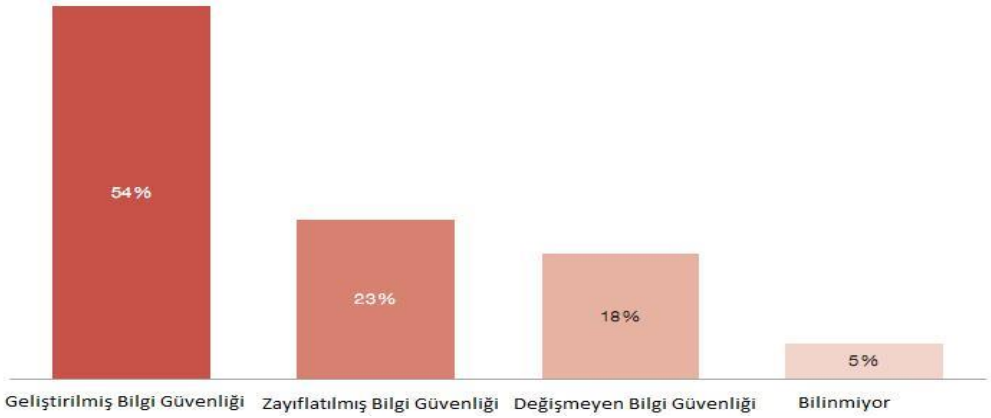
Sevda Çimen

152120131020

1.ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

İçinde bulunduğumuz 21 inci yüzyılın ilk çeyreğinde bilişim sistemlerinin, ağ teknolojilerinin kullanım alanlarının hızla artması ve özellikle bulut bilişimin birçok işletmede, kamu kurum ve kuruluşunda kullanılıyor olması, üretilen ve işletilen bilginin güvenliğinin sağlanmasını da zorunlu hale getirmiştir. Kurum ve işletmelerde bilgi güvenliğinin önemi ve tüm paydaşların bu yöndeki bilinç düzeyi de her geçen gün atmakla birlikte, "Kurumuma/şirketime ait bilgiyi nasıl korumalıyım, bilgi güvenliğimi nasıl sağlayabilirim?" vb. gibi sorular halâ güncelliğini korumaktadır[1].Bu yüzden gerekli koruma ve önemlemlerin alınması günümüz şartlarında her birey,kurum ve kuruluş açısından hayati önem taşımaktadır.Temel alınan bilginin çeşitleri olabildiği gibi bu bilginin tipi de güvenlik şartlarını değiştirmektedir.



Şekil 1.Bulut bilişimin Bilgi Güvenliği üzerindeki etkisi(GSISS,2012)

Bilