgi teknolojisine ait tüm süreçlerde; uygulamalara, sistemlere veri tabanları gibi tüm araçlarda uygun bir erişim kontrol sistemi uygulanmalıdır.

aa) Erişim kontrolü politikası (Madde A.9.1.1)

İş ve bilgi güvenliği ihtiyaçlarına uygun bir şekilde oluşturulmuş bir erişim kontrol politikası, dokümante edilmiş ve gözden geçirilmiş olmalıdır.

bb) Ağ ve ağ hizmetlerine erişim (Madde A.9.1.2)

Kullanıcıların yalnız, kullanım için açıkça yetkilendirilmiş oldukları, ağ ve ağ hizmetlerine erişimleri sağlanmış olmalıdır.

b) Kullanıcı erişim yönetimi (Madde A.9.2)

Bu maddede amaç; sistemlere ve hizmetlere, yetkili kullanıcı erişimini sağlamak ve yetkisiz erişimi önlemektir.

aa) Kullanıcı kaydetme ve kaydı silme (Madde A.9.2.1)

Rol ve görev tanımlarına uygun olarak; resmi ve tanımlanmış bir kullanıcı kaydetmeg ve silme süreci oluşturulmuş olmalıdır.

bb) Kullanıcı erişiminin sağlanması (Madde A.9.2.2)

Tüm kullanıcı tipleri için, tüm sistem ve hizmetlere erişim haklarının tahsisini ve geri alınmasını sağlamak üzere, resmi bir kullanıcı erişiminin sağlanması süreci uygulanmış olmalıdır.

cc) Ayrıcalıklı erişim haklarının yönetimi (Madde A.9.2.3)

Ayrıcalıklı erişim haklarının tahsisi ve kullanımı, sınırlandırılmış ve kontrol edilmiş olmalıdır.

çç) Kullanıcı gizli kimlik doğrulama bilgisinin yönetimi (Madde A.9.2.4)

Kimlik doğrulama bilgisi gizlidir ve bu bilgilerin kullanıcılara iletilmesiyle ilgili olarak resmi bir yönetim süreci oluşturulmalıdır.

dd) Kullanıcı erişim haklarının gözden geçirilmesi (Madde A.9.2.5)

Bilgi varlıklarının sahipleri tarfından; kullanıcıların bilgiye erişim haklarını belirli ve düzenli aralıklarla gözden geçirmelerini sağlayacak bir süreç oluşturulmalıdır.

ee) Erişim haklarının kaldırılması veya düzenlenmesi (Madde A.9.2.6)

Tüm çalışanlar ve dış kaynak çalışanlarının, bilgi ve bilgi işleme araçları üzerindeki erişim yetkileri; istihdamın, sözleşmenin veya anlaşmanın sona ermesiyle kaldırılmış, istihdamın, sözleşmenin veya anlaşmanın değiştirilmesi halinde ise düzenlenmiş olmalıdır.

c) Kullanıcı sorumlulukları (Madde A.9.3)

Kullanıcıları, kendi kimlik doğrulama bilgilerinin emniyeti için hesap verebilir kılmak amacıyla bu madde yazılmıştır.

aa) Gizli kimlik doğrulama bilgisinin kullanımı

Kullanıcılardan, kurumun gizli kimlik doğrulama bilgisinin kullanımı hakkındaki uygulamalarını, izlemeleri istenmiş olmalıdır.

d) Sistem ve uygulama erişim kontrolü (Madde A.9.4)

Sistemlere ve uygulamalara yetkisiz erişimi engellemek bu maddenin amacıdır.

aa) Bilgi erişim kısıtlaması (Madde A.9.4.1)

Bilgi, uygulama ve sistemlere erişim, tanımlanmış erişim kontrol politikasına uygun olarak sınırlandırılmalıdır.

bb) Güvenli oturum açma prosedürleri (Madde A.9.4.2)

Sistemlere, uygulamalara ve veri tabanlarına güvenli bir oturum açma sistemi oluşturulmalıdır. Bu sistem erişim kontrol politikasıyla belirlenmeli ve buna ait bir prosedür oluşturulmalıdır.

cc) Parola yönetim sistemi (Madde A.9.4.3)

Kurum endüstri standartlarına uygun bir parola yönetim sistemi geliştirmeli ve nitelikli parola kullanımı sağlanmalıdır.

çç) Yardımcı sistem programlarının kullanımı (Madde A.9.4.4)

Sistemin üzerinde değişiklik yapabilme yeteneği olabilecek yardımcı sistem programlarının kullanımı sınırlandırılmalı ve güçlü kontroller uygulanmalıdır.

dd) Program kaynak kodu kullanımına erişim (Madde A.9.4.5)

Program kaynak koduna erişim sınırlandırılmalıdır.

6. Kriptoloji (Madde A.10)

Kriptoloji, ISO 27001'in 2005 sürümünde ayrı bir ana madde olarak yer almamaktaydı fakat 2013 sürümünden ayrı bir ana madde haline getirildi. Kriptoloji; bilginin belirli bir yönteme göre şifrelenmesi ve güvenli bir şekilde deşifre edilmesi yöntemidir. Bu ana madde; tek bir alt madde ve iki kontrol içermektedir.

a) Kriptolojik kontroller (Madde A.10.1)

Bilginin gizliliğini ve bütünlüğünü kriptografik yöntemlerle korumak amacıyla oluşturulmuş bir maddedir.

aa) Şifreleme kontrollerin kullanımına yönelik politika (Madde A.10.1.1)

Bilginin güvenliğinin sağlanması için şifreleme kontrolleri uygulanmalı ve bunun kullanımına ait bir politika oluşturulmalıdır.

bb) Anahtar yönetimi (Madde A.10.1.2)

Kurumun kriptografik teknikleri kullanmasını sağlamak için anahtar yönetimi süreci oluşturulmalı ve uygulanmalıdır.

7. Fiziksel ve Çevresel Güvenlik (Madde A.11)

ISO 27001 BGYS sadece BT'ye özgü bir kavram olmadığından bahsetmiştik. Bu standart bir bilgi güvenliği standardıdır ve bu nedenle de bilgi varlıklarına yönelik olarak fiziksel ve çevresel güvenlik de ISO 27001'in konusu kapsamındadır. İki alt maddede tam 15 adet kontrol içermektedir.

a) Güvenli alanlar (Madde A.11.1)

Kurumun binalarına ve veri merkezi vb. bilgi işleme alanlarına yetkisiz fiziksel erişimi ve müdahaleyi engellemek bu maddenin amacıdır.

aa) Fiziksel güvenlik sınırı (Madde A.11.1.1)

Kuruma ait kritik bilgi sistemleri ortamlarının (veri merkezleri gibi) korunması için güvenlik kontrolleri uygulanmalıdır.

bb) Fiziksel giriş kontrolleri (Madde A.11.1.2)

Güvenli ve kritik yerlere, sadece yetkili personelin erişimine izin verilecek uygun giriş kontrolleri konulmalıdır.

cc) Ofisleri, odaları ve olanakları korumaya alma (Madde A.11.1.3)

Ofisler, odalar ve olanaklar için fiziksel güvenlik önlemleri oluşturulmalı ve buna uygun bir süreç tasarlanmalıdır.

çç) Dış ve çevresel tehditlere karşı koruma (Madde A.11.1.4)

Doğal felaketlerden, tehditlerden ve kazalardan kaynaklanabilecek hasara karşı fiziksel koruma önlemleri tasarlanmalıdır.

dd) Güvenli alanlarda çalışma (Madde A.11.1.5)

Güvenli alanlarda çalışmak için gerekli prosedürler tasarlanmalı ve uygulanmalıdır.

ee) Açık erişim, dağıtım ve yükleme alanları (Madde A.11.1.6)

Dağıtım ve yükleme alanları gibi yerler ve yetkisiz kişilerin içeri girebileceği diğer kritik yerler kontrol edilmeli ve yetkisiz erişimi engellemek için bilgi işleme olanaklarından arındırılmalıdır.

b) Teçhizat (Madde 11.A.2)

Bu maddenin amacı; bilgi varlıkların kaybını, zarara uğramasını, çalınmasını veya tehlikeye girmesini ve kurumun faaliyetlerinin kesintiye uğramadan sürdürülmesini sağlamaktır.

aa) Teçhizat yerleştirme ve koruma (Madde A.11.2.1)

Teçhizatlar, fiziksel ve çevresel tehditlerden kaynaklanan bilgi güvenliği riskleri ve yetkisiz erişim ihtimallerini en aza düşürmek için uygun bir şekilde yerleştirilmeli ve gerekli koruma düzeyi oluşturulmalıdır.

bb) Destek hizmetleri (Madde A.11.2.2)

Teçhizatlar, destek hizmetlerindeki problemlerden kaynaklanan diğer bozulmalara ve hasarlara karşı korunmalıdır.

cc) Kablolama güvenliği (Madde A.11.2.3)

Veri taşıyan ya da bilgi işlem hizmetlerini destekleyen elektrik ve ağ kabloları, fiziksel hasarlara karşı korunmalıdır.

çç) Teçhizat bakımı (Madde A.11.2.4)

Teçhizatın kesintisiz kullanılabilirliğini ve bütünlüğünü korumak için doğru bir biçimde bakımları yapılmalıdır.

dd) Varlıkların çıkarılması (Madde A.11.2.5)

Teçhizat, yazılım ve bilgi önceden yetki almadan kuruluş dışına çıkarılmamalıdır.

ee) Kuruluş dışındaki teçhizatın ve varlıkların güvenliği (Madde A.11.2.6)

Kuruluş dışında ki teçhizat için kuruluş dışında çalışmanın farklı risklerini dikkate alarak güvenlik uygulanmalıdır.

ff) Teçhizatın güvenli olarak elden çıkarılması ya da tekrar kullanımı (Madde A.11.2.7)

Teçhizatın depolama ortamı içeren tüm parçaları, elden çıkarılmadan önce, mutlaka hassas ve kritik bir veri içerip içermediğine göre kontrol edilmeli, lisanslı yazılım varsa kaldırılmalı veya güvenli bir biçimde üzerine yazılmasını sağlayacak kontroller oluşturulmalıdır.

gg) Gözetim altında olmayan kullanıcı teçhizatı (Madde A.11.2.8)

Kullanıcılar, gözetim altında bulunmayan teçhizatın uygun bir biçimde korumasını sağlamaya çalışmalıdır.

ğğ) Temiz masa ve temiz ekran politikası (Madde A.11.2.9)

Kâğıtlar, depolama aygıtları vb. ortamlar için bir temiz masa ve temiz ekran politikası oluşturulmalıdır.

8. Operasyonların Güveliği (Madde A.12)

7 alt madde ve 14 kontrol içeren Operasyonların Güvenliği ana maddesi, ISO 27001:2013 sürümüyle gelen bir başlıktır. 2005 sürümünde, Haberleşme ve İşletim Yönetimi ana maddesi altında incelenmekteydi.

a) Operasyonel Prosedürler ve Sorumluluklar (Madde A.12.1)

Amaç: Bilgi işleme tesislerinin doğru ve güvenli olarak operasyonunu sağlamaktır.

aa) Dokümante edilmiş işletim prosedürleri (Madde A.12.1.1)

İşletim prosedürleri dokümante edilmeli, sürdürülmeli, gerektiğinde güncellenmeli ve ihtiyacı olan tüm kullanıcıların erişileceği şekilde düzenlenmelidir.

bb) Değişiklik yönetimi (Madde A.12.1.2)

Kuruluş, iş süreçleri, bilgi işleme tesisleri ve sistemlerde ki bilgi güvenliğini etkileyen değişiklikler kontrol edilmelidir.

cc) Kapasite yönetimi (Madde A.12.1.3)

Verimli bir sistem performansı oluşturmak için, kaynakların kullanımı izlenmeli, düzenlenmeli ve gelecekteki kapasite gereksinimleri ortaya çıkarılmalıdır.

çç) Geliştirme, test ve operasyonel çalışma ortamlarının ayrımı (Madde A.12.1.4)

Yetkisiz erişimlerden veya operasyonel ortamda yapılan değişikliklerden doğan riskleri düşürmek için geliştirme, test ve operasyonel çalışma ortamları ayrılmalıdır.

b) Zararlı koddan korunma (Madde A.12.2)

Amaç: Bilgi ve bilgi işleme araçlarının zararlı koda karşı korunmasını sağlama

aa) Zararlı koda karşı kontroller (Madde A.12.2.1)

Zararlı kodlara karşı tespit, önleme ve kurtarma kontrolleri uygulanmalı ve kullanıcı farkındalığı ile desteklenmelidir.

c) Yedekleme (Madde A.12.3)

Bu maddenin amacı Veri kaybını önlemektir.

aa) Bilgi yedekleme (Madde A.12.3.1)

Bilgi, yazılım ve sistem imajları vb. bilgi varlıkları için yedekleme prosedürleri oluşturulmalı ve bu prosedülerine uygun bir şekilde düzenli olarak yedekler alınmalı ve geri dönüş testleri yapılmalıdır.

ç) Kaydetme ve izleme (Madde A.12.4)

Amaç olayları kaydetme ve kanıtları oluşturmaktır.

aa) Olayların kaydedilmesi (Madde A.12.4.1)

Kullanıcı faaliyetleri, ayrıcalıklar, hatalar ve bilgi güvenliği olayları üretilmeli, saklanmalı ve düzenli aralıklarla gözden geçirilmelidir.

bb) Olay kayıtlarının korunması (Madde A.12.4.2)

Kayıt gerçekleştiren cihazlar ve kayıt bilgileri yetkisiz değişikliğe ve bozulmalara karşı korunmalıdır.

cc) Sistem yöneticisi ve operatör kayıtları (Madde A.12.4.3)

Sistem yöneticisi ve operatör faaliyetleri kaydedilmeli ve düzenli olarak gözden geçirilmesini sağlayacak süreçler tanımlanmalıdır.

çç) Saat senkronizasyonu (Madde A.12.4.4)

Bir kurumdaki tüm ilgili bilgi sistemlerinin saatleri, doğru ve uygun bir şekilde doğru bir zaman kaynağı ile senkron hale getirilmelidir.

d) Operasyonel yazılımın kontrolü (Madde A.12.5)

Operasyonel sistemlerin bütünlüğünü sağlamak amacıyla bu madde oluşturulmuştur.

aa) Operasyonel sistemlere yazılım kurma (Madde A.12.5.1)

Operasyonel sistemlere yazılım kurmayı kontrol etmek amacıyla gerekli prosedürler uygulanmalıdır.

e) Teknik Zafiyet Yönetimi (Madde A.12.6)

Bu maddenin amacı; teknik zafiyetlerin kullanılarak saldırı yapılmasını engellemektir.

aa) Teknik açıklıkların yönetimi (Madde A.12.6.1)

Bilgi sistemlerine ait teknik zafiyetler hakkında zamanında bilgi elde edilmeli, kurumun teknik zafiyetlere maruz kalması durumu değerlendirilmeli ve bunlara ilişkin güvenlik risklerini gidermeye yönelik uygun önlemler alınmalıdır.

bb) Yazılım kurulumu ile ilgili kısıtlama (Madde A.12.6.2)

Kullanıcılar tarafından gerçekleştirilecek kurulumları düzenleyen kurallar belirlenmeli ve uygulanmalıdır.

f) Bilgi Sistemleri Denetim Hususları (Madde A.12.7)

Bu maddedeki amaç; operasyonel sistemler üzerinde ki denetim faaliyetlerinin etkisini azaltmaktır.

aa) Bilgi sistemleri denetim kontrolleri (Madde A.12.7.1)

İş süreçlerini engelleyebilecek güvenlik risklerini en aza indirmek için, operasyonel sistemlerde kontrolleri içeren denetim gereksinimleri ve faaliyetleri dikkatli bir biçimde planlanmalıdır.

9. İletişim Güvenliği (Madde A.13)

İletişim güvenliği, ISO 27001:2005 sürümünde Operasyon Yönetimiyle beraber bir başlık olarak ele alınıyordu ancak 2013 sürümünde ayrı bir ana madde haline getirildi. Temel olarak ağ güvenliğinin sağlanmasında kullanılacak kontrolleri ortaya koymaktadır. İki alt maddede toplam yedi kontrol yer almaktadır.

a) Ağ Güvenlik Yönetimi (Madde A.13.1)

Ağdaki bilginin ve ağ güvenlik ürünlerinin korunması sağlanmalı, uygun bir ağ güvenlik yönetimi sistemi kurulmalıdır.

aa) Ağ kontrolleri (Madde A.13.1.1)

Sistemlerde ve uygulamalarda bulunan bilgiyi korumak amacıyla, ağlar uygun şekilde yönetilmeli ve kontrol edilmelidir.

bb) Ağ hizmetleri güvenliği (Madde A.13.1.2)

Tüm ağ hizmetlerinin güvenlik mekanizmaları, hizmet seviyeleri ve yönetim gereksinimleri belirlenmeli ve bu gereksinimler ağ hizmetlerine ilişkin anlaşmalarda yer almalıdır.

cc) Ağlarda ayrım (Madde A.13.1.3)

Ağlarda uygun bir ayrım yapılmalı, kritik ortamlar izole edilerek güvenli bir ağ yapısı kurulmalıdır.

b) Bilgi İletişimi (Madde A.13.2)

Amaç: Kurum içinde veya herhangi bir dış taraf ile gerçekleştirilen bilgi transferinin güvenliğinin sağlanması

aa) Bilgi iletişim politikaları ve prosedürleri (Madde A.13.2.1)

Tüm ağ üzerinden gerçekleşen bilgi iletişimini korumak için resmi bilgi iletişim politikaları, prosedürleri ve kontrolleri mevcut olmalıdır.

bb) Bilgi transfer anlaşmaları (Madde A.13.2.2)

Kuruluş ve ilgili taraflar arasında gerçekleşen bilgi transferine yönelik güvenlik hususları anlaşmalarda bulunmalıdır.

cc) Elektronik mesajlaşma (Madde A.13.2.3)

Elektronik mesajlaşma sistemleri ve elektronik postalarda yer alan bilginin korunmasına yönelik süreçler oluşturulmalıdır.

çç) Gizlilik ve ifşa etmeme anlaşmaları (Madde A.13.2.4)

Bilginin güvenliğinin sağlanması için kurumun ihtiyaçlarını yansıtan gizlilik anlaşmalarının gereksinimleri tanımlanmalı, dokümante edilmeli ve düzenli olarak gözden geçirilmelidir.

10. Sistem Edinim Geliştirme ve Bakımı (Madde A.14)

Üç alt maddede toplam 13 adet kontrol içermektedir. Bu maddenin amacı; bilgi sistemleri altyapısının, uygulamaların ve süreçlerin güvenliğinin sağlanması, yeni güvenlik gereksinimlerinin belirlenmesidir. Bilgi sistemleri edinimlerinde nelere dikkat edilmesi gerektiğini ortaya koyan kontroller yer almaktadır.

a) Bilgi Sistemlerinin Güvenlik Gereksinimleri (Madde A.14.1)

Amaç: Bilgi güvenliğini, bilgi sistemleri yaşam döngüsünün tamamlayıcı parçası haline getirme. Bu ayrıca halka açık ağlar üzerinden sağlanan bilgi sistemleri için ihtiyaçları da içermektedir.

aa) Bilgi güvenliği ihtiyaçlarının analiz edilmesi ve belirtilmesi (Madde A.14.1.1)

Yeni bilgi sistemleri veya mevcut bilgi sistemlerinin iyileştirilmesine bilgi güvenliği ile ilgili ihtiyaçlar dâhil edilmelidir.

bb) Halka açık uygulama servislerinin güvenliği (Madde A.14.1.2)

Halka açık ağlar üzerinden geçen uygulama servisleri içerisinde ki bilgiler su istimale, kontrat ihtilafına, yetkisiz ifşaya ve değişikliğe karşı korunmalıdır.

cc) Uygulama işlemlerinin (Transaction) korunması (Madde A.14.1.3)

Uygulama işlemlerinde yer alan bilgiler; yetkisiz mesaj değiştirilmesini, yetkisiz ifşayı, yetkisiz mesaj çoğaltması engellenmelidir.

b) Geliştirme ve Destek Süreçlerinde Güvenlik (Madde A.14.2)

Amaç: Bilgi sistemlerinin geliştirme yaşam döngüsü içerisinde bilgi güvenliğini tasarlama ve uygulama.

aa) Güvenli geliştirme politikası (Madde A.14.2.1)

Yazılım ve sistem geliştirmeye dair kurallar belirlenmeli ve Kuruluş içerisinde gerçekleştirilen geliştirme faaliyetlerine uygulanmalıdır.

bb) Sistem değişiklik kontrol prosedürleri (Madde A.14.2.2)

Geliştirme yaşam döngüsü içerisinde bulunan sistemlerde ki değişiklikler resmi değişiklik kontrol prosedürleri ile kontrol edilmelidir.

cc) İşletim sistemindeki değişikliklerden sonra teknik gözden geçirme (Madde A.14.2.3)

İşletim sistemleri değiştirildiğinde, kurumsal işlemlere ya da güvenliğe zarar verecek bir değişiklik olmaması için kritik uygulamalar gözden geçirilmeli ve test edilmelidir.

çç) Yazılım paketlerindeki değişikliklerdeki kısıtlamalar (Madde A.14.2.4)

Yazılım paketlerinde yapılacak değişiklikler; ihtiyaçlar dışında önlenmeli ve tüm değişiklikler sıkı bir şekilde kontrol edilmelidir.

dd) Güvenli sistem mühendisliği prensipleri (Madde A.14.2.5)

Bilgi sistemleri uygulamaları için güvenli sistem mühendisliği prensipleri oluşturulmalı, dokümante edilmeli, uygulanmalı ve sürdürülmelidir.

ee) Güvenli geliştirme ortamı (Madde A.14.2.6)

Kurum, güvenli geliştirme ortamını kurmalı ve uygun şekilde korumalıdır. Bu çalışma tüm sistem yaşam döngüsünü içerecek biçimde sistem geliştirme ve entegrasyon eforlarını içermelidir.

ff) Dışarıdan alınan yazılım geliştirme (Madde A.14.2.7)

Dışarıdan alınan veya dışarıdan bir firma tarafından geliştirilen yazılımlar kurum tarafından denetlenmeli ve izlenmelidir.

gg) Sistem güvenlik testi (Madde A.14.2.8)

Güvenlik fonksiyonlarının testi geliştirme sırasında gerçekleştirilmelidir.

ğğ) Sistem kabul testi (Madde A.14.2.9)

Yeni alınan bilgi sistemleri ürünleri, yazılımlar veya sistemlerin güncellemeleri veya yeni sürümler için kabul test programları ve ilgili kriterler belirlenmelidir.

a) Test Verisi (Madde A.14.3)

Test için kullanılan veriler; maskeleme, şifreleme vb. uygun yöntemlerle korunarak kullanılmalı ve güvenliği sağlanmalıdır.

aa) Sistem test verisinin korunması (Madde A.14.3.1)

Test verileri dikkatli bir şekilde seçilmeli, kontrol edilmeli ve güvenliği sağlanmalıdır.

11. Tedarikçi ilişkileri (Madde A.15)

Kurumların bilgi güvenliği yönetim sistemlerinde kurmalarında ve bilgi güvenliğinin sağlanmasında karşılaştıkları önemli konulardan biri de tedarikçilerle olan ilişkileridir.

Tedarikçilerle olan bilgi paylaşımlarında dikkat edilmesi gereken noktaları belirlemek amacıyla iki alt madde ve beş adet kontrol maddesi oluşturulmuştur.

a) Tedarikçi ilişkilerinde bilgi güvenliği (Madde A.15.1)

Amaç: Tedarikçiler tarafından erişilen Kuruluş varlıklarını koruma

aa) Tedarikçi ilişkileri için bilgi güvenliği politikası (Madde A.15.1.1)

Tedarikçinin kuruluş varlıklarına erişiminden doğan risklerin düşürülmesi için gerekli bilgi güvenliği gereksinimleri tedarikçi ile karşılıklı olarak anlaşılmalı ve dokümante edilmelidir.

bb) Tedarikçi anlaşmalarında güvenliği adresleme (Madde A.15.1.2)

Kuruluşun bilgi teknolojileri altyapı bileşenlerine erişen, işleyen, depolayan veya bileşenleri sağlayan tedarikçiler ile tüm bilgi güvenliği ihtiyaçları karşılıklı olarak anlaşılmalı ve dokümante edilmelidir.

cc) Bilgi ve iletişim teknolojileri tedarik zinciri (Madde A.15.1.3)

Bilgi ve iletişim teknoloji servisleri ve ürün tedarik zinciri ile ilgili bilgi güvenliği risklerini ortadan kaldıracak şekilde gizlilik anlaşmaları yapılmalıdır.

b) Tedarikçi Hizmet Sunum Yönetimi (Madde A.15.2)

Amaç: Tedarikçi anlaşmalarında tanımlanmış üzerinde anlaşılan seviyede bilgi güvenliğini ve hizmet sunumunu sürdürme

aa) Tedarikçi servislerinin izlenmesi ve gözden geçirilmesi (Madde A.15.2.1)

Kuruluş, tedarikçi hizmetlerini düzenli aralıklarla izlemeli, gözden geçirmeli ve denetlemelidir.

bb) Tedarikçi servislerinin değişiklik yönetimi (Madde A.15.2.2)

Tedarikçiler tarafından sağlanan servislerde ki değişiklikler iş bilgisininin, sistemlerin ve süreçlerin kritikliği dikkate alınarak yönetilmelidir. Değişiklikler, mevcut bilgi güvenliği politikaları, prosedürleri ve kontrollerinin iyileştirilmesi ve sürdürülmesini de içermelidir.

12. Bilgi güvenliği ihlal olayı yönetimi (Madde A.16)

Tek bir alt madde ve yedi adet kontrol maddesi içermektedir. Bu madde bilgi güvenliği ihlal olaylarının tespit edilmesi ile ilgili kontroller içermektedir.

a) Bilgi Güvenliği İhlal Olayları Yönetimi ve İyileştirmeleri (Madde A.16.1)

Bilgi güvenliği ihlal olaylarının etkin şekilde önlenmesi, ortaya çıkarılması, zafiyetlerin giderilmesine yönelik olarak etkili bir süreç kurgulanmalı ve sürekli olarak iyileştirilmelidir.

aa) Sorumluluklar ve prosedürler

Bilgi güvenliği ihlal olaylarına hızlı, etkili ve düzenli bir yanıt verilmesini sağlamak için yönetim sorumlulukları ve prosedürleri oluşturulmalıdır.

bb) Bilgi güvenliği olaylarının rapor edilmesi

Bilgi güvenliği olayları uygun yönetim kanalları aracılığıyla mümkün olduğu kadar hızlı biçimde rapor edilmelidir.

cc) Bilgi güvenliği zayıflıklarının rapor edilmesi

Kuruluşun bilgi sistemlerini ve servislerini kullanan çalışanlar ve yükleniciler, sistemler ve servisler üzerinde gözlediği veya şüphelendiği olayları not etmeli ve raporlamalıdır.

çç) Bilgi güvenliği olaylarını değerlendirme ve karar alma

Bilgi güvenliği olayları değerlendirilmeli ve meydana gelen olayın bilgi güvenliği ihlal olayı olup olmadığına göre sınıflandırılmalıdır.

dd) Bilgi güvenliği ihlal olaylarına tepki verme

Bilgi güvenliği ihlal olaylarına dokümante edilmiş prosedürlere uygun olarak tepki verilmelidir.

ee) Bilgi güvenliği ihlal olaylarından öğrenme

Bilgi güvenliği ihlal olaylarının çözümünden ve analizinden edinilen bilgiler gelecekte oluşabilecek ihlal olaylarının etki veya olasını düşürmek üzere kullanılmalıdır.

ff) Kanıt toplama

Kuruluş, kanıt niteliği taşıyabilecek bilgilerin tanımlanması, toplanması, edinilmesi ve korunması için gerekli prosedürleri tanımlamalı ve uygulamalıdır.

13. İş Sürekliliği Yönetiminin Bilgi Güvenliği Yönü (Madde A.17)

a) Bilgi Güvenliği Sürekliliği (Madde A.17.1)

Amaç: Bilgi güvenliği sürekliliğini Kurumun iş sürekliliği yönetim sistemi içerisine bütünleşik hale getirilmesidir.

aa) Bilgi güvenliği sürekliliğinin planlanması (Madde A.17.1.1)

Kuruluş kötü durumlar için bilgi güvenliği ve bilgi güvenliği yönetimi süreklilik ihtiyaçlarını tanımlamalıdır. Örnek olarak kriz veya felaket durumları verilebilir.

bb) Bilgi güvenliği sürekliliğinin uygulanması (Madde A.17.1.2)

Kuruluş kötü durumlar için ihtiyaç duyduğu bilgi güvenliği sürekliliğini sağmak üzere gerekli kontrolleri oluşturmalı, dokümante etmeli, uygulamalı ve sürdürmelidir.

cc) Bilgi güvenliği sürekliliğinin doğrulanması, gözden geçirilmesi ve değerlendirilmesi (Madde A.17.1.3)

Kurum, oluşturduğu ve uyguladığı bilgi güvenliği süreklilik kontrollerini olası kötü durumlarda geçerli ve etkin olduğunu belirlemek üzere düzenli aralıklarla doğrulamalıdır.

b) Yedeklilik (Madde A.17.2)

Amaç: Bilgi işleme araçlarının erişilebilirliğini sağlama

aa) Bilgi işleme tesislerinin erişilebilirliği (Madde A.17.2.1)

Bilgi işleme tesisleri, erişilebilirlik ihtiyaçlarını karşılamak üzere yeterli yedeklik yapısına sahip olmalıdır.

14. Uyum (Madde A.18)

Bilgi sistemlerinin kurulumunda, kullanımında yasal düzenlemeler ve düzenlemelere uyum gerekmektedir. Bununla ilgili maddeleri düzenlemek amacıyla iki alt madde ve sekiz adet kontrol maddesi tanımlanmıştır.

a) Yasal ve anlaşmalardan doğan ihtiyaçlara uyum (Madde A.18.1)

Her türlü hukuka, yasal, düzenleyici ya da sözleşmeye tabi yükümlülüklere uyumsuzluktan sonucunu doğurabilecek güvenlik ihlalleri önlenmesi amacıyla bu madde oluşturulmuştur.

aa) Uygulanabilir yasaları ve sözleşme gereksinimlerinin tanımlanması

İlgili tüm yasal, düzenleyici ve sözleşmeden doğan gereksinimlerin ve kurumun bu gereksinimleri karşılama yaklaşımı her bilgi sistemi ve kurum için açıkça tanımlanmalı, dokümante edilmeli ve güncel tutulmalıdır.

bb) Fikri mülkiyet hakları (IPR)

Fikri mülkiyet haklarına göre araçların ve patentli yazılımların kullanımı üzerindeki yasal, düzenleyici ve anlaşmalarla uyumlu prosedürler geliştirilmelidir.

cc) Kayıtların korunması

Kayıtların kaybedilmesi, silinmesi, yetkisiz erişimlere karşı; yasalar, düzenleyiciler ve anlaşmalardan doğan ihtiyaçlar doğrultusunda uygun olarak korunmalıdır.

çç) Kişisel tanımlayıcı bilgilerin mahremiyeti ve korunması

Kişisel tanımlayıcı bilgilerin gizliliği ve mahremiyeti ilgili yasal ve düzenleyici kurallara göre sağlanmalıdır.

dd) Şifreleme kontrolleri düzenleme

Yasalar, düzenlemeler ve sözleşmelerle uyum için şifreleme kontrolleri kullanılmalıdır.

b) Bilgi Güvenliği Gözden Geçirme

Sistemlerin kurumsal güvenlik politikaları ve standartlarıyla uyumunu sağlamak amacıyla bu madde oluşturulmuştur.

aa) Bilgi güvenliğinin bağımsız gözden geçirmesi

Kurumun bilgi güvenliği yönetimi yaklaşımı ve uygulanması, düzenli olarak belirli aralıklarla veya önemli değişiklikler olduğunda bağımsız bir gözden geçirmeye tabi tutulmalıdır.

bb) Güvenlik politikaları ve standartlarla uyum

Yöneticiler; güvenlik politikalarına, standartlara ve diğer güvenlik ihtiyaçlarına uyumun sağlanması için kendi sorumluluk alanlarındaki tüm güvenlik prosedürlerinin ve süreçlerinin doğru bir şekilde yapılmasını sağlamalıdırlar.

cc) Teknik uyumun gözden geçirilmesi

Bilgi sistemlerinin, kuruluşun bilgi güvenliği politikaları ve standartları ile uyumlu olup olmadığı düzenli aralıklarla gözden geçirilmelidir.

§ 5. BÖLÜM

BİLGİ GÜVENLİĞİ RİSK YÖNETİMİ

I. RİSK NEDİR?

Kurumsal bilgi güvenliğinin sağlanmasında ve ISO 27001 bilgi güvenliği yönetim standardının kurulmasında en önemli konuların başında bilgi güvenliği risklerinin yönetimi ve risk analizi konuları gelmektedir.

Riskin en basit olarak tanımı amaçlar üzerindeki belirsizlik etkisi olarak belirtilmektedir.[20] Bunun dışında bilgi güvenliği açısından en sık kullanılan tanım ise bir varlıktaki bir açıklığın bir tehdit tarafından kullanılma olasılığına risk denilmektedir. Risk için farklı birçok tanım daha vardır ancak bilgi güvenliği risk denildiğinde en çok bilinen tanım budur.

Yukarıda tanımlamaya çalıştığımız risk kavramının içerisinde geçen varlık, tehdit ve zafiyet kavramlarının da burada açıklanmasında yarar var.

A- TEHDİT NEDİR?

Tehdit; bir varlığa zarar verme olasılığı olan olaylar şeklinde ifade edilebilir. Tehditler farklı kategorilerde yer alır.

- İç kaynaklı insan yapımı tehditler (Kurum çalışanları)
- Dış kaynaklı insan yapımı tehditler (Saldırganlar)
- Doğal ve fiziksel tehditler (Sel, Deprem, Yangın vb.)
- Teknik iç tehditler (Bilgi sistemlerindeki teknik sorunlar)

[20] ISO/IEC 31000 Kurumsal Risk Yönetimi Standardı

Kurumlar tehditlerini ve tehdit kaynaklarını iyi yönetebilmeli, siber dünyada yer alan tehditler izlenmeli ve bu tehditlerin yaratacağı etkiler risk analizi yöntemleriyle ortaya konmalıdır.

B- ZAFİYET NEDİR?

Bir varlığın bir tehditten zarar görmesine yol açacak zafiyetler, varlığın korunmasız olma durumu şeklinde ifade edilebilir. Bir varlıktaki zafiyetler, bir tehdit tarafından kullanıldıklarında ortaya çıkan etkiye risk denmektedir. Bu nedenle kurum bilgi varlıklarının envanteri çıkarılmalı, bu varlıkların kurum açısından değerleri belirlenmeli ve zafiyetleri ortaya çıkarılmalıdır. Bu zafiyetlere, kritiklik seviyelerine göre öncelik verilmeli ve ortadan kaldırılma yöntemleri uygulanmalıdır. Kurum varlıklarının zafiyetlerini belirlemek için belirli aralıklarla zafiyet taramaları yapılması çok önem taşımaktadır.

C- VARLIK NEDİR?

Varlık; kurum açısından değer taşıyan, korunması gereken her şey olarak tanımlanır. Bizim için burada belirtilen varlıklar bilgi varlıklarıdır.

Varlıklar süreç akışları incelenerek belirlenir. Kurum için varlıkların envanterinin yapılması ve varlık değerlerinin hesaplanması mühimdir. Kurum için hangi varlığın bilgi güvenliği açısından daha önemli ve kritik olduğu, ortaya çıkabilecek risklerin kuruma yaratacağı etkinin hesaplanması açısından gereklidir. Bir varlığın bilgi güvenliği açısından değerinin hesaplanmasında; varlığın gizlilik, bütünlük ve erişilebilirlik açısından değerlendirilmesi gerekmektedir. Bu sayede kaynaklar daha etkin olarak kullanılır. Aşağıdaki iki şekilde varlıkların envanter tablosu için örnek ve varlığın bilgi güvenliği açısından değerinin hesaplanma biçimi yer almaktadır.

Sıra No:	Varlık Grubu	Varlık	Kategori	Varlık Sahibi	Varlık Kullanıcısı	Gizlilik Değeri	Bütünlük Değeri	Erişilebilirlik Değeri	Değer	Varlığın Eklenme Tarihi	Açıklama
1											
2											
3											

Şekil 4- Varlık envanter tablosu

Güvenlik Hedefi	Düşük	Orta	Yüksek	Çok Yüksek
Gizlilik				
Bütünlük				
Erişilebilirlik				

Şekil 5- Varlık değeri tablosu

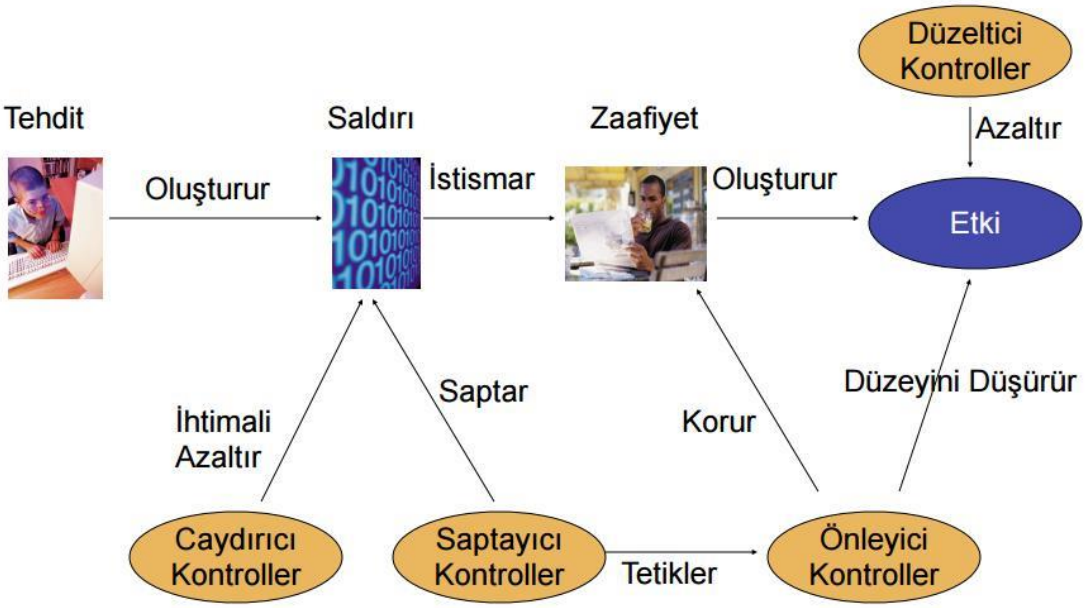
D- KONTROL NEDİR?

Kontrol kavramı; bilgi güvenliği risklerinin azaltılması için alınan tedbirler olarak ifade edilebilir. Kontroller aşağıdaki şekilde sınıflandırılabilir:[21]

- Önleyici kontrol
- Tespit edici kontrol
- Düzeltici kontrol
- Caydırıcı kontrol

Bilgi güvenliği kontrolleriyle ilgili olarak aşağıdaki şekle bakmak kontrollerin etkinliğini anlamak açısından faydalı olacaktır.

[21] Fatih Özavcı, Bilgi Güvenliği Temel Kavramlar, http://viproy.com/files/bgtk.pdf



Şekil 6- Risk Yönetim Kontrolleri[22]

II. BİLGİ GÜVENLİĞİ RİSK ANALİZİ

Bilgi güvenliği risk analizi kavramını; ortaya çıkabilecek güvenlik risklerin meydana gelmeden önce detaylı bir biçimde ve tüm yönleriyle tanımlanarak değerlendirilmesi, bu güvenlik risklerini en aza indirecek veya tamamen ortadan kaldıracak önlemlerin alınması olarak tanımlayabiliriz.

Kurumlar için bilgi güvenliğinin sağlanmasında yapmaları gereken en temel konulardan biri risk analizidir. Risk analizinin amacı; kurumun süreçlerindeki risk seviyesinin istenen düzeye getirilmesidir. Risk analizi kurumlara bilgi güvenliği varlıklarını ve süreçlerinin karşı karşıya kaldığı tehditleri ortaya koyarak, bu tehditlerin hangi varlık veya süreçlerdeki zafiyetleri kullanarak, kuruma hangi tür risklerle yüzleşebileceklerini ve bu risklerin işlenmesi olanağı sunmaktadır.

Varlıkların potansiyel tehditlere karşı ne kadar açık olduğunun bir ölçüsü olan risklerin değerlendirilmesinin ve analiz edilmesinin üç ana hedefi vardır.[23]

[22] a.g.e.
[23] Eren Veysel Ersoy, ISO/IEC 27001 Bilgi Güvenliği Standardı Tanımlar ve Örnek Uygulamalar, s.67 (ODTÜ Yayıncılık, 2012)

Bunlar;

- Tehditleri ve riskleri tanımlamak
- Potansiyel tehlike ve tehditlerin varlıklar üzerinde yapacağı olumsuz etkiyi tahmin etmek
- Riskleri en aza indirebilmek için karşı önlemlerin maliyeti ile risklerin yaratacağı olumsuz etkileri birlikte değerlendirerek dengeli bir yaklaşımla karşı önlemlerin uygulamasını gerçekleştirmek

A- BİLGİ GÜVENLİĞİ RİSK ANALİZİ YÖNTEMLERİ

Temel olarak güvenlik risk analizi için iki farklı yaklaşım vardır.[24] Nitel yöntemlerde analiz; riski düşük, orta, yüksek şeklinde sıfatlar kullanarak sınıflandırmayla yapılır. Nicel yöntemlerde ise matematiksel ve istatistiki ifadeler kullanılır ve sayısal değerler ortaya konur. [25]. Bu iki yöntemin beraber olarak kullanılabildiği durumlar da vardır. Kurumlar risk analizi yöntemlerini belirlerken, kendi ihtiyaçlarını temel alarak, kendisine en uygun risk analizi yöntemini seçmelidir. Bu amaçla zaman ve para harcanacağı için, uygulamadaki mevcut risk analizi yöntemlerini karşılaştırıp değerlendirerek kendi ihtiyaçlarıyla örtüşen bir yöntemi seçmesi kritiktir. Seçim için en iyi yol, bu yöntemlerin tarafsız ve nicel olarak karşılaştırılmasıdır. [26]

B- BİLGİ GÜVENLİĞİ RİSK ANALİZİ YAKLAŞIMLARI

Yukarıda güvenlik risk analizi için uygulanabilecek iki yöntemden bahsettik. Bu risk analizinde kullanılacak yöntemi belirlemek amacıyla kullanılır. Bunun yanı sıra güvenlik risk analizi yapılırken iki farklı yaklaşım daha vardır. Bu iki yaklaşım temelde birbirine çok yakın olmakla birlikte bilgi güvenliği risk analizi yapılırken bilgi varlıkları olarak nelerin seçildiğine

[24] Karabacak, B. Soğukpınar, I, 2004. ISRAM: Information Security Risk Analysis Method, Computers & Security, 24(2), 147-129.
[25] Özden Aktaş, F. Soğukpınar, İ. Bilgi Güvenliğinde Uygun Risk Analizi ve Yönetimi Yönteminin Seçimi İçin Bir Yaklaşım, Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, s.41
[26] Vorster, A., Labuschagne, L., 2005. A framework for comparing different information security risk analysis methodologies, Proceedings of the 2005.

göre değişmektedir. ISO/IEC 27001 yine bu konuda bize bu iki farklı yaklaşıma iki farklı sürümünde yönlendirmektedir. ISO/IEC 27001:2005 sürümü daha çok varlık tabanlı bir risk analizi yaklaşımı benimserken, ISO/IEC 27001:2013 sürümü ile birlikte bu yaklaşım daha çok süreç tabanlı bir risk analizi yaklaşımını önermektedir.

Yine ISO/IEC 27001'in bu iki sürüm farklı risk yönetimi ile ilgili standartlarında da görülmektedir. ISO/IEC 27001:2005 sürümünde risk yönetimi için belirlenen standart ISO 27000 BGYS ailesinin bir standardı olan ISO/IEC 27005 iken, ISO/IEC 27001:2013 daha çok ISO/IEC'nin farklı bir standardı olan ve kurumsal risk yönetimini adresleyen ISO/IEC 31000 Risk Yönetimi standardına yönlendirmiştir. Bilgi güvenliği risk yönetimi yaklaşımının kurumsal risk yönetimi çerçevesi içinde değerlendirilmesi de ISO/IEC'nin bakış açısındaki bir yenilik olarak değerlendirilmelidir.

1. Varlık Tabanlı Risk Analizi Yaklaşımı

Bilgi güvenliği riskini tanımlarken; bir varlık üzerindeki bir zafiyetin bir tehdit tarafından kullanılması sonucu ortaya çıkan etki tanımını yapmıştık. Bilgi güvenliği risk analizi için uygulanan yaklaşım genelde bu şekilde ifade edilmiştir ve güvenlik riski; varlık, tehdit ve zafiyet arasındaki bir ilişkidir. ISO/IEC 27001:2005 sürümü daha çok varlık tabanlı risk analizi yaklaşımını benimsemiştir. Varlık tabanlı risk analizinde en önemli hususun varlık envanteri olduğunu söylememiz gerekmektedir. Kurumlar için yapılması zor ama önemli konuların başında varlık envanteri gelmektedir. Varlık envanterinin yönetilmesi varlık tabanlı güvenlik risk analizi yapılmasının en koşuludur. Bunun ardından ise nicel veya nitel bir yöntem belirlenerek, kapsama dâhil edilen varlıklar üzerindeki zafiyetlerin belirlenmesi ve bu zafiyetlere tehditlerin etkileri hesaplanarak güvenlik risk analizi gerçekleştirilir.

Şekil 7- Varlık tabanlı risk analizi

Varlık tabanlı risk analizinde; varlık envanterinin oluşturulmasından sonra her bir varlığın bilgi güvenliği açısından varlık değeri hesaplanır. Varlık değerinin hesaplanması ise varlığın gizlilik, bütünlük ve erişilebilirlik açısından değeri bulunarak gerçekleştirilir. Varlık değerinin hesaplanması için kullanılabilecek örnek bir varlık envanter ve varlık değeri tablosu aşağıdadır:

2. Süreç Tabanlı Risk Analizi Yaklaşımı

ISO/IEC 27001:2013'le birlikte varlık tabanlı risk analizi yaklaşımı yerine daha çok süreç tabanlı bir risk analizi yaklaşımı benimsenmiştir. Süreçler üzerinden yapılacak bu bilgi güvenliği risk analizi iş birimlerinin daha çok katılımının sağlandığı bir yaklaşımdır. Süreçlerle bilgi sistemi varlıkları arasındaki ilişkilerin ortaya konmuş olması gerekmektedir. Yapılan risk analizi adı üstünde bilgi güvenliği risk analizidir ve değerli olan bilginin kendisidir. İster süreçler üzerinden ister bilgi varlıklar üzerinden gidilirse gidilsin bilgi-varlık-süreç arasındaki ilişkinin kurulmuş olması gerekmektedir. Aksi takdirde yapılacak bilgi güvenliği risk analizi yetersiz ve eksik olacaktır.

Şekil 8- Süreç tabanlı risk analizi

Bu konuyla ilgili olarak bilgi güvenliği yönetişimin en önemli parçalarından biri olan bilgi sınıflandırması ve etiketlenmesi konusunda detaylı olarak değineceğiz.

III. ISO/IEC 27001'E GÖRE RİSK YÖNETİMİ

Bilgi güvenliği yönetim sisteminin kurulması ve bilgi güvenliğinin yönetişimin sağlanmasında bilgi güvenliği risklerinin analiz edilmesi ve yönetiminin yapılması en temel konuların başında geliyor. ISO/IEC 27001 bize yine bu konuda en önemli çerçeveyi sunuyor. ISO/IEC 27001'e göre aşağıdaki sıra ile ifade edebiliriz.

- Kapsam Belirlenmesi
- Risk Değerlendirme Yaklaşımı
- Risk Analizi ve risk derecelendirme

- Risk İşleme
  - Kontrol Seçimi
  - Artık Risk Onayı
- Yönetim Onayı

Gerek BGYS'nin kurulması gerekse de risk analizinin gerçekleştirilmesinde yapılması gereken ilk işlem kapsamın belirlenmesidir. Belirlenen kapsam için daha sonra risk değerlendirme yaklaşımına karar verilir. Sonrasında risk analizi gerçekleştirilir ve riskler nitel veya nicel yöntemlere göre derecelendirilir. Risk analizi ile ilgili detaydan yukarıda bahsetmiştik. Bundan sonraki adım ise risk işleme adımıdır. Burada risk işleme adımından bahsedeceğiz.

A- RİSK İŞLEME

Risk yönetiminde ikinci aşama risk işleme aşamasıdır. Bu aşama risk analizinde belirlenen risklerin nasıl işleneceğine karar verilmesi, önceliklendirilmesi ve riski azaltacak kontrollerin seçilerek uygulanmasından oluşur.[27]

Risklerin tamamen ortadan kaldırılması her zaman mali açıdan mümkün olmamaktadır. [28] Bu durumlarda risk işleme yöntemlerinin kullanılması gerekmektedir. Risklerin azaltılması veya ortadan kaldırılması için en uygun ve en düşük maliyetli seçim yapılır.

1. Risk işleme yöntemleri

Risklere karşı alternatif yaklaşımları şu şekildedir: [29]

[27] Risk yönetim süreci kılavuzu, Tübitak UEKAE, https://www.bilgiguvenligi.gov.tr/dokuman-yukle/bgys/...risk.../download.html
[28] a.g.e.
[29] TS ISO/IEC 27001:2005 BGYS Standardı, s.6

a) Riskin transfer edilmesi

Risklere karşı varlıkların sigorta edilmesi veya riskin servis sağlayıcılara aktarılmasıdır. Bu yöntemde riskin gerçekleşmesi durumunda ortaya çıkacak olan zarar başkasına aktarılmaktadır.

b) Risklerin azaltılması

Risklerin seviyelerinin düşürülmesi için karşı önlemler alınması, uygun kontrollerin belirlenmesi yöntemidir.

c) Risklerden kaçınmak

Riski yaratan sebebin tamamen ortadan kaldırılmasıdır. Örneğin yeni bir sistem kuruluyor, uygulama yazılıyorsa tasarım aşamasında riske yer vermemektir veya riske sebep olan bir uygulama veya sistemin tamamen kullanılmamaya başlanması da risklerden kaçınmaktır.

d) Riskin kabul edilmesi

Risk değerlendirme yaklaşımı belirlenirken, riskle ilgili bir risk iştahı belirlenir. Risk analizi sonucu ortaya çıkan risk, bu risk iştahının altında kalıyorsa veya yönetim tarafından risk için alınacak önlemin maliyeti riskin kendisinden daha maliyetli olduğuna karar veriliyor ise böyle durumlarda risk kabul işlemi gerçekleştirilir.

§ 6. BÖLÜM

UYUM

Bilgi güvenliği yönetişimi ile ilgili çok önemli bir başka konu ise uyum konusudur. İngilizce compliance kelimesinin karşılığı olarak kullandığımız uyum kavramı ile yasa, yönetmelik ve tebliğler, sektörel düzenlemeler ile standart ve çerçeveler anlaşılmaktadır. Bunlardan bazılarına burada değinerek, bilgi güvenliği yönetişimi açısından etkilerine ve neler getirdiklerine, neleri değiştirdiklerine değineceğiz.

- Kişisel Verilerin Korunması Kanunu
- Elektronik Haberleşme Kanunu
- Bankacılık sektöründeki düzenlemeler
  - Bankacılık Kanunu
  - Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ
  - Bankaların Destek Hizmet Almalarına İlişkin Yönetmelik

I. KİŞİSEL VERİLERİN KORUNMASI KANUNU

6698 sayılı Kişisel Verilerin Korunması Kanunu, 24 Mart 2016 tarihinde yasalaşarak hayatımıza girdi. Kanun; *kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemekte*.

Kanun kısaca ve özetle temelde aşağıdaki konuları içermekte:[30]

- Kişisel verilerin işlenme şartlarını
- Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini
- Kişisel verilerin aktarılmasını
- Kişisel verilerin yurtdışına aktarılmasını
- Veri sorumlusunun yükümlülüklerini

[30] 6698 sayılı Kişisel Verilerin Korunması Kanunu, R.G., Sayı:29677, Tarih:24.03.2016, Kanunun tam metni için bkz. http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf

- Kişisel verileri işlenen ilgili kişilerin haklarını
- Veri güvenliğine ilişkin yükümlülükleri
- Başvuru, şikâyet, suç ve kabahatler

Kanun, her kurumu bütün yönleriyle ilgilendirmekte olduğu gibi uyumluluk konusunda Bilişim Teknolojileri bölümleri ve bilgi güvenliği ekiplerine önemli sorumluluklar yüklemektedir. Burada kanunun bilgi güvenliği ile ilgili olan ilişkisi kısmına değineceğiz.

Kanun mevcut haliyle veri güvenliğinin sağlanmasına yönelik olarak ayrı bir madde içeriyor. Kanunun üçüncü bölüm ve 12. Maddesi veri güvenliğine ilişkin olarak veri sorumlusunun yükümlülüklerini açıklıyor. Maddeye göre: [31]

Veri sorumlusu aşağıdaki amaçlar doğrultusunda, uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda.

- Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek
- Kişisel verilerin hukuka aykırı olarak erişilmesini önlemek
- Kişisel verilerin muhafazasını sağlamak

Yukarıda kısaca değindiğimiz Kişisel Verilerin Korunması Kanunu'nun kurumlara bilgi güvenliği açısından ne gibi etkileri olacak? Veri sorumlusu olarak kanunda yer alan kavram, bir kurum açısından bakıldığından kurumun kendisini işaret etmekte. Bu nedenle de veri sorumlusunun kanuna yükümlülük için alacağı bütün tedbirler bir kurumun yapması gereken başlıklar ve bunların tamamı bilgi güvenliğinin meselesi.

Çalışmanın bilgi güvenliği ile ilgili bölümünde bilgi güvenliğinin üç temel prensibi olan; gizlilik, bütünlük ve erişilebilirlik kavramlarına değinmiştik. İşte Kişisel Verilerin Korunması Kanunu; kişisel verilerin işlenmesi, silinmesi, yok edilmesi veya anonim hale getirilmesi, üçüncü kişilere veya yurtdışına aktarılması gibi konularda yükümlülükler getiriyor. Kanunda bahsedilen yükümlülükler tamamen bilgi güvenliğinin üç temel prensibinin sağlanmasına yönelik olan yükümlülükler. Bu nedenlerle Kişisel Verilerin Korunması Kanunu, kurumlar için öncelikli olarak bir bilgi güvenliği meselesidir. Kanun, bu yönüyle kurumların bilgi güvenliği yönetimlerini çok ciddi bir şekilde düzenlemektedir.

[31] 6698 Sayılı Kanun, R.G., Sayı: 29677, Tarih: 07.04.2016

Kurumlar kanuna uyum için gerekli süreçleri oluşturmak zorundalar. Bilgi güvenliği ekipleri de bu süreçlere uygun olacak şekilde kişisel verilerin güvenliğini sağlayacak kendi süreçlerini ve önlemlerini alacaklar. Özellikle düzenlemelerle birlikte bilgi güvenliği yönetişim anlayışı daha ileri düzeyde olan Bankacılık ve Telekomünikasyon sektörleri bir adım önde görünmekteler. Bu sektörlerde daha evvel konmuş düzenlemelerle beraber bilgi güvenliğinin sağlanmasına yönelik olarak önemli düzenlemeler oluşturulmuş ve olgunluk artırılmıştı.

II. ELEKTRONİK HABERLEŞME KANUNU

Bilgi güvenliği açısından değinmemiz ve değerlendirmemiz gereken bir başka önemli kanun da 5809 sayılı Elektronik Haberleşme Kanunu. Elektronik haberleşme sektörünü düzenleyen bu kanun ile kurumlara bilgi güvenliği yönetişimi açısından ne gibi etkileri olduğunu, 60. Maddede yer alan Kurumun yetkisi ve idari yaptırımlar konusunu bilgi güvenliği yönetişimi açısından değerlendirmeye çalışacağız.

İlk olarak; işletmecilerin hak ve yükümlülüklerinin ifade edildiği 12.maddede kurumlara; kişisel veri gizliliği ve korunması, izinsiz erişime karşı gerekli güvenlik önlemlerinin alınması ile ilgili yükümlülükler getiriyor. Ancak kişisel veriler konusunda esas düzenlemenin yer aldığı kişisel verilerin işlenmesi ve gizliliğinin korunması başlıklı 51. Madde. Anayasa Mahkemesi tarafından 2014 yılında iptal edilen madde 2015 yılında yapılan düzenleme ile yürürlükte yer alıyor.

51.Maddenin 1.fıkrasında tıpkı Kişisel Verilerin Korunması Kanunu'nda yer aldığı gibi; kişisel verilerin hukuk ve dürüstlük kurallarına uygun bir biçimde, doğru, güncel, gerektiğinde ulaşılabilir, açık ve meşru amaçlar için işlenmesi, işin gerektirdiği ölçüde sınırlı olacak şekilde işlenmesi ve muhafaza edilmesini gerektiriyor. Haberleşmenin dinlenmesinin ve kaydedilmesinin yasaklandığı 2.fıkrada ise özel hayata ve haberleşme hakkına dair bir bilgi güvenliği prensiplerinden gizlilik özelinde bir düzenleme görülmekte. 51.maddeye ait diğer fıkralarda da özellikle kişisel verilerin gizliliği sağlanması noktasında kurumlara önemli yükümlülükler getiriliyor. Bilgi güvenliği açısından baktığımızda Elektronik Haberleşme Kanunun özellikle 51. Maddesinin Kişisel Verilerin Korunması Kanunu'ndan çok ayrı düşünülemeyeceği ifade edilebilir.

Elektronik Haberleşme Kanunu'nun özellikle Siber Güvenlik açısından baktığımızda, Bilgi Teknolojileri Kurumu'na bazı yetkiler ve haklar tanıdığını görmekteyiz. Sanıyorum, özellikle

bu konuya ilişkin düzenlemeler Bilgi Güvenliği Yönetişimi açısından değerlendirmemiz gereken noktalar. Bunun için de Kanunun 60.maddesini değerlendirmemiz gerekiyor.

9 fıkradan oluşan bu maddeye 2016 yılında yapılan 671 nolu KHK ile 4 fıkra daha eklendi. 60. Madde Bilgi Teknolojileri Kurumu'nun yetkisini ve idari yaptırımlarını düzenliyor. Madde ile BTK'ya kuruluşları denetleme ve denetimleri sonucunda gerekli görülmesi halinde bir önceki yıldaki net satışların yüzde üçüne kadar idari para cezası kesme hakkı veriliyor. Burada yine BTK'nın kuruluşların tesislerine; milli güvenlik, kamu düzeni veya kamu hizmetinin gereği gibi yürütülmesi amacıyla tazminat karşılığında devralma hakkı bulunuyor. [32]

60.madde ile ilgili olarak bizi bilgi güvenliği açısından ilgilendiren asıl kısım 2016 yılında yapılan değişiklikle getirilen fıkralar. Madde 60/10'da Kanun, BTK'ya kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması için her türlü tedbiri alması veya aldırması yükümlülüğü getirildi. Tabi burada kamu kurum ve kuruluşları için alınması gerekecek siber güvenlik tedbirlerinin neler olacağı, kurum ve kuruluşların bunları nasıl gerçekleştirebileceği, buna ilişkin gerekli altyapı ve yönetişim anlayışına sahip olup olmadıkları sorulması gereken sorular arasında yer alıyor.

Elektronik Haberleşme Kanunu'nun 60.maddesi kapsamında, BTK kritik altyapılar olarak belirlenmiş kuruluşlarda siber saldırılara karşı SOME (Siber Olaylara Müdahale Ekibi)'lere güncel tehditlerle ilgili olarak USOM üzerinden bilgilendirmeler yapmakta ve özellikle 60/10'daki görev ve yetkisini ifa etmeye çalışmaktadır.

Yine KHK ile düzenlenen 11. Fıkra ise sanıyorum asıl tartışılması gereken düzenleme. Bu fıkra ile BTK'ya verilen; *"görevi kapsamında ilgili yerlerden bilgi, belge, veri ve kayıtları alabilir ve değerlendirmesini yapabilir; arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanabilir, bunlarla irtibat kurabilir ve bu kapsamda diğer gerekli önlemleri alabilir veya aldırabilir."*[33]

Yukarıdaki fıkrada yer alan, BTK'nın kurumlardan bilgi, belge, veri ve kayıtları alabilir olması, kurumların veri merkezlerinden ve iletişim altyapısından yararlanabilir olması BTK'ya son derece büyük yetkiler vermiş oluyor. Bunun kurumların bilgi güvenliği açısından önemi ne olabilir? Burada bütün bu verilere ve veri merkezlerine el koyma, yararlanma hakkı Devletin bir kurumuna dahi veriliyor olsa bile bu son derece dikkate değer ve eleştiriye açık bir

[32] 5809 Sayılı Elektronik Haberleşme Kanunu R.G., Sayı: 27050, Tarih: 05.11.2008, tam metni için bkz: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5809.pdf
[33] 5809 Sayılı Kanun, Madde 10/11

düzenleme. Kurumsal yönetişimin önemli ilkelerinden birinin şeffaflık olduğunu ifade etmiştik. Bilgi güvenliği yönetişimi açısından ise gizlilik en önemli üç ilkeden bir tanesi, tabi burada şeffaflık ile gizlilik arasında bir çatışma akla gelebilir. Bir kurumun bilgi güvenliği için gizlilik ilkesi fevkalade önemli olsa da düzenleyiciler ile olan paylaşımlarda ise şeffaflık bir yönetişim için oldukça gerekli. Fakat tüm istenilen verilere erişilmesi, veri merkezlerinin kullanımının devralınması şeklindeki bir düzenlemenin kurumsal bilgi güvenliği perspektifinden baktığımız zaman kurumların tüzel kişiliklerine zarar verebileceğini söyleyebiliriz. Sonuç olarak bu kurumlar özel teşebbüsler ve devlet dahi olsa bu şekilde bir devralma, el koyma yetkisinin bir kuruma veriliyor olması sakıncalı olarak değerlendirilebilir. Bunun kurumlar üzerinde bir baskı oluşturması da ayrıca söz konusu. Biz burada bilgi güvenliği ile ilgili sınırlı olarak bu maddeyi değerlendirmeye çalıştık.

Kanunda, siber güvenlik konusu da önemli bir yer tutuyor. Her ne kadar çalışmada, siber güvenlik konusunu kapsam içerisinde ayrıca ele almayıp daha üst bir başlıkta bilgi güvenliği genelinde konuyu değerlendiriyor olsak da; kanunda yer alan siber güvenlik ile ilgili hususlara da kısaca değinmekte yarar var.

Ek Madde olarak Siber Güvenlik Kurulu'nun kurulduğuyla ilgili bir madde yer alıyor Kanun'da. Bu ek madde ile Siber Güvenlik Kurulu'nun yetkileri ve görevleri belirleniyor. Bilgi güvenliği yönetişimi açısından çalışmanın önemli bir yerini işgal eden insan faktörü de Elektronik Haberleşme Kanununda yer alan bir başka husus. 5.madde 1.fıkrada yer alan Bakanlığın görevleri ve yetkileri başlığına 2014 yılında eklenen "h" bendinde Bakanlığa; siber güvenlik farkındalığının artırılması konusunda çalışmalar yapılması görevi veriliyor. Yine aynı bentte siber güvenlik alanında faaliyet gösteren gerçek ve tüzel kişilerin uyması gereken kural ve hususları hazırlama görevi Bakanlığa verilmekte.

Yukarıda bahsettiğimiz 5.madde 1.fıkra h. Bendinde, Bakanlığa siber güvenlikle ilgili milli çözümlerin üretilmesi ve geliştirilmesi ile ilgili olarak Bakanlığa bir görev verildiği görülüyor. Yeri gelmişken bu konu üzerinde biraz durmak istiyoruz. Çalışmada kurumsal bir bilgi güvenliği yönetişimi için genel kavramları ve bilgi güvenliği yönetişiminde insan rolünü ortaya koyan bir kapsam ortaya koymuş olsak da, bilgi güvenliğinin bir kısmı siber güvenlik dediğimiz başlık. Siber güvenlik deyince de bir saldırgan ve kurumun güvenlik altyapısı gelmekte. Fakat girişte de açıkladığımız gibi bu sadece para kazanmak veya kişisel hırsları için bir "hackleme" olayı gerçekleştirmek isteyen "hacker" ile kurumların güvenlik ekiplerinin mücadelesinin de ötesinde devletler arası bir savaş yöntemi haline gelmiş bulunuyor. Bu konu mutlaka üzerinde ayrıca çalışılması gereken geniş bir konu fakat kurumsal bir bilgi güvenliği yönetişimi açısından

baktığımız zaman özellikle ülkelerin kendi milli güvenlik yazılımlarını üretiyor olmaları ve bunları gerek kamu kurum ve kuruluşlarında gerekse de özel sektörlerinde kullanmaları önemli.

Ülkemiz açısından bakıldığında yerli ve milli güvenlik yazılımlarının yeterli olduğunu söylemek imkansız. Bankacılık, Enerji, Telekomünikasyon sektörleri başta olmak üzere birçok kritik altyapıyı içeren sektörde kullanılan bilgi teknolojileri ürünleri, çözümleri, güvenlik yazılımları çok büyük bir oranla yabancı üreticilere ait. Bu durum da siber güvenliğin artık milli güvenliğin bir parçası haline geldiği günümüz dünyasında hem kamu kurumlarının hem de özel sektör kurumlarının yeterince güvende olmadığı sonucuna bizi ulaştırabilir.

Kurumlarımız, bilgi güvenliği yönetişimlerini teknoloji-süreç-insan odaklı bir biçimde gerçekleştirmeye çalışırken, yerli güvenlik teknolojileri çözümlerini kullanamıyor olmaları, onları ancak bir yere kadar güvende tutabilecektir.

III. BANKACILIK SEKTÖRÜNE AİT DÜZENLEMELER

A- BANKACILIK KANUNU

5411 sayılı Bankacılık Kanunu, Bankacılık sektörünü düzenleyen en önemli kanun. Bankacılık kanunun özellikle bilgi güvenliğini yakından ilgilendiren maddelerini ifade etmemiz gerekir. Bankacılık Kanunda yer alan sırların saklanması ile ilgili olan 73. Madde müşteri ve bankacılık sırrı kapsamına giren bilgilerin ifşa edilmesi, açıklanması ve saklanması konularını düzenlemektedir.[34] Banka bilgi güvenliği ekipleri için bu maddeye göre alınması gereken tedbirler bulunmaktadır.

Bankacılık Kanunu'nu; bilgi güvenliği açısından değerlendirdiğimiz zaman müşteri ve bankacılık sırrı olarak nitelendirilen bilgilerin, bankalar tarafından korunmasına yönelik gerekli tedbirleri almakla yükümlü tuttukları görülmektedir. Ancak Bankacılık Kanunu'nda ifade edilen müşteri ve bankacılık sırrı ile ilgili bilgilerin korunmasına yönelik tedbirleri esas düzenleyen sektörde kısaca İlkeler Tebliği olarak ifade edilen "Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğidir.

[34] 5411 Sayılı Bankacılık Kanunu, R.G., Sayı: 25983, Tarih: 01.11.2005, tam metni için bkz: https://www.bddk.org.tr/websitesi/turkce/Mevzuat/Bankacilik_Kanunu/15405411_sayili_bankacilik_kanunu.pdf

B- BDDK İLKELER TEBLİĞİ

BDDK tarafından "Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlklere İlişkin Tebliğ" bankaların, faaliyetlerinin ifasında kullandıkları bilgi sistemlerinin yönetiminde esas alınacak asgari usul ve esasları düzenlemek amacıyla 2007 yılında yayınlanmıştır.[35] Sektörde daha çok BDDK İlkeler Tebliği olarak bilinmektedir.

İlkeler Tebliği üç ana kısımdan oluşuyor. Başlangıç kısmı Bilgi sistemleri yönetiminin önemi üzerinde duruyor. İkinci kısım 'Risk Yönetimi ve İç Kontrollerin Tesisi", üçüncü kısım ATM ve İnternet Bankacılığı gibi iki tane özellik arz eden işlemlerden oluşuyor. İlkeler tebliği, risk yönetimi odaklı bir yaklaşıma sahip ve yönetim gözetimi son derece önemli.

BDDK bu tebliği ile bankacılık sektörü için aşağıdaki konu başlıklarında belirli kurallar getirmekte ve düzenlemektedir:

- Bilgi sistemleri risk yönetimi ve iç kontrollerin tesisi,
- Güvenlik kontrollerinin tesisi,
- Kimlik doğrulama,
- Görevler ayrılığı prensibi,
- Yetkilendirme,
- İşlemlerin ve kayıtların bütünlüğünün sağlanması,
- Denetim izlerinin oluşturulması,
- Veri gizliliği ve müşteri bilgilerinin mahremiyeti ve korunması,
- Bilgi sistemleri süreklilik planı
- ATM, İnternet Bankacılığı gibi özellik arz eden işlemlere ilişkin olarak uyulması gereken kurallar

Sektörde daha çok, kısaca İlkeler Tebliği olarak bilinen düzenleme Bankacılık sektöründe bilgi sistemlerini detaylı olarak düzenlemektedir. BDDK, İlkeler Tebliği'nin yanı sıra iki yılda bir COBIT üzerinden bağımsız denetim kuruluşları aracılığıyla sektörü denetlemektedir.

[35] Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ, R.G., Sayı: 26643, Tarih: 14.09.2007, tebliğ tam metni için bkz. http://www.bddk.org.tr/websitesi/turkce/mevzuat/bankacilik_kanununa_iliskin_duzenlemeler/9491ilkelerteblig.pdf

COBIT konusunu 3. Bölümde incelemiştik. COBIT, BDDK'nın sektörü denetlemek için kullanmış olduğu yönetişim çerçevesidir.

İlkeler Tebliği, bilgi sistemlerini düzenleyen bir tebliğ ise de ağırlık yine bilgi güvenliği üzerindedir. Tebliğ bilgi güvenliği ile ilgili konularda ne yapılması gerektiğini, nasıl yapılması gerektiği detayına girmeden ortaya koymaktadır.

BDDK tebliği ile öncelikle Bankalarda bilgi sistemlerinin önemini vurgulamakta, bankanın bilgi sistemlerinin yönetim anlayışının kurumsal yönetim uygulamalarının içinde ele alması gerekliliğini ortaya konmaktadır.[36] Bu önemi "*Bankanın operasyonlarını istikrarlı, rekabetçi ve gelişen bir çizgide sürdürebilmesi için bilgi sistemlerine ilişkin stratejinin iş hedefleri ile uyumlu olması sağlanır, bilgi sistemleri yönetimine ilişkin unsurlar yönetsel hiyerarşi içerisinde uygun yere yerleştirilir ve bilgi sistemlerinin doğru yönetimi için gerekli finansman ve insan kaynağı tahsis edilir"* [37] şeklinde ifade etmektedir.

Tebliğe göre Bankalar; bilgi sistemleri üzerinde kurulan yönetimin etkinliği; risk yönetimi, iç kontrol sistemi ve iç denetim kapsamında yürütülecek çalışmaların da katkısıyla sağlanacaktır. Banka yönetimi, bilgi sistemlerine ilişkin politikalar, prosedürler ve süreçleri tesis etmek zorundadır.[38]

Bankalar, bankacılık faaliyetlerinin yürütülmesini artık tamamen bilgi teknolojileri ile sağlamaktadır ve BDDK, Bankalardan bankacılık faaliyetlerini bilgi teknolojileri üzerinden sürdürmelerinden kaynaklanan riskleri ölçmek, izlemek, kontrol etmek ve raporlamak üzere gerekli önlemleri[39] almasını beklemektedir.

Tebliğ, Bankalara özellikle üst yönetimlerin gözetimi ve desteği konusunda önemli sorumluluklar yüklemektedir. Banka üst yönetiminin bilgi sistemlerinden kaynaklanan risklerin yönetilmesi için etkin bir gözetim yürütmesi gerekmektedir. *Bu amaçla üst yönetim tarafından değerlendirmeden geçirilmiş ve uygunluğu onaylanmış, bilgi sistemlerinin kullanımından kaynaklanan risklerin yönetilmesine yönelik, kapsamlı bir süreç üst düzey yönetim tarafından hazırlanmalıdır*.[40]

Yönetim Kurulu tarafından onaylanmış bilgi güvenliği politikaları, çalışanların bilgi güvenliği farkındalığını yükseltecek çalışmaların yapılması yine önemli konulardandır. Banka

[36] Ahmet Uçar, Bankacılık Sektöründe Bilişim Suçları, s.49
[37] 26643 Sayılı Tebliğ, Madde 4/1
[38] 26643 Sayılı Tebliğ, Madde 4/3
[39] 26643 Sayılı Tebliğ, Madde 5/1
[40] 26643 Sayılı Tebliğ, Madde 6/1

üst yönetiminin bilgi güvenliği politikaları kapsamında güvenlik risklerinin yönetildiğinden ve bu risklere karşı önlemler alındığından emin olmak için güvenlik kontrol süreci kurması gerekmektedir.

Tebliğde yer alan önemli konulardan biri de bankaların destek hizmetleri alımıyla ilgilidir. BDDK'nın konu özelinde ayrıca bir yönetmeliği da bulunuyor. Banka üst yönetiminden, *bilgi sistemleri kapsamında alınacak destek hizmetlerine ilişkin olarak, söz konusu hizmetin destek hizmeti alımı yoluyla gerçekleştirilmesinin banka açısından doğuracağı risklerin yeterli düzeyde değerlendirilmesi, yönetilmesi ve destek hizmeti kuruluşu ile ilişkilerin etkin bir şekilde yürütülebilmesine olanak sağlayacak yeterli bir gözetim mekanizması tesis edilmesi beklenmektedir.*[41]

İlkeler tebliğinde; müşterilerin bilgilendirilmesi ve müşteri bilgilerinin mahremiyeti konuları ayrı birer başlık olarak ele alınmıştır. Banka tarafından sunulan elektronik bankacılık/alternatif dağıtım kanalları (internet, telefon, televizyon, WAP/GPRS, Kiosk, ATM vb.) hizmetlerinden yararlanacak müşterilerin hizmetlere ilişkin şartlar, riskler ve istisnai durumlarla ilgili olarak açık bir şekilde bilgilendirilmesi gerekmektedir. Bankanın söz konusu hizmetlere ilişkin risklerin etkisini azaltmaya yönelik benimsediği güvenlik prensipleri ve korunma yöntemlerini müşterinin dikkatine sunması gereklilikleri belirtilmiştir. Müşteri bilgilerinin mahremiyetini sağlamaya yönelik gerekli tedbirlerin alınması, bununla ilgili politika ve prosedürlerin oluşturulması ve ilgili tüm birimlere iletilmesi ve bankanın faaliyetleri kapsamında edindiği, müşteriye ait bilgileri amaçları dışında kullanamayacağı, saklayamayacağı ve diğer taraflarla paylaşamayacağı tebliğde ifade edilmektedir.

BDDK İlkeler tebliğinin başlık ayırdığı önemli konulardan iki tanesi de kimlik doğrulama ve yetkilendirme konusudur. Bu iki başlık, Bilgi güvenliğinin sağlanması için kritik öneme sahiptir. Bankalar, bilgi sistemleri üzerinden gerçekleştirilen işlemler için uygun bir kimlik doğrulama mekanizması kurmak zorundadır. BDDK, bankanın hangi kimlik doğrulama tekniğini bankanın kendisine bırakmasına rağmen bu tekniği belirlerken, bunun risk değerlendirmesi sonucuna göre yapılması gerekliliğini yine ortaya koymaktadır. Risk değerlendirmesi yaparken göz önünde bulundurulması gereken noktalarda ifade edilmektedir. BDDK da tebliği yazarken bilgi güvenliği-risk değerlendirmesi ilişkisini hiç gözden kaçırmamış ve tebliğin bütününe bu anlayışı yerleştirmiştir.

[41] 26643 Sayılı Tebliğ, Madde 8/1

Kimlik doğrulama mekanizmasının işlemlerin başlangıcından sona ermesine kadar sağlanması, kimlik doğrulama verilerinin yer aldığı veri tabanlarının güvenliğinin sağlanması, kimlik doğrulama verilerinin veri tabanlarında şifreli bir şekilde saklanması, verilerin aktarılmasında gizliliğin sağlanması ve denetim izlerinin güvenliğinin sağlanması, BDDK'nın bankalardan beklentileridir.

Bankaların bilgi sistemlerinde yer alan veri tabanlarına, uygulamalara ve sistemlere erişim için uygun bir kimlik doğrulama, yetkilendirme ve erişim kontrolü mekanizması oluşturması beklenmektedir. Yetkilendirmede erişim haklarının rol ve görev tanımlarına göre asgari seviyede tutulması önem arz etmektedir.

İlkeler tebliğin önemli bölümlerinden biri özellik arz eden işlemlerdir. Bu konuda öncelikle internet bankacılığı ve ATM konuları işlenmiştir. Tebliğe göre internet bankacılığına ilişkin her türlü altyapı bankanın bilgi sistemlerinin bir parçası olarak[42] değerlendirilmesi gerekmektedir. Yönetim gözetiminin öneminin burada da altı çiziliyor. Kritik konulardan biri de güvenlik kontrollerinin yeterliliğini test etmek üzere bağımsız ekiplere, en az yılda bir kez olmak üzere, internet bankacılığı faaliyetleri kapsamındaki sistemler için sızma testlerinin yaptırılması ve internet bankacılığı faaliyetleri kapsamında gerçekleşen sıra dışı ve şüpheli işlemleri tespit etmek için takip mekanizmaları kurulmasıdır.[43]

İnternet bankacılığıyla ilgili olarak uygun bir kimlik doğrulama mekanizmasının kurulması önem arz etmektedir. BDDK, müşterilere uygulanan kimlik doğrulama mekanizmasının birbirinden bağımsız en az iki bileşenden oluşturulması gerekliliğini bankalara tebliğ etmektedir. Bu iki bileşen; müşterinin "bildiği", müşterinin "sahip olduğu" veya müşterinin "biyometrik bir karakteristiği olan" unsur sınıflarından farklı ikisine ait olmak üzere seçilebilir.[44] Bunun yanı sıra kimlik doğrulamada kullanılan parolanın güvenliği, PIN'lerin güvenliğinin sağlanmasına ilişkin hususlar tebliğde yer almaktadır.

İlkeler Tebliğinin son olarak yer verdiğim kısım ise ATM güvenliği ilgili. Tebliğe göre; Bankaların ATM cihazlarına yönelik olarak gerçekleşebilecek hırsızlık, sahtekârlık, fiziksel saldırı gibi tehditlere ilişkin riskleri minimize edecek önlemleri tesis etmesi gerekiyor. Bunun yanı sıra müşterilerin ATM cihazlarının güvenli kullanımıyla ilgili farkındalıklarının artırılması da bankalardan beklenenler arasında yer alıyor.

[42] 26643 Sayılı Tebliğ, Madde 24/1
[43] 26643 Sayılı Tebliğ, Madde 26/2
[44] 26643 Sayılı Tebliğ, Madde 27/4

ATM güvenliği konusunun önemli bir kısmı ATM cihazlarıyla ilgili alınacak fiziksel önlemlerden oluşuyor. Bu nedenle ATM cihazlarının bulunduğu yerlerde güvenlik kamerasının bulundurulması gerekmektedir. Bankalar, ATM cihazları üzerine, zararlı içerikli programların kötü niyetli kişilerce yüklenmesini ve yetkisiz erişimi engelleyecek gerekli tedbirler almaktan, cihaza yetkisiz kişilerin başka bir elektronik cihaz bağlamasını sağlayacak bütün giriş noktaları erişime kapatılmasını sağlamaktan da sorumludur. Tebliğ, tıpkı internet bankacılığında olduğu gibi ATM'lerde de kimlik doğrulama için iki bileşenli erişimi zorunlu kılıyor. Burada bahsedilen iki bileşen müşterinin "bildiği", müşterinin "sahip olduğu" veya müşterinin "biyometrik bir karakteristiği olan" unsur sınıflarından farklı ikisine ait olmak üzere seçilmesi gerekiyor. Müşterinin "bildiği" unsur olarak PIN bilgisi gibi bileşenler, "sahip olduğu" unsur olarak ATM kartı gibi bileşenler kullanılabilir.

Alınması gereken tedbirlerden bir tanesi de ATM cihazları üzerinden gerçekleşen işlemler için kullanılan iletişim ağının veri güvenliği, gizliliği ve bütünlüğünü sağlayacak şekilde oluşturulmasıdır.

ATM güvenliği konusunda en önemli konulardan biri yine eğitim ve farkındalık konusu. Gerek müşterilerin gerekse de ATM cihazlarından sorumlu tekniker ve operatörlerin ATM cihazlarıyla ilgili sahtekârlık yöntemleri konusunda farkındalıklarının artırılması çok önemli bir yer tutmakta.

İlkeler tebliğinin bankacılık sektörü açısından neleri düzenlediğini ve kurumlardan bilgi güvenliği açısından neler beklediğini yukarıda ifade ettik. Tebliğin bir bütünlük açısından bakıldığında genel hatlarıyla sektörü düzenlediği, 2008 yılından itibaren de denetimler yoluyla bankacılık sektöründe bilgi güvenliği ile ilgili olarak bankaların önemli yol almasını sağladığını da ifade etmemiz gerekiyor. Bunun yanı sıra başta bulut bilişim, biyometrik kimlik doğrulama gibi konularda bir takım açık noktaların bulunduğunun da altını çizmemiz gerekmekte. Bu ve benzeri sebeplerle ilkeler tebliğinin güncellenmeye ihtiyacı olduğu söylenebilir. Bunun yanı sıra bankacılık sektörü açısından bakıldığında hem COBIT hem İlkeler tebliği açısından yapılan denetimler hem de tebliğin bankalara kendi iç denetim ekipleri üzerinden yaptırdığı denetimler çoğu zaman bankaları zor ve gereksiz bir yükün altına soktukları da görülmektedir. Bu açıdan da baktığımızda İlkeler Tebliğinin daha detaylı ve genel bir standart haline getirilmesi yerinde görülebilir.

C- BANKALARIN DESTEK HİZMETİ ALMALARINA İLİŞKİN YÖNETMELİK

Bankacılık sektöründe bilgi sistemleri ve bilgi güvenliği konusundaki bir başka düzenleme ise Bankaların Destek Hizmeti Almalarına İlişkin Yönetmeliktir. Yönetmeliğin amacı; bankalarca destek hizmeti alımına ilişkin usul ve esasları düzenlemektir.[45]

Yönetmelik ile bankaların hangi tür hizmetleri banka dışından alabilecekleri ve bu hizmetler için uymaları gereken kuralları düzenlemektedir. Yönetmelikte bilgi sistemleriyle ilgili olarak; bilgi sistemleri, bankacılık faaliyetlerini destekleyen bir araç olarak değerlendirilmek suretiyle, bankacılık mevzuatının gerektirdiği bankacılık faaliyet ve yükümlülükleri bakımından yönetim, içerik tasarımı, erişim, kontrol, denetim, güncelleme, bilgi/rapor alma gibi fonksiyonlarda karar alma gücünün ve sorumluluğun bankada olması şartıyla destek hizmeti alımına konu edilebileceği belirtilmektedir.[46]

Yönetmeliğe göre; bankalar tarafından destek hizmeti de dâhil olmak üzere alınan her türlü hizmet alımlarında banka ve müşteri sırrının güvenliğinin sağlanması için gerekli tedbirlerin alınması zorunludur. Hizmet alınan tarafından bilgiye erişimin gerekli olması durumlarda; sisteme erişim, veriye erişim veya veriyi görme yetkisi işin gerektirdiği bilgiyi kapsayacak şekilde sınırlandırılması gerekmektedir. Veri güvenliğinin sağlanması için alınan hizmetin niteliğine göre önemli nitelikteki bilgilerin; maskelenmesi, şifrelenmesi veya kodlanması, veri girişi yapılacak ise sistem erişim yetkisi verilmeden harici bir yerde veri girişinin yapılması ve bu verilerin daha sonra banka tarafından sisteme aktarılması gerekmektedir. Destek hizmeti sağlayan kuruluşta müşteri verisinin saklanmaması bankanın sorumluluğunda yer alan bilgi güvenliği ile ilgili bir başka konudur.

[45] Bankaların Destek Hizmeti Almalarına İlişkin Yönetmelik, R.G., Sayı: 28106, Tarih: 05.11.2011, yönetmeliğin tam metni için bkz. https://www.bddk.org.tr/websitesi/turkce/Mevzuat/Bankacilik_Kanununa_Iliskin_Duzenlemeler/10310destek_yonetmelik_islenmis.pdf

[46] 28106 Sayılı Yönetmelik

§ 7. BÖLÜM

BİLGİ GÜVENLİĞİ YÖNETİŞİMİ

I. BİLGİ GÜVENLİĞİ YÖNETİŞİMİ NEDİR?

Bilgi güvenliği yönetişimi konusu son yıllarda git gide önem kazanan, üzerinde çalışmaların yapılmaya başlandığı bir alan. Teknolojinin hızlı gelişimi beraberinde bilgi güvenliği kavramının da değerini artırdı. Bilgi güvenliğinin artan önemi de dolayısıyla bilgi güvenliğinin nasıl daha efektif olarak yönetilebileceği konusunu gündeme taşıdı.

Bilgi güvenliği yönetişimi kısaca; kurumlardaki bilgi güvenliği sorumluluğunun kurumun üst yönetiminde olması, üst yönetimin bilgi güvenliği ile ilgili kararları alması ve bu kararların uygulandığının takip edilmesi olarak özetlenebilecek bir kavramdır.[47] Bilgi güvenliği yönetişimi yönetim kurulu düzeyinde üst yönetimin sorumluluğundadır. Üst yönetimin bilgi güvenliği ile ilgili yeterli ve gerekli farkındalığının oluşturulması bilgi güvenliği yönetişimi prensibinin ilk adımı olarak ifade edilmelidir.

Yönetişim kavramından bahsederken; yönetişimin, yönetimden farklı olarak tüm paydaşların karar alma süreçlerinde katkıda bulunması gerektiğini ifade etmiştik. Bilgi güvenliği yönetişimi için de durum aynıdır. Yönetim Kurulunun ve üst yönetimin sorumluluk alanına giren bilgi güvenliği yönetişimine tüm kurum ortaktır. Bu ortaklık etkileşimli bir bilgi güvenliği yönetişimi modeli oluşturulmasıyla mümkündür. Bunun için de tüm çalışanlar bilgi güvenliğinden sorumludur ve yeterli bilgi güvenliği bilincine sahip olmalıdır.

Bilgi güvenliği yönetişimi; kurumsal yönetişimin bir parçası olmalı ve BT yönetişim çerçevesiyle uyuşmalıdır.[48] Üst yönetimin en önemli sorumluluklarından biri; bilgi güvenliğinden kaynaklanan risklerin farkında olmak ve bu risklerin giderilmesi için gerekli kontrollerin oluşturulmasını sağlayacak süreçlerin oluşturulmasını sağlamaktır.

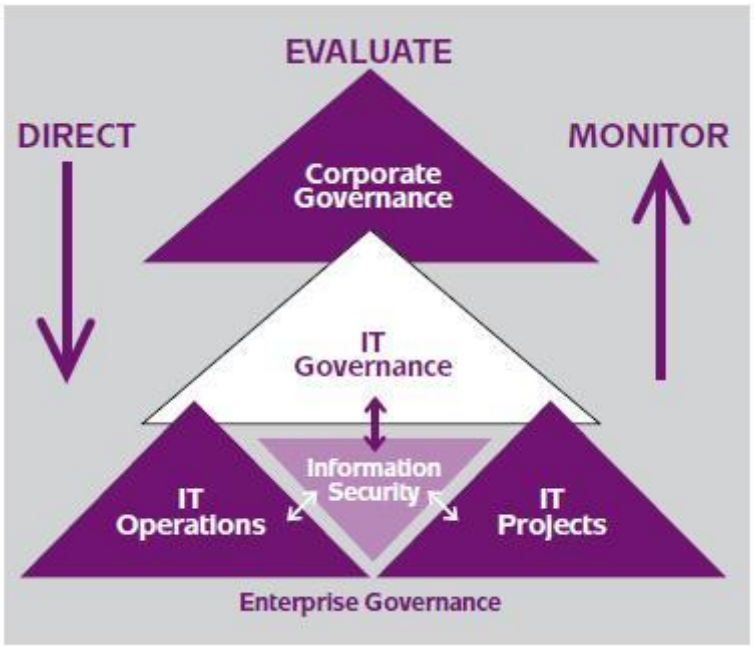
[47] Bilge Karabacak, ISO/IEC 27001:2005 ve Bilgi Güvenliği Yönetişimi – Türkiye Analizi, TÜBİTAK BİLGEM, 2008

[48] Information Security Governance, Guidance for Boards of Directors and Executive Management, 2nd Edition IT Governance Institute, USA, 2003 s.11

Bilgi güvenliği yönetişiminin birçok yönü vardır. Bunlar;[49]

- Bilgi güvenliği yönetişiminin istenen sonuçları vermesi
- Bilgi varlıklarının korunması
- Süreçlerle entegrasyon
- Bilgi güvenliği yönetişiminin faydaları

Bilgi güvenliği yönetişimini anlamak için 8 numaralı şekle bakmamızda yarar var. Bilgi güvenliği yönetişiminin; kurumsal yönetişim, BT yönetişimi, BT operasyonları ve BT projeleriyle olan ilişkisini ve bunlar arasında ölçme, değerlendirme ve izleme açısından etkileşim anlatılmaktadır.



Şekil 9- Bilgi Güvenliği Yönetişimi Üçgeni [50]

II. BİLGİ GÜVENLİĞİ YÖNETİŞİMİ NEDEN GEREKLİDİR?

Bilgi güvenliği yönetişimi risk odaklı bir yaklaşımdır. Bilgi güvenliği yönetişimine olan ihtiyacı anlamak için bilgi teknolojileri ve risklerine değinmek gerekmektedir. Günümüzde

[49] a.g.e.
[50] Global Technology Audit Guide(GTAG) 15, Information Security Governance,

kurumların iş süreçlerinin önemli bir bölümünü bilgi teknolojileri ortamlarına taşımalarıyla birlikte bilgi teknolojileri risklerinin önemi artmıştır. Geçmişte kurumlar için bilgi güvenliği açısından en önemli risk kâğıt ortamında yer alan bilginin çalınma riski iken artık bilgi teknolojilerinden kaynaklanan çok çeşitli riskler söz konusu olmuştur.

Bilgi teknolojileri iş süreçlerini hızlandırmış ve kolaylaştırmıştır. Ancak bilgi güvenliği risklerini de önemli ölçüde artırmıştır. Bilgi teknolojileri; bilgiye uzaktan erişim olanağı sağlar ve bu durum saldırganlar için bilgiye ulaşmanın bir yolu haline gelmiştir. Bilgi güvenliğinin temel özellikleri olan; bilginin gizliliği, bütünlüğü ve sürekli erişilebilirliğinin sağlanması noktasında riskleri ortaya çıkarmıştır.

BT'den kaynaklanan bilgi güvenliği riskleri kurumların iş süreçlerini de yakından etkilemekte ve bu süreçleri kesintiye uğratabilmektedir. Bilgi güvenliği yönetişimi kavramını daha iyi anlamak için bilgi güvenliği riskleri üzerinden biraz daha ayrıntılı olmak durmamız gerekiyor.

Bilgi güvenliği ile ilgili riskleri dört kategoride ifade edilebilir:

- Finansal riskler
- İtibar riskleri
- Uyum riskleri
- Operasyonel riskler

Bilgi güvenliği sadece teknoloji ile ilgili bir konu değildir. Teknolojinin yanı sıra süreç ve insan faktörü bilgi güvenliği açısından çok önemli bir yer tutmaktadır. Özellikle çalışanların bilgi güvenliği farkındalık seviyeleri bilgi güvenliğinin sağlanması için son derece kritiktir ve bu konuya bu bölüm içerisinde ayrıntılı olarak yer vereceğiz. Bilgi güvenliği risklerini anlamak ve bu riskleri gidermek için de teknolojiden kaynaklı bilgi güvenliği risklerinin yanında süreçlerden ve insan kaynaklı bilgi güvenliği risklerine de odaklanmak gerekmektedir.

Bilgi güvenliği sadece BT'nin veya bilgi güvenliği ekiplerinin konusu değildir. Bilgi güvenliği, üst yönetimin sorumluluğu ve desteği olmadan yönetilebilir olamaz. Bu durum da bilgi güvenliği yönetişimi gerekli kılınır.

Teknolojiden kaynaklanan bilgi güvenliği risklerini gidermek için kurumlar, teknolojik yatırımlara büyük önem vermekte ancak daha soyut riskler olarak nitelendirebileceğimiz süreç

ve insan odaklı bilgi güvenliği riskleri arka planda kalabilmektedir. Kurumlar teknoloji kaynaklı bilgi güvenliği risklerini giderebilmek için aldıkları önlemlerden bazılarını aşağıdaki şekilde sıralayabiliriz:

- Firewall (Güvenlik Duvarı)
- IPS (Saldırı Önleme Sistemleri)
- WAF (Web Uygulama Güvenlik Duvarı)
- DLP (Veri Sızıntısı Engelleme Programı)
- Veri Tabanı Güvenlik Duvarları
- Kimlik Doğrulama Sistemleri
- Veri Tabanı Aktivite Monitörü
- Güvenlik Olay Yönetimi ve Korelasyon Sistemi
- DOS/DDOS Koruma Sistemleri
- E-Posta Güvenlik Sistemleri
- Sunucu ve İstemciler için Antivirüs Sistemleri
- URL Filtreleme ve Proxy Çözümleri
- NAC (Ağ Erişim Kontrol Ürünleri)
- Kurumsal Mobil Cihaz Yönetim Çözümleri
- Güvenlik Operasyon Merkezleri (SOC Çözümleri)
- Veri Sınıflandırma Ürünleri
- Veri Tabanı Şifreleme Çözümleri
- Disk ve Dosya Şifreleme Çözümleri
- İkincil Faktör Doğrulama Çözümleri
- Zafiyet Yönetimi Araçları
- APT (Hedef Odaklı Saldırı) Koruma Çözümleri
- DNS Güvenlik Çözümleri
- E-Posta ve Dosya Arşivleme Çözümleri
- Ağ İzleme Sistemleri
- VDI (Sanal Masaüstü Altyapısı) Sistemleri
- Yük Dengeleme Sistemleri
- VPN Sistemleri
- Elektronik Kasa Sistemleri

Teknolojik gelişmelerle birlikte güvenlik ürünlerin çeşitliliği artmakta ve bilgi güvenliği risklerinin yönetimi için kullanılmaktadır. Süreç faktörlü bilgi güvenliği risklerinin giderilmesi için de karşımıza standartlar, yasal düzenlemeler, COBIT vb. çerçeveler çıkmakta ve süreç kaynaklı bilgi güvenliği risklerinin azaltılması sağlanmaktadır. İnsan kaynaklı bilgi güvenliği risklerinin giderilmesi için ise kuşkusuz en önemli faaliyet çalışanların ve yönetimin bilgi güvenliği farkındalığı seviyesinin yükseltilmesidir.

Bilgi güvenliği ile ilgili riskleri aşağıdaki şekilde kaynak biçimlerine göre de sınıflandırabiliriz. [51]

- Teknoloji kaynaklı riskler
- İnsan kaynaklı riskler
- Süreç kaynaklı riskler
- Fiziksel riskler
- Dokümantasyon kaynaklı riskler

Bilgi güvenliği yönetişimi neden gereklidir sorusuna verilecek en temel yanıt bilgi güvenliği risklerinin giderilmesi için kurumsal yönetişimin bir parçası olarak, yönetim kurulu düzeyinde desteğin ve farkındalığın sağlanması, sorumluluk alınmasıdır.

III. BİLGİ GÜVENLİĞİ YÖNETİŞİMİ NASIL DAHA ETKİN OLUR?

Bilgi güvenliği yönetişimin dört tane temel unsuru vardır.

- Üst Yönetim taahhüdü (Desteği, Sorumluluğu)
- Güvenlik vizyonu ve stratejisi
- Bilgi güvenliği yönetimi yapısı
- Eğitim ve farkındalık

Bilgi güvenliği risklerinin proaktif olarak yönetilmesi için;

- Farklı tehdit seviyelerine göre etkin olan bir güvenlik mimarisi oluşturulmalıdır.

[51] Bilge Karabacak, ISO/IEC 27001:2005 ve Bilgi Güvenliği Yönetişimi – Türkiye Analizi, TÜBİTAK BİLGEM, 2008

- Endüstrinin ve düzenlemelerin belirlediği içeriğe göre mevcut durumun ortaya çıkarılması için GAP (boşluk) analizleri yapılmalıdır.
- İş hedefleriyle uyumlu bir güvenlik stratejisi ve vizyonu oluşturulmalıdır.
- Bu güvenlik stratejisi ve vizyonu eyleme dönüştürülmelidir.[52]

A- GÜVENLİK MİMARİSİNİN OLUŞTURULMASI

Kurumun bilgi güvenliği yönetişimi için insan, süreç ve teknoloji ile bütünleşik bir güvenlik mimarisi oluşturulması gerekir. Güvenlik mimarisinin oluşturulması sadece teknolojik önlemler ve yatırımlarından ziyade, güvenlik uygulamalarının iş hedefleriyle uyumlu hale getirilmesini sağlayacaktır. Kurulan bu güvenlik mimarisi, diğer bölümlerle de iletişim halinde olan bir hiyerarşik sistem olmalı, her seviyede izlenen, sektöre göre kıyaslanan ve karşılaştırılan bir yapı olmalıdır.[53]

B- GÜVENLİK YÖNETİMİNİN PERFORMANSININ ÖLÇÜLMESİ

Güvenlik ile ilgili olarak performansın ölçülmesi konusunda güvenlik metrikleri ve KPI'ların önemli bir yeri vardır. Bu konuya ilerleyen kısımda daha ayrıntılı değineceğiz. Burada güvenlik metriklerinin temel özelliklerinin neler olması gerektiğini kısaca ifade etmemiz gerekirse;

- Güvenlik metrikleri kurumun amaçlarına ulaşılmasını sağlayacak biçimde ölçülmeli, izlenmeli ve raporlanmalıdır.
- Güvenlik metriklerinin ölçülmesiyle güvenlik yönetiminin performansı kaynakları doğru yerlere ayırmayı sağlayacaktır.
- Etkin bir bilgi güvenliği yönetişimi bir gecede kurulabilecek bir sistem değildir. Doğru ve yeterli bir ölçümlemeyle beraber sürekli iyileştirilmeli ve desteklenmelidir.[54]

[52] Information Security Governance, Guidance for Boards of Directors and Executive Management, 2nd Edition IT Governance Institute, USA, 2003 s.29
[53] a.g.e.
[54] Information Security Governance, Guidance for Boards of Directors and Executive Management, 2nd Edition IT Governance Institute, USA, 2003 s.30

C- MEVCUT ORTAMIN DEĞERLENDİRİLMESİ

GAP(boşluk) analizleri ISO/IEC 27001 BGYS'nin de koşullarından biridir. İyi bir bilgi güvenliği yönetişimi için de mevcut ortamın değerlendirilmesini sağlayan GAP analizleri gerekmektedir.

Bilgi güvenliği yönetişimi için GAP analizlerinde cevaplanması gereken bazı noktalar:[55]

- Güvenlik yönetimi içinde karar verme ve raporlamayı sağlayan bir yapı var mı?
- Güvenlik aktiviteleri iş hedefleriyle uyumlu mu?
- Güvenlik politika, prosedür ve standartları doğru kaynaklar kullanılarak mı üretilmiş?
- Güvenlik organizasyonu kurum için yeterli bir rehberlik sağlayabiliyor mu?
- Güvenlik ve gizlilik BT süreçlerinin bir parçası mı?
- Bilgi güvenliği olay yönetimi etkin bir şekilde işletiliyor mu?
- Güvenlik altyapısı ve mimarisi doğru bir şekilde kurulmuş ve işletiliyor mu?
- Güvenliğin operasyonel tarafı kurum ihtiyaçlarını karşılıyor mu?

D- İŞ HEDEFLERİYLE UYUMLU BİR GÜVENLİK STRATEJİSİ

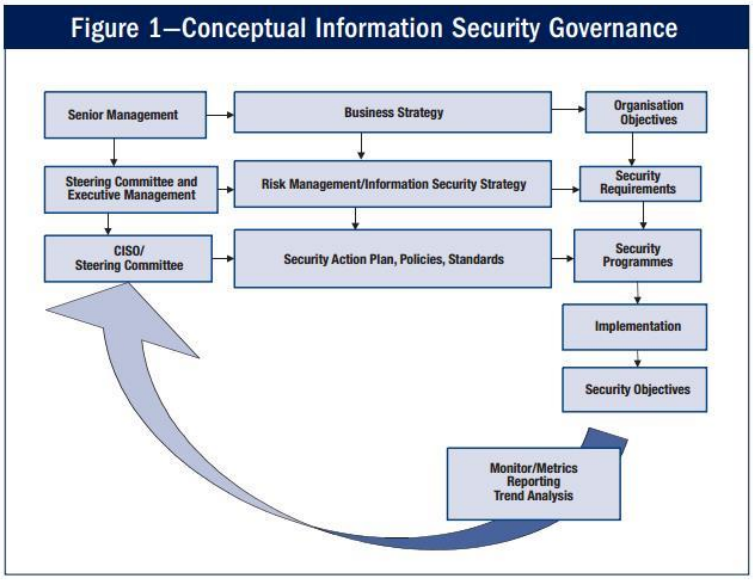
Bilgi güvenliği yönetişimi için kurumun bir güvenlik stratejisine sahip olması gerekmektedir. Bu güvenlik stratejisi oluşturulurken; GAP analizleriyle ve kurumun güvenlik kapasitesinin olgunluk seviyesinin değerlendirilmesi, kurum açısından yüksek öncelikli risklerin analiz edilmesi, ihtiyaçların ve kaynakların belirlenmesi ve kurumun iş hedefleri, stratejisi ve vizyonuna uygun bir güvenlik stratejisi geliştirilmeli ve dokümante edilmelidir.[56]

Bu belirlenen stratejiye uygun olarak da düzenli olarak ileride değineceğimiz bilgi güvenliği planı oluşturulmalıdır.

[55] Information Security Governance, Guidance for Boards of Directors and Executive Management, 2nd Edition IT Governance Institute, USA, 2003 s.37
[56] Information Security Governance, Guidance for Boards of Directors and Executive Management, 2nd Edition IT Governance Institute, USA, 2003 s.29

IV. BİLGİ GÜVENLİĞİ YÖNETİŞİMİ MODELİ

Bilgi güvenliği yönetişimi; kurumun stratejilerine uygun bir bilgi güvenliği yönetim modelinin sağlanmasını gerektirir. Aşağıda yer alan şekil bilgi güvenliği yönetişimi için örnek bir gösterimdir.



Şekil 10- Kurumsal Bilgi Güvenliği Yönetişim Süreci [57]

Örnek bir bilgi güvenliği yönetişimi modeli için en önemli kavramlardan birinden bahsetmemiz gerekiyor.

A- CISO/CSO

CISO (Chief Information Security Officer) ve CSO (Chief Security Officer) bilgi güvenliği yönetişimi için örnek bir modelde büyük önem arz etmektedir. Kısaca güvenlikten sorumlu başkan veya bilgi güvenliğinden sorumlu başkan olarak açabiliriz. CISO/CSO kurumda bilgi güvenliğinden sorumlu olan üst düzey yöneticidir ve Yönetim Kurulu'na bilgi güvenliği ile ilgili konuları aktarmaktan, bilgi güvenliğinin sürdürülmesinden sorumludur.

[57] Information Security Governance, Guidance for Boards of Directors and Executive Management, 2nd Edition IT Governance Institute, USA, 2003 s.19

CISO ve CSO'lara ihtiyaç duyulmasının en önemli sebeplerinden biri olarak CIO veya CTO'ların bilgi güvenliği konusunda yeterli zamana, efora ve hatta bilgiye sahip olmamalarıdır. Bu nedenle de sadece bilgi güvenliği konusuna odaklanmış, konu hakkında deneyimli, bilgili ve yetkin bir rol, bilgi güvenliği yönetişimin sağlanması açısından son derece kritik ve önemlidir.[58]

CSO/CISO'lar bilgi güvenliği konusunda derin bilgiye sahip olabilmekte, bilgi güvenliği risklerini çok daha iyi analiz edebilme şansına sahiptirler. CISO/CSO'lar aynı zamanda bilgi güvenliği zafiyetleri, tehditleri konusunda geniş bir perspektife de sahiptirler. Bu yetkinlikleri sadece teknoloji ile ilgili değildir. Bu yetkinlik de CSO veya CISO'ların kurumlar için önemini artırmaktadır.

CSO ve CISO'ların görev tanımları arasında; bilgi güvenliğinden kaynaklanabilecek riskleri azaltmak, iş sürekliliğini sağlamak, veri kayıplarını önlemek, gizlilik ve dolandırıcılık gibi konularda önlemler almak yer alıyor. Bunun yanı sıra CISO ve CSO'lar kurumun stratejileriyle uyumlu bir bilgi güvenliği yönetişimin sağlanmasından sorumlu olan kişilerdir. Bazı kurumlarda CSO ve CISO'lar CIO ya da CTO'lara bağlı olarak çalışabilmektedir. Fakat CEO'lara bağlı olması kurumsal bilgi güvenliği yönetişimi açısından daha kabul edilebilir ve doğru bir yönetişim şeklidir.

CISO ve CSO'ların fonksiyonları arasında bilgi güvenliği ile ilişkili olarak aşağıdaki konuları sıralayabiliriz:

- Gelişen teknolojiler ve pazar eğilimleri
- Kimlik ve erişim yönetimi
- Olay ve kriz yönetimi
- Bilgi ve gizliliğin korunması
- Risk ve uyum yönetimi
- Güvenlik mimarisi
- Kurumsal esneklik programları ve değerlendirmeleri
- Tehdit, istihbarat ve güvenlik zafiyet yönetimi

[58] Sharon Florentine, Why you need a CSO/CISO? http://www.cio.com/article/3048074/careers-staffing/why-you-need-a-cso-ciso.html

B- GÜVENLİK KOMİTESİ/FORUMU

Bilgi güvenliği yönetişimi modeli için bir başka önemli unsur da güvenlik komitesidir. ISO/IEC 27001'in de gerekli gördüğü güvenlik komitesi/forumu, örnek bir bilgi güvenliği yönetişimi modelinde kritik ve etkin bir roldür. Güvenlik komitesi; kurumun farklı unsurlarını bir araya getirerek kurumsal stratejilerine uyumlu bir bilgi güvenliği yönetişiminin sağlanmasına katkıda bulunur. Güvenlik komitesi sayesinde bilgi güvenliği kaynaklı risklerin giderilmesi daha kolay hale gelecektir.

Güvenlik komitesinin görevleri olarak aşağıdaki başlıkları sıralayabiliriz:

- Kurumun itibarını, iş sürekliliğini etkileyecek bilgi güvenliği risklerine karşı alınacak önlemlerin belirlenmesi
- Kurumun stratejilerine uygun bilgi güvenliği yönetim modelinin belirlenmesi
- Yönetim kuruluna bilgi güvenliği ile ilgili önem arz eden konuların iletilmesi
- Güvenlik metriklerinin değerlendirilmesi

Bilgi güvenliği yönetişimin etkin olarak yürütülmesi için gerek CISO/CSO rolleri gerekse de güvenlik komitesi/forumunun varlığı kritik önem arz eden organizasyon birimleridir.

Yukarıda belirttiğimiz roller dışında bilgi güvenliği yönetişimi ile ilgili olarak önem arz eden bazı hususlardan daha bahsedilmesi gerekiyor.

V. BİLGİ GÜVENLİĞİ YÖNETİŞİMİ İÇİN KURUMSAL ORGANİZASYON

Bilgi güvenliği yönetişimi açısından sonuç bölümünde değerlendireceğimiz kurumsal organizasyon yapısı üzerinde bu kısım içerisinde değinmek istiyoruz. Bu bizim için hem insan faktörü açısından daha bir değerlendirme hem de teknoloji-süreç faktörleri açısından bir değerlendirme imkanı sunacak.

Kurumların bilgi güvenliği yönetişimi için farklı organizasyon modelleri bulunuyor. Çalışmada bunu iki model üzerinde değerlendirmek istiyoruz; Merkezi bir yönetim modeli ve dağıtık bir yönetim modeli şeklinde. Değindiğimiz bilgi güvenliği yönetişim kuşkusuz bilgi güvenliğinden sorumlu ekipleri bünyesinde barındıran kurumlar için olacak. Aksi hallerde yönetilen kurumlar için bir bilgi güvenliği yönetişiminden zaten söz edemeyiz.

Değinmeye çalışacağımız organizasyon yapıları süreçler ve teknolojilerin kullanımı açısından olmayacak sadece. Çalışmanın her aşamasında bahsettiğimiz gibi insan faktörünün merkezi ve dağıtık olarak değerlendirilmesi olarak ele almak daha yerinde olacaktır.

A- MERKEZİ BİLGİ GÜVENLİĞİ ORGANİZASYONU

Merkezi bir bilgi güvenliği yönetişim modelinde tüm güvenlik teknolojilerinin, güvenliğe dair tüm süreçlerin ve güvenlikten sorumlu bilgi güvenliği çalışanlarının tek bir organizasyonda yer almaları. Bu modelde genel olarak CISO veya CSO dediğimiz ve yukarıda bahsettiğimiz bilgi güvenliğinden sorumlu bir başkanın yer alması ve başkanın CIO'ya direk bağlı olmasıdır. Bu tip bir yapıda güvenlik operasyonlarını yapan birimler ile güvenlik yönetişimini yapan birimler aynı çatı altında olmaları beklenebileceği gibi farklı bir yapı da söz konusu olabilir.

Merkezi bilgi güvenliği organizasyonunda tüm süreçler tüm teknolojiler ve tüm insan kaynağının tek bir başkan altında toplanmış olmasının çeşitli avantajları vardır. Böyle bir yapıda bilgi güvenliğinden sorumlu bir başkanın olması ve üst yönetime direk raporluyor durumda oluşu kurumda bilgi güvenliği farkındalığının artması ve daha iyi bir yönetişim ortaya çıkaracaktır. Bu yapıda BT ile bilgi güvenliği ekipleri farklı bir organizasyon yapısı altındadır ve temelde ulaşmaya çalıştığım sonuçta olduğu gibi güvenlik sadece bu birimlerin ve bu kişilerin sorumluluğu olarak değerlendirilecektir. Özellikle bilgi güvenliği teknolojileriyle ilgili çözümlerin tek bir bilgi güvenliği ekibi altında toplanmaya çalışılması önemli bir açmaz doğurur. Çünkü birçok BT çözümü güvenlik ile ilintilidir ve bunların tamamının güvenlik ekiplerinde yer alması beklenemez. Böyle bir yapıda başta güvenlik çözümleriyle ilintili diğer sistem/ağ ekipleri gibi altyapı ekipleri, yazılım ekipleri ve diğer çalışanlar sorumluluk almaktan kaçınabileceklerdir.

B- DAĞITIK BİLGİ GÜVENLİĞİ ORGANİZASYONU

Dağıtık bilgi güvenliği organizasyonlarında da yine bilgi güvenliğinden sorumlu bir başkan organizasyonda yer alabilir. Bu başkanın olması tüm güvenlik ekiplerinin tek bir çatı altında toplanmasını gerekli kılmaz. Böyle bir yapıda bilgi güvenliği yönetişimini yapan ekipler ile güvenlik operasyonlarını sürdüren ekipler ayrı organizasyonlar içinde yer alabilir.

Dağıtık olarak adlandırdığımız modelde Güvenlik Komitesi gibi kuruluşlar önem kazanır. Güvenlik Komitesi, bilgi güvenliği yönetişiminin sağlanmasında tüm kurumun katılımını sağlar. Dağıtık bir modelde roller ve sorumluluklar her bölüme daha çok yansıtılmış olur. Diğer BT ekipleri de bilgi güvenliği sürecinin dışında kalmayacaklardır. Dağıtık bir modelden kast ettiğimiz daha çok bilgi güvenliği rol ve sorumlulukların dağıtık hale getirilmesidir. Aksi halde sadece güvenlik teknolojilerinin ve süreçlerinin dağıtık veya merkezi olması arasında önemli bir fark olmayacaktır.

VI. BİLGİ GÜVENLİĞİ YÖNETİŞİM UYGULAMASI

Kurumların bilgi güvenliği yönetişimi sağlamakta uygulamaları gereken ve iyi bir yönetişim için gerekli olan bazı konular bulunuyor. Bu kısımda bunlardan bahsedeceğiz.

A- BİLGİ GÜVENLİĞİ PLANI

Bilgi güvenliği planı COBIT 4.1'de DS5-Sistem Güvenliğinin Sağlanması domainin 11 kontrol maddesinden biridir ve oldukça önemlidir. Çünkü kurumun bir sonraki yıl için bilgi güvenliği ile ilgili yapacakları bu plan içerisinde yer alır.

Bilgi güvenliği planı; kurumun iş hedefleri, güvenlik ve uyum gereksinimlerinin dikkate alınarak oluşturulduğu ve periyodik olarak gözden geçirilmesi gereken bir plandır. Bilgi güvenliği planının oluşturulmasında göz önünde bulundurulması gereken süreçler ve konuları aşağıdaki şekilde özetlemek mümkündür:

- Kurumun stratejik planı ve iş hedefleri
- BT stratejik planı ve BT proje çalışmaları
- Uyum gereksinimleri
- Bilgi güvenliği politikaları
- Güvenlik riskleri
- Denetim bulguları
- Güvenlik metrikleri
- Güvenlik farkındalığı test sonuçları

- Bilgi sınıflandırma sonuçları ve veri güvenliği çalışmaları
- Güvenlik ile ilgili eğitim ihtiyaçları
- Gerçekleşen siber güvenlik olayları
- Bilgi sistemleri sızma test sonuçları
- Uygulama güvenlik testi sonuçları
- Sistemlerde yapılan zafiyet tarama sonuçları ve güvenli yapılandırma gereksinimleri
- Gerçekleşmesi muhtemel saldırılar
- Personel, yazılım, donanım ve servislerle ilgili kaynak ve yatırım ihtiyaçları
- Güvenlik altyapı gereksinimleri (ek kapasite, altyapı yenileme, konsolidasyon, güncel seviyelere yükseltme, performans problem çözümü)
- Kriptoloji ile ilgili gereksinimler
- Yeni nesil güvenlik çözümleri ile ilgili araştırma sonuçları

Bilgi güvenliği planın bazı çıktıları olması gerekmektedir. COBIT'e göre bir bilgi güvenliği planında;

- Güvenlik projeleri, aktiviteler, sorumluluklar, gerekli efor
- Bütçe (Yazılım, donanım, eğitim, iş sürekliliği, yenilenmesi gereken sözleşmeler, lisans)
- Güvenlik ekipleri tarafından diğer ekiplere verilecek proje desteği
- Bilgi güvenliği farkındalığı çalışmaları
- Eğitim planı
- Politika çalışmaları
- Test planı (Zafiyet taramaları, proje ve uygulama bazında yapılacak olan güvenlik testler)

Bilgi güvenliği planı yönetim tarafından onaylanmış ve desteklenmiş olmalıdır. Plan, gerektiği durumlarda güncellenmelidir. Bunun yanı sıra bilgi güvenliği planı tüm kurumu etkileyecek bir plan olduğu için diğer süreçlerle ilişki içerisinde olmalı ve plan oluşturulurken diğer BT süreçlerinin çıktılarından faydalanılmalıdır.

Bilgi güvenliği planının ilişkili olduğu BT süreçleri (COBIT 4.1'e göre):

- PO1 (Stratejik BT Planının Tanımlanması)
- PO2 (Bilgi Mimarisinin Tanımlanması)

- PO3 (Teknolojik Yönün Belirlenmesi)
- PO6 (Yönetim Amaçlarının ve Talimatlarının İletilmesi)
- PO9 (BT Risklerinin Değerlendirilmesi ve Yönetimi)
- ME3 (Dış Gereksinimlere Uyumun Sağlanması)
- AI1 (Otomasyon Çözümlerinin Belirlenmesi)
- AI2 (Uygulama Yazılımının Edinimi ve Bakımı)
- AI3 (Teknoloji Altyapısının Edinimi ve Bakımı)
- DS1 (Hizmet Seviyelerinin Tanımlanması ve Yönetimi)
- DS2 (Üçüncü Şahıslardan Alınan Hizmetlerin Yönetimi)
- DS9 (Konfigürasyon Yönetimi)

B- GÜVENLİK METRİKLERİ

Metrikler birçok süreçte olduğu gibi bilgi güvenliği açısından da oldukça önemlidir. Kurumların belirledikleri metrikleri ölçerek bilgi güvenliği olgunluk seviyelerini belirlemeleri, eksik alanları ve düzeltilmesi gereken noktaları ortaya çıkarmalarını sağlayacaktır.

Metriklerle beraber KPI'lardan da bahsedilmesi gerekmektedir. KPI (Key Performance Indicator) adını verdiğimiz anahtar performans göstergelerine de değinilmesi gerekmektedir. Burada metrik ve KPI kavramları arasındaki farka değinmemiz lazım. Her metrik bir KPI'dır, ancak her KPI bir metrik değildir. KPI'lar daha metriklere göre daha kritik ve önemli göstergelerdir.

İyi metriklerin özellikleri aşağıdaki şekilde yer almaktadır:

Şekil 11- İyi metriklerin özellikleri

Güvenlik metrikleri farklı kategorilerde sınıflandırılabilir. Teknik önlemlere göre aşağıdaki dört gruba güvenlik metriklerini ayırabiliriz:

- Sınır güvenliği
- Kapsama ve kontrol alanı
- Süreklilik
- Uygulama güvenliği

Güvenlik metriklerinin izlenmesi kurumun bilgi güvenliği yönetişim için oldukça kritik öneme sahip demiştik. Bu metriklerin güvenlik ekipleri tarafından ölçülüyor ve izleniyor olması yeterli değildir. Bilgi güvenliği yönetişiminin sağlanması için güvenlik metriklerinin üst yönetime raporlanıyor olması büyük öneme sahiptir. Bu raporlama üst yönetişimin sorumluluk almasını ve aksayan yerlerin düzeltilmesine sebep olacaktır.

C- BİLGİ GÜVENLİĞİ POLİTİKALARI

Kurumun bilgi güvenliği yönetişimi modelinde gerçekleştirmesi gereken kritik ve öncelikli konuların başında bilgi güvenliği politikalarının oluşturulması, yayımlanması ve uygulanması gelmektedir. Gerek ISO/IEC 27001, gerek COBIT gibi standartlar, gerekse de bankacılık bilgi sistemlerini düzenleyen İlkeler Tebliği gibi yasal düzenlemeler bilgi güvenliği politikalarının

bir kurumda mutlaka yer almasını ve bunun üst yönetimin sorumluluğunda olduğunu açıkça ifade etmektedirler.

Bilgi güvenliği yönetişiminin üst yönetimin sorumluluğu olduğunu daha önce ifade etmiştik. Bilgi güvenliği politikaları, kurum üst yönetiminin bu sorumluluklarını yerine getirmelerinin en önemli adımlarından biridir ve belki en önemlisi olarak da ifade edilebilir.

Bilgi güvenliği politikaları; kurumun bilgi güvenliği yönetişimi konusundaki bakış açısını ve genel yaklaşımını ortaya koyarak, bilgi güvenliği ekiplerinin kurumda politikada yer alan kuralları uygulamalarıyla ilgili iradelerini ortaya koymalarını sağlamaktadır.

Bilgi güvenliği politikaları kurumlarda farklı şekillerde uygulanabilmektedir. Bazı kurumlar tek bir bilgi güvenliği politikası yazmakta, bazı kurumlar ise farklı konularda birden çok bilgi güvenliği politikası yazma yoluna gitmektedirler. Bilgi güvenliği politikaları sadece bilgi güvenliği ekiplerinin ya da BT ekiplerinin sorumluluğunda olan kurallar seti değildir. Çoğu zaman kurumlarda bu durum tam anlaşılamamakta ve sadece bilgi güvenliği ekiplerinin sorumluluğuymuş gibi algılanmaktadır. Bu son derece büyük bir hatadır. Bilgi güvenliğinden tüm kurum çalışanlarının sorumludurlar. Bu nedenle de bilgi güvenliği politikaları tüm kurum çalışanlarını ilgilendirir, tüm kurum çalışanlarının okuması ve uygulaması gereken dokümanlardır.

Tüm çalışanların sorumluluğunda olan bilgi güvenliği politikaları bu nedenle anlaşılır ve uygulanabilir olmak zorundadır. ISO/IEC 27001 BGYS sistemi kurulurken bilgi güvenliği politikası oluşturulmasını şart koşar ancak tüm çalışanların bu politikayı okumalarının zor olması nedeniyle özet bir bilgi güvenliği politika el kitabı oluşturulmasını tavsiye eder.

Bilgi güvenliği politikaları için önereceğimiz yaklaşım; tüm çalışanların okuyabilecekleri ve anlayacakları bir üst seviye kurumsal bilgi güvenliği politikasının oluşturulmasıdır. Bu üst seviye kurumsal bilgi güvenliği politikasıyla beraber de alt güvenlik politikaları oluşturulmalıdır. Bu bahsettiğimiz alt bilgi güvenliği politikaları da kurum çalışanları tarafından bilinen dokümanlar olmalıdır. Bilgi güvenliği ana ve alt politikalarının bir alt kademesinde ise BT ve güvenlik ekiplerinin sorumluluklarını anlatan teknik bilgi güvenliği politikaları ve prosedürleri yer alır ve böylece bilgi güvenliği politika hiyerarşisi oluşturulmuş olur.

Bilgi güvenliği politikası olarak yazılabilecek çok sayıda konu vardır. Bunlardan bazılarını örnekleyebiliriz:

- Elektronik posta güvenliği politikası
- Firewall politikası
- Kimlik doğrulama ve erişim kontrol politikası
- İnternet erişim politikası
- Mobil cihaz güvenliği politikası
- Bilgi varlıkları yönetim politikası
- Parola politikası
- Operasyon güvenliği politikası
- Ağ güvenliği politikası
- Antivirüs politikası
- İnsan kaynakları güvenliği politikası
- Fiziksel ve çevresel güvenlik politikası
- Veri koruma politikası

Bu politikalar alt politika veya teknik politikalar olarak oluşturulabilir. Çok daha farklı güvenlik ile ilgili konular da yer almakta, bunlar için ayrı politikalar da oluşturulabilmektedir. Fakat unutmamak gerekir ki tüm çalışanların bilgi güvenliği politikalarını okumaları, uygulamaları ve takip etmeleri zordur. Bu nedenle bilgi güvenliği politikaları mümkün olduğunca; kısa, öz, anlaşılır ve ne olması gerektiğini yazmalıdır. Nasıl olması gerektiği üst seviye politikaların değil teknik politikaların işidir.

D- BİLGİNİN SINIFLANDIRILMASI VE ETİKETLENMESİ

Bilgi güvenliğinin temel hedefi bilginin korunmasıdır. Bilginin korunmasının öncelikli yöntemi ise hangi bilginin daha kritik olduğunu belirlemekle başlar. Bilgiyi koruyacağız fakat bilgi kurumda nerede yer alıyor sorusuna yanıt bulunması gerekiyor. Bilginin nerede olduğunu belirlendikten sonra ise bilgi; gizlilik, bütünlük ve erişilebilirlik açısından değerlendirilmeli ve önceliklerine göre sınıflandırılmalıdır.

Bilgi sınıflandırma yapılmadan bilgi güvenliği sağlamaya çalışmak; eksik, yetersiz ve kurumsal olmaktan uzaktır. Bu durum kurumun kaynaklarının boşa heba edilmesinin yanı sıra asıl riskin nerede olduğunun gözden kaçırılması sonucunu da doğuracaktır. O halde öncelikli olan bilginin kurumda keşfedilmesi, sonrasında ise sınıflandırılmasıdır.

Sınıflandırılmış bilgi için bir sonraki aşama etiketlenmesidir. Bilginin korunması için etiketleme mutlaka yapılması gerekmektedir. Bu noktada bilginin sınıflandırılması ve etiketlenmesi için bilginin bulunduğu yerlerden bahsedilmesi gerekir.

Bilginin korunması için verilerin iki türlü olduğunu açıklamalıyız. Veriler; yapısal veriler ve yapısal olmayan veriler olmak üzere ikiye ayırabiliriz.

Yapısal veriler; veri tabanı ortamlarında yer alan veriyi anlatmaktadır. Yapısal olmayan veriler ise veri tabanı ortamlarında yer almayan; dosya sunucularında, bilgisayarlarda, akıllı cihazlarda, intranet ortamlarında yer alan verileri kast etmektedir. Fiziksel ortamlarda yer alan veriler de yani print edilmiş (kâğıt ortamda yer alan veriler) veriler de yapısal olmayan veriler kategorisinde değerlendirilir.

Yapısal ve yapısal olmayan veriler için farklı sınıflandırma araçları kullanılmaktadır. Ancak yöntemleri farklı dahi olsa her iki veri türü için de bilgi sınıflandırması yapmak mühimdir.

Etiketleme için en çok kullanılan türleri ise aşağıdaki şekilde belirtebiliriz. Bu etiket türleri kurumların ihtiyaçlarına göre azaltılabilir ya da artırılabilir.

- Gizli
- Sınırlı Erişim
- Hizmete Özel
- Kurum içi
- Genel

§ 8. BÖLÜM

BİLGİ GÜVENLİĞİ FARKINDALIĞI

Bilgi güvenliği için üç önemli faktörden bahsetmiştik. Bunlar; teknoloji, insan ve süreçtir. Bilgi güvenliği ancak bu üç faktörün beraber değerlendirilmesiyle sağlanacaktır. Burada belki de en önemli faktör olarak insan faktörünü görmek mümkün. Bir zincirin en zayıf halkası kadar güçlü olduğu söylenir. İnsan faktörü de bilgi güvenliğinin en zayıf faktörü olarak karşımıza çıkmaktadır.

Kurumlarda hem çalışanların hem de üst yönetimin bilgi güvenliği farkındalığı seviyelerinin artırılması gerekmektedir. Ancak bu sayede kurum daha güvenli hale gelebilir. Bu nedenle de kurumlar, çalışanlarının bilgi güvenliği farkındalıklarını artırmak için başta eğitimler olmak üzere çeşitli çalışmalar yapmaktadırlar.

Bilgi güvenliği farkındalığı ile ilgili olarak yapılan bazı çalışmalar:

- Yerinden sınıf içi eğitimler
- Uzaktan eğitimler
- Bilgi güvenliği e-posta duyuruları
- Bilgi güvenliği intranet sayfaları
- Sosyal mühendislik ve oltalama testleri
- Kurum içi afişler, posterler, kartlar
- Seminerler ve paneller
- Bilgi güvenliği günleri

Çalışanların bilgi güvenliği farkındalığı seviyesinin artırılması, iyi bir bilgi güvenliği yönetişimi için son derece önemlidir. Sonuç bölümünde değineceğimiz bilgi güvenliği yönetişimi yaklaşımı için de başta ayrıcalıklı yetkilere sahip kullanıcılar olmak üzere tüm kurum çalışanlarının bilgi güvenliği farkındalıklarının yüksek olması gerekmektedir. Burada bilgi güvenliği farkındalığı eğitimi içeriği konusuna değineceğiz.

I. BİLGİ GÜVENLİĞİ GENEL KAVRAMLAR

Bilgi güvenliği genel kavramlar başlığı altında aşağıdaki konu başlıkları üzerinde durulmalıdır.

- Bilgi nedir?
- Bilgi Nerede Bulunur?
- Bilgi güvenliği nedir ve neden önemlidir?
- Bilgi güvenliğinin Temel Unsurları
- Bilgilerimizi kaybedersek ne olur? (Para kaybı, zaman kaybı, itibar kaybı, suçlanmak, operasyonel kayıplar vb. kayıplar)

Bilgi güvenliği ile ilgili genel kavramların neredeyse tamamına 2.bölümde değindiğimiz için burada detaya girmeyeceğiz.

II. SOSYAL MÜHENDİSLİK

Günümüzde bilgi güvenliği farkındalığı ile ilgili en önemli konuların başında sosyal mühendislik gelmektedir. Sosyal mühendislik saldırıları, bilgi güvenliği ihlal olaylarında en çok kullanılan yöntemlerin başında geliyor. Sosyal mühendislik eğitimlerinde yer alması gereken konu başlıkları ve eğitim içeriğinde olması gerekenler:

- Sosyal Mühendislik nedir?
- Sosyal mühendislik saldırıları nasıl gerçekleşir?
- En çok kimler hedef olabilirler?
- Sosyal mühendisler, insanların hangi zaaflarından faydalanırlar?
- İnsanlar; kendilerine mail, yüz yüze, telefon vs. gibi yöntemlerle ulaşan sosyal mühendisleri nasıl tanıyabilirler?
- Sosyal mühendislik saldırıları ile karşılaştıklarında ne yapmaları gerekir?

A- SOSYAL MÜHENDİSLİK NEDİR?

Sosyal Mühendislik; insanların zafiyetlerinden faydalanarak, çeşitli ikna ve kandırma yöntemleriyle istenilen bilgileri elde etmeye çalışmaktır. İnsanların karar verme süreçlerini

değiştirmeye yönelik teknikler içerir. Sosyal Mühendislik saldırılarını çoğu kez anlaşılamayabilir.

Sosyal Mühendisler aşağıdaki teknikleri sıklıkla kullanırlar:

- Güven uyandırmak
- Yardım teklif etmek – Size yardım edebilirim
- Yardım istemek – Bana yardımcı olabilir misiniz?
- Sahte siteler oluşturmak ve zararlı ekler göndermek
- Acındırma, suçluluk hissi yaratma veya baskı altına almak

B- SOSYAL MÜHENDİSLİK SALDIRILARI NASIL GERÇEKLEŞİR?

1. Sahte Senaryolar Uydurmak

Genellikle telefonla iletişim üzerinden gerçekleşen bir yöntemdir. Saldırgan amacına ulaşmak için sahte bir senaryo oluşturur. Bu senaryonun ardından saldırgan, hedefteki kritik ve hassas bilgiye (bir sonraki adımda kullanmak üzere kişisel bilgiler, şifreler gibi erişim bilgileri) ulaşması şeklinde gerçekleşir.

2. Güvenilir Bir Kaynak Olduğuna İkna Etmek

Saldırgan, amacına ulaşmak için saldırılanı güvenilir ya da doğruluğu sorgulanamaz bir kaynaktan geldiğine inandırır. Burada e-posta, telefon ve hatta yüz yüze olmak üzere çeşitli yöntemler kullanılabilir. Kendisini güvenilir bir kaynak olarak gösteren saldırgan bu sayede saldırı öncesi bilgi de toplayabilir, saldırıyı da gerçekleştirebilir.

3. Güven Kazanma Yöntemiyle Bilgi Edinmek

Saldırganın hedefine; işte veya iş dışında hedefinin güvenini sağlayacak şekilde iletişime geçerek ikna etmesi, hedefinden bu şekilde bilgi alması ve istediklerini yaptırmasına dayalı bir yöntemdir.

4. Truva Atları (*Trojanlar)* Kullanmak

Zararsız görünen ancak aslında zararlı olan yazılımlar bu özelliklerinden dolayı Truva atı olarak adlandırılırlar. Truva atları; güvenli olmayan kaynaklardan, bilinen bir yazılım görünümünde indirilen programlarla, internetten indirilen dosyalarla ya da kimliği belirsiz veya şüpheli kaynaklardan gönderilen yazılımlar aracılığıyla hedefteki sistemlere yerleştirilebilmektedir.

5. Diğer Yöntemler

Omuz sörfü: Saldırgan tarafından hedefteki kişi şifresini yazarken ya da kritik sistemlere erişim esnasında hedefin izlenmesi yöntemidir

Çöp karıştırmak: Çöp karıştırma da bir sosyal mühendislik yöntemidir. Çöpe atılmış disket, CD, post-it, imha edilmemiş kâğıt vb. hassas ve kritik bilgi içerebilecek araçları ya da dokümanları inceleme yöntemidir.

Eski donanımları kurcalamak: Hurdaya çıkarılmış, ikinci el e-ticaret sitelerinde satışa sunulmuş, çöpe atılmış, kullanılmadığı için hibe edilmiş donanımların içerikleri incelenerek de sosyal mühendisler bilgi toplamaktadırlar.

C- EN ÇOK KİMLER HEDEF OLABİLİR?

Sosyal Mühendislik saldırılarında, saldırganlar her çalışanı hedef alabilir ancak bazı çalışanlar daha fazla hedef haline gelmektedir.

- Direkt ulaşılabilir personel (Servis elemanları, telefonlara yanıt veren çalışanlar)
- Önemli personel (Yöneticiler, gizli bilgiye erişim hakkı olan personel)

- Sempati sahibi personel
- Destek ihtiyacındaki son kullanıcılar:
- Kandırılmış, aldatılmış ya da ikna edilmiş personel

D- SOSYAL MÜHENDİSLİK YÖNTEMLERİ

Sosyal Mühendislik saldırılarını gerçekleştiren kişilerin sıklıkla başvurduğu ve büründükleri bazı roller vardır. Bunlara kısaca değinmek gerekir.

Sosyal mühendislerin kullandıkları yöntemlerden ilki otoriter bir yaklaşım göstermektir. Kendilerini; yetkili, üst düzey yönetici veya ayrıcalık bir müşteri gibi göstererek karşıdaki kişiyi etkilemeye ve ikna etmeye çalışırlar.

Bir başka yöntem ise yardım önermektir. Sosyal mühendisler; desteğe ve yardıma ihtiyacı olan müşteri veya çalışanları, kendilerinin yetkili bir personel olduğuna ikna etmeye çalışırlar. Sosyal mühendisler, çalışanlarla aralarında gerçekte olmayan çeşitli sosyal bağlantılar oluşturmayı da denerler. Bunlar arasında; akrabalık, ortak arkadaş veya meslek vb. sayılabilir.

İstenen bir iyilik için karşılık önermek, kuruma bağlı bir çalışanı isteğinin yapılmaması durumunda kuruma zarar vereceğine ikna etmek veya kuruma bağlılığı yeterince güçlü olmayan bir çalışanı çeşitli kandırma ve aldatma yöntemleriyle ikna etmek sosyal mühendislerin kullandıkları diğer yöntemler arasında sayılabilir.

III. OLTALAMA

Oltalama konu başlığı altında bilgi güvenliği farkındalığı eğitimlerinde aşağıdaki konulara değinilmeli ve çalışanların bu konularla ilgili farkındalık seviyelerinin yükseltilmesi sağlanmalıdır.

- Oltalama nedir?
- Oltalama saldırıları nasıl anlaşılır?
- Oltalama saldırılarında kullanılan yöntemler nelerdir?
- Korunmak için nelere dikkat etmeli?

- Oltalama e-postaları nasıl anlaşılır?
- Tuzağa düştüğünüzü fark ettiğinizde ne yapmalısınız?

Oltalama (phishing) aslında bir sosyal mühendislik türüdür. Ancak yaygınlığı ve elektronik ortamda yapılan bir saldırı türü olduğu için ayrı bir başlık olarak değerlendirilmesi daha isabetli olur.

A- OLTALAMA NEDİR?

Oltalama *(phishing)* saldırısında; saldırgan, hedefine e-posta göndererek saldırı gerçekleştirmektedir. Bu e-postalar, bilinen web sitelerinden veya kullanıcının hesabının bulunduğu bankadan gelmiş gibi görünmekte, kişisel bilgi girişi veya güncellemesi için e-postada bulunan linke tıklanması, ekinde gönderilen zararlı yazılım içeren ekli dosyayı açması istenmektedir. Bu sayede kurbanın bilgileri oltalama *(phishing)* saldırısını yapan kişiye iletilir veya zararlı içerik kurbanın bilgisayarına indirilmiş olur.

B- OLTALAMA SALDIRILARINDAN KORUNMA YOLLARI

Oltalama saldırılarından korunmak için en temel kural, bilmediğiniz bir kaynaktan gelen herhangi bir e-posta ekini veya e-posta gövdesinde yer alan linki açmamaktan geçiyor. Bunun yanı sıra; şifre, banka kartı, kişisel bilgi ve benzeri bilgileri e-postayla yönlendirildiğiniz sayfalara kesinlikle yazılmaması gerekmektedir. Çünkü hiçbir banka veya büyük kuruluş, kullanıcının kişisel bilgilerini e-posta yoluyla talep etmez.

Web sayfasının sol üst kısmında yer alan kapalı kilit işareti güvenli ve şifreli bir sayfada işlem yaptığınızı gösterir. Girdiğiniz web sitelerinin sol üst kısmında kapalı kilit işareti olup olmadığını kontrol edilmelidir. Ayrıca, e-postalardaki kısaltılmış URL linklerine (bit.ly,ow.ly, tinyurl.com, is.gd, goo.gl, tiny.cc, cli.gs vb.) tıklanmamalıdır.

C- OLTALAMA E-POSTALARI NASIL ANLAŞILIR?

Saldırganın e-postada gönderdiği link kurbanın hesabının olduğu kurumun veya bankanın linkine çok benzeyecektir. Bağlantıya tıklandığında açılan web sayfası kurbanın kullandığı web sayfasına çok benzeyecek şekilde tasarlanmış olacaktır. Bu nedenle bu şekilde bağlantı içeren e-postaların içerdiği bağlantılar konusunda dikkatli olunması ve adresin doğru olduğundan emin olunması gerekmektedir.

"Değerli Müşterimiz" gibi ifadeler ile başlayan e-postalar e-postayı gönderenin, hedef kişiyi tanımadığı anlamına gelir bu e-posta için dikkatli olunması gerekir. E-postanın içeriğinde acilen bir şeyler yapılması isteniyor ve "aksi takdirde hesabınız x süre içinde kapanacaktır" gibi ifadeler içeriyor ise bu tür e-postalar oltalama e-postaları olabilir bu nedenle e-postanın doğru adresten geldiğinden emin olunması gerekmektedir. E-postaya yanıtla dediğinizde yanıt adresi size e-posta gönderen adresten farklı ise dikkatli olunması gereken bir başka durumdur.

IV. PAROLA GÜVENLİĞİ

Bilgi güvenliğinin yine mühim konularından biri kimlik doğrulamadır. Kimlik doğrulama yöntemlerinin de en bilinen kullanım şekli paroladır. Parola güvenliği için bilgi güvenliği farkındalığı eğitimlerinde bulunması gereken konu başlıkları şu şekildedir:

- Parola(Şifre) güvenliği neden önemlidir?
- Güçlü parola nedir ve nasıl oluşturulur?
- Güçlü parola oluşturulurken dikkat edilmesi gerekenler
- Parola güvenliği için dikkat edilmesi gerekenler

A- GÜÇLÜ PAROLA NASIL OLUŞTURULUR?

Tahmin edilmesi kolay olmayan ya da deneme yanılma yolu ile ele geçirilmesi oldukça zor olan parolalara güçlü parola denir.

Güçlü parola nasıl oluşturulur?

- En az 8 karakterden oluşur.
- Harflerin yanı sıra, rakam ve "?, @, !, #, %, +, -, *, %" gibi özel karakterler içerir.
- Büyük ve küçük harfler bir arada kullanılır.

Her ne kadar parolaların yukarıda bahsettiğimiz özelliklerine uygun olsa da güçlü parola oluştururken yapılan bazı hatalara dikkat edilmesi gerekir.

- Kişisel bilgiler gibi kolay tahmin edilebilecek bilgiler parola olarak kullanılmamalıdır. (Örneğin; adınız, doğum tarihiniz, çocuğunuzun adı, soyadınız, ... gibi).
- Sözlükte bulunabilen kelimeler parola olarak kullanılmamalıdır.
- Çoğu kişinin kullanabildiği aynı veya çok benzer yöntem ile geliştirilmiş parolalar kullanılmamalıdır.

B- PAROLA GÜVENLİĞİ İÇİN DİKKAT EDİLMESİ GEREKENLER

Parola güvenliğiyle ilgili olarak unutulmaması gereken ilk şey; parolaların kişiye özel oldukları ve asla kimse ile paylaşılmaması gerektiğidir. Parolalar ofis, servis, telefon vb. hiçbir ortamda kimseye söylenmemelidir. Kurum çalışanlarının bunu unutmamaları gerekmektedir. Bunun yanı sıra;

- Parolalar kâğıda yazılarak monitöre, çalışma masasına veya benzer bir yere yapıştırılmamalı, bırakılmamalıdır.
- Parolalar bilgisayarlarda, akıllı telefonlarda bir yerlere kayıt edilmemelidir.
- Parolalar belli aralıklarla değiştirilmelidir.
- Farklı sistemlerde farklı parolalar kullanmaya özen göstermeli, her yerde aynı parola kullanılmamalıdır.

V. SOSYAL MEDYA KULLANIMI

Bilgi güvenliği farkındalığı eğitimlerine son dönemde giren ancak yaygın kullanımı nedeniyle önem arz eden bir konu sosyal medya kullanımıdır. Sosyal medya kullanımıyla ilgili aşağıdaki konulara bilgi güvenliği eğitimlerinde yer verilmelidir:

- Sosyal Medya'da bilgi paylaşımlarında nelere dikkat etmeli?
- Giriş için kullandıkları mail adresi nasıl olmalı?
- Kişisel bilgilerini paylaşırken nelere dikkat etmeliler ve gizlilik ayarları nasıl olmalı?
- Yer bildirimleri yapmanın ne gibi sakıncaları olabilir?

- Sosyal medyada oyun oynarken ya da uygulama kullanırken nelere dikkat etmek gerekir?
- Sosyal medyada gelen arkadaşlık teklifleri kabul edilmeli mi? nelere dikkat etmek gerekir?
- Sosyal Medyada arkadaşınız sandığınız kişi gerçekten arkadaşınız olan kişi midir?
- Sosyal medyada hakaret, küfür edilebilir mi? Ne gibi sakıncaları olabilir?
- Sosyal medyada paylaşılan bilgiler nasıl saldırı aracı olabilirler?

Sosyal medya kullanımıyla ilgili dikkat edilmesi gereken konulardan bazıları şunlardır:

- Sosyal Medya hesaplarında kişisel e-posta adresleri kullanılmalıdır. Kurumsal e-posta adreslerini kullanılmaması gerekmektedir.
- Sosyal medya hesaplarında güçlü parolalar kullanılmalıdır.
- Twitter, Facebook gibi sosyal medya ortamlarında önerilen gizlilik ayarlarını kullanılmalıdır.
- Kişiler, tanımadıkları insanları listelerine kabul etmemelidirler.
- Paylaşımlarda özel bilgilere mümkün olduğunca yer verilmemelidir (Telefon, e-mail, adres, finansal bilgiler, katılacağınız sosyal etkinlikler veya tatil ile ilgili bilgiler vb.).
- Uygulama davetleri genellikle risklidir. Kim senin profiline bakmış? X oyununda 100.000 altın kazanmak için bu uygulamayı indir gibi gönderilere itibar edilmemelidir.
- Kişiler; paylaştıkları içeriklerinden sorumlu olduğunu unutmamalıdır. Suç oluşturabilecek paylaşımlardan uzak durmaları gerekir.

VI. MOBİL CİHAZ GÜVENLİĞİ

Tıpkı sosyal medya gibi son yıllarda insanların hayatına giren ve giderek yaygınlaşan mobil cihazlar da çalışanların çok dikkat etmeleri gereken bir başka konu başlığıdır.[59]

A- KİŞİSEL MOBİL CİHAZLAR İÇİN GÜVENLİK

[59] https://tuketici.btk.gov.tr/File/?path=ROOT%2F2%2FDocuments%2FHaber%2Fsmartphone_sec_android.pdf

1. **Ekran koruyucusu kilidi kullanılmalıdır**

Telefonlardaki mail, resimler gibi kişisel verilerin yetkisiz kişilerin eline geçmesini engellemek için mutlaka PIN kullanılmalıdır.

2. **Cihazın temel güvenlik ayarlarını değiştirilmemelidir**

IOS işletim sistemlerinde "jailbreak", android işletim sisteminde "rooting" gibi işlemler telefonları farklı saldırılara karşı güvensiz hale getirecektir.

3. **Uygulamaları yalnızca güvenilir kaynaklardan indirilmelidir**

Jailbreak yapılan IOS telefonlarda farklı kaynaklardan da uygulama indirilebilmektedir. Aynı şekilde android işletim sisteminde de sadece google play gibi resmi uygulama indirme ortamlarından uygulama indirilmelidir.

4. **Güncellemeleri zamanında ve düzenli olarak yapılmalıdır**

Akıllı telefonlarda kurulu olan uygulamaları güncel tutulmalıdır. Uygulamaların güncel sürümleri keşfedilen hata ve güvenlik açıklarından arındırılmış olacaktır bu nedenle de daha kararlı çalışacaktır. Aynı şekilde üretici firma güncel işletim sistemi yayınlandığında işletim sisteminde güncellenmelidir.

5. **Ortak kullanıma açık kablosuz ağların kullanımında dikkat edilmelidir**

Ortak kullanıma açık kablosuz ağları kullanırken dikkatli olunması gerekir. Şifresiz herkese açık kablosuz ağ trafiği bu hizmeti bedava veren kişi tarafından dinleniyor olabilir. Şifresiz internetin kimin tarafından sunulduğuna emin olunan, güvenilir kablosuz ağları kullanılmalı veya mobil operatörlerin internet servisini tercih edilmelidir.

§ 9. BÖLÜM

SONUÇ

Bilgi güvenliği yönetişiminin kurumlarda sağlıklı ve verimli gerçekleştirebilmesinin en öncelikli koşulu üst yönetim desteğidir. Bu desteğin Yönetim Kurulu seviyesinde olması gerekmektedir. Üst yönetimin bilgi güvenliğini sahiplenmesi, sorumluluk üstlenmesi, destek vermesi halinde ancak kurumsal bilgi güvenliği yönetişimi sağlanabilecektir.

Kuşkusuz bu ilk koşul olmakla birlikte yeterli bir koşul değildir. Üst yönetimin sahiplenmesi de kadar tüm çalışanların ve diğer paydaşların kurumsal bilgi güvenliği yönetişimine inanmaları ve sahiplenmeleri gerekmektedir. Bilgi güvenliği farkındalığı konusunda değindiğimiz gibi çalışanlardan bir tanesinin bile bu kültürün dışına çıkmaları bilgi güvenliği risklerini beraberinde getirmektedir.

Kurum çalışanlarının bilgi güvenliği yönetişimine katılımı sadece bilgi güvenliği farkındalığı eğitimlerini almaları ile sınırlı olamaz. Tüm kurum çalışanları iş süreçlerinde bilgi güvenliğinden bağımsız hareket etmemelidir. Bu noktada mutlaka dikkat edilmesi gereken bir noktanın altını çizmemiz gerekmektedir. Günümüzde orta ve büyük ölçekli tüm kurumlarda hatta kimi küçük kurumlarda bile bilgi teknolojileri bölümleri bulunmaktadır. Orta ve büyük ölçekli kurumlarda ayrı bir bilgi güvenliği bölümü veya bilgi güvenliği yöneticileri istihdam edilmektedir. Fakat bu durum kurumun diğer çalışanlarının bilgi güvenliği konusunu çoğunlukla bilgi güvenliği bölümlerine ya da bilgi güvenliği yöneticilerine bırakmaktadırlar. Hatta BT bölümleri dahi -özellikle büyük kurumlarda yaşanmaktadır- bilgi güvenliğini sahiplenmemektedirler.

BT'nin dahi bilgi güvenliği süreçlerinin dışında durmak istemeleri, bilgi güvenliği yönetişiminin önündeki en büyük engellerden biri olarak karşımıza çıkmaktadır. Çoğu kurum bilgi güvenliği teknolojisi ile ilgili ürünlerini, çözümlerini ve süreçlerini ya BT içerisinde bir bilgi güvenliği ekibine ya da bir kısmı BT dışında bir kısmı ise BT içindeki güvenlik ekiplerine aktararak bilgi güvenliği yönetişimini sağlama yolunu seçmektedir. Kurumların genel yaklaşımı bu şekildedir. Ancak giderek artan CSO/CISO üzerinden bir bilgi güvenliği yönetişimi yaygınlaşmaktadır. Bunun da yeterli olup olmadığı tartışmalıdır.

Bilgi güvenliği yönetişimi için tüm kurum çalışanlarının ve özellikle BT çalışanlarının (başta ayrıcalıklı hesapları yöneten kullanıcılar) güvenlik süreçlerine dâhil edilmeleridir. Yedinci bölümde bahsettiğimiz "Dağıtık bilgi güvenliği yönetimi" olarak kast ettiğimiz de budur. Bilgi güvenliği yönetişimi uçtan uca gerçekleştirilmesi gereken bir kavramdır. Bu nedenle de tüm çalışanları bu sürecin içinde yer almalı ve sorumluluk hissetmelidir. Aksi takdirde bilgi güvenliği riskleri kurumların karşısında ciddi bir sorun olarak çıkmaya devam edecektir.

Burada sorulabilecek soru şu olabilir: Tüm çalışanlar bilgi güvenliği yönetişimi süreçlerine nasıl katılabilir? Bunun için ön koşul yine üst yönetim desteği olacaktır. Üst yönetim desteğiyle birlikte tüm çalışanların ve özellikle BT çalışanlarının, rol ve görev tanımları içerisine, sorumluluk alanlarına bilgi güvenliği bir madde olarak mutlaka eklenmelidir. Kurum çalışanları çoğu kez iş süreçlerinde bilgi güvenliğini dikkate almazlar ve bunun bilgi güvenliği ekiplerinin işi olduğunu düşünürler. Yapılması gereken ise bu noktada çalışanlara bilgi güvenliği sorumluluğun kendilerinin de bir görevi olduğunu hatırlatmak, öğretmektir. Bu şekilde tüm çalışanların bilgi güvenliğini sahiplenmeleri ve sorumluluk hissetmeleri sağlanacak, iş süreçlerinde bilgi güvenliğine uymayan herhangi bir noktaya yer vermeyeceklerdir.

Bu bahsettiklerimizi örneklememiz de mümkündür. Örneğin; kurumun yazılım geliştirme bölümlerinde yer alan çalışanlar doğal olarak önceliklerini projelerini yetiştirmeye vermektedirler. Ancak kod ve ekran geliştiren yazılım ekiplerini bu geliştirmelerini güvenlik gereksinimlerinin dışında yapamamalıdırlar. Yazılım geliştirme süreçlerine kurumlarda güvenlik konuları dâhil edilse de çalışanların farkındalığının ve sorumluluğunun gelişmesi öncelikli olmalıdır.

Sonuç olarak; bir kurumu birçok penceresi olan büyük bir eve benzetebiliriz. Bu evin tüm pencerelerinin her zaman kapalı olmasını sağlamak sadece bilgi güvenliği ekipleriyle sağlanamaz, bu pencerelerin kenarlarında bulunan her çalışan da bu sorumluluğu hissederlerse ancak bilgi güvenliği yönetişimi gerçekleştirilebilir ve bilgi güvenliği riskleri en aza indirilebilir.

Yedinci bölümde bilgi güvenliği organizasyonu için merkezi ve dağıtık modeller ortaya koyarken belirttiğimiz gibi, bilgi güvenliği ile ilgili teknolojik çözümlerin tamamının da BT güvenlik ekiplerinde yer alması gerekmemektedir. Bu ürünlerin tamamının BT güvenlik ekiplerinde toplanması bir yöntem olsa da bunun yerine ilgili diğer BT ekiplerinin bu ürünleri yönetmelerinde sakınca yoktur aksine diğer BT çalışanlarının da katılımını sağlar.

BT, özellikle büyük kurumlarda (Bankacılık, Telekomünikasyon vb.) çok sayıda çalışana sahip büyük organizasyonlardır. Bu nedenle bilgi güvenliğini sadece BT güvenlik ekiplerinin sağlamasını beklemek çok iyimser bir yaklaşımdır. Bunun yerine daha önce de belirttiğimiz gibi diğer BT çalışanları da güvenlik bilinci yüksek insanlar olmalıdır.

Kurumların bu organizasyona sahip olmaları büyük öneme sahiptir. İyi bir bilgi güvenliği yönetişimi modeli kurulamamış ise yapılacak büyük yatırımlar da atıl ve verimsiz olabilmekte, bilgi güvenliği riskleri azaltılamamakta ve kurumlar ciddi siber tehditlerle, bilgi güvenliği olaylarıyla karşı karşıya kalabilmektedir.

Bu nedenlerle merkezi bir bilgi güvenliği yönetişimi yerine dağıtık bir bilgi güvenliği yönetişim organizasyonu daha avantajlı olacaktır. Dağıtık bir modelde; dağıttığımız sadece güvenlik teknolojilerinin veya süreçlerin yönetilmesi değil bilgi güvenliği rol ve sorumluluklarının BT ekiplerine ve tüm diğer çalışanlara dağıtılması şeklinde anlaşılmalıdır. Aksi halde her iki yapının birbirinden üstünlükleri olmayacaktır.

Kurumların bilgi güvenliği yönetişimi'ne tüm çalışanlarını katmaları için neler yapılabilir noktasında da bir takım öneriler getirerek çalışmamızı tamamlayabiliriz.

- Tüm çalışanlara işe başlangıçlarında bilgi güvenliği farkındalığı eğitimleri eksiksiz bir biçimde sınıf içi eğitim olarak verilmelidir. Sınıf içi eğitimler özellikle büyük kurumlar için her ne kadar zor olsa da bilgi güvenliği kritik bir konudur ve uzaktan eğitimler verimsiz kalmakta, çalışanlara rol ve sorumlulukları yeterince aktarılamamaktadır.
- Tüm çalışan rol ve sorumluluklarına bilgi güvenliği eklenmelidir. Bilgi güvenliğinin iş süreçlerinin bir parçası olduğu mutlaka aktarılmalı, bilgi güvenliği ilkeleri olmaksızın bir iş sürecinin olmayacağını bilmeleri sağlanmalıdır.
- Kuşkusuz kurumlardaki en büyük güç Yönetim Kurulu ve üst yönetimdir. Yönetim Kurulu ve üst yönetime bilgi güvenliği farkındalığı mutlaka verilmelidir. Üst Yönetimin sorumluluk alacağı ve destek vereceği bir bilgi güvenlik anlayışı bilgi güvenliği yönetişiminin esasını oluşturur. Bilgi güvenliğinin Yönetim Kurulu ve üst yönetim tarafından desteklendiği, takip edildiği tüm çalışanlara farklı zamanlarda hatırlatılmalıdır.
- Bilgi güvenliği politikaları, kurumların bilgi güvenliğini ele alışları açısından en önemli dokümandır. Bu nedenle tüm çalışanların okuyup, anlayabilecekleri ve temel esasları içeren özet bilgi güvenliği politika dokümanları hazırlanmalı, bu politikaların tüm

çalışanlar tarafından içselleştirilmesi sağlanmalıdır. Bunun için çalışanların dikkatini çekecek pratik yöntemler mevcuttur.

- Oyunlaştırma son dönemde dikkate değer bir aşama kaydetmiş önemli bir teknolojidir. Çalışanların bilgi güvenliği farkındalığı süreçlerinin dışında kalmamaları için bu yöntem kullanılabilir ve tüm çalışanlar farkındalıklarını bu şekilde koruyabilir.
- Kurum içinde bilgi güvenliği ile ilgili olarak yarışmalar düzenlenebilir, çalışanların dikkatini ve ilgisini çekecek organizasyonlar yapılabilir. Yine kurum içerisinde çalışanların görebilecekleri alanlara posterler asılıp, bilgilendirmelerin yapıldığı alanlar kurularak bilgi paylaşımlarında bulunulabilir.
- Tüm çalışanların işlerinde en çok kullandığı ortamların başında elektronik posta gelmektedir. Tüm çalışanlara yönelik olarak elektronik posta yoluyla bilgilendirici paylaşımlar yapılmalıdır.
- Çalışanların hedef kartlarına bilgi güvenliği ile ilgili çeşitli hedefler konmak suretiyle, bilgi güvenliğine ilişkin yaklaşımları artırılabilir.
- Siber saldırılar için en önemli konuların başında ayrıcalıklı yetkiye sahip hesaplar gelmektedir. Mutlaka siber saldırganlar ayrıcalıklı hesapları ele geçirmeye veya sistemlerde ayrıcalıklı hesap oluşturmaya gayret etmektedirler. Çünkü ayrıcalıklı hesaplar adeta kilitli çelik kasaların anahtarı gibidirler. Bu nedenle ayrıcalıklı hesapları yöneten kullanıcılara yönelik olarak bilgi güvenliği rol ve sorumlulukları çok daha sık hatırlatılmalı, bu kullanıcılara farklı düzeyde eğitimler sağlanmalıdır.
- Bilgi güvenliğinin çok büyük oranda artık bilişim sistemleri üzerinde gerçekleştiğini ifade etmiştik. Bu nedenle Güvenlik, Sistem, Ağ ve Yazılım ekiplerinin bilgi güvenliği farkındalıklarının çok daha yüksek olması, özellikle bu çalışanların rol ve sorumluluklarında bilgi güvenliğinin yer alması olmazsa olmazdır.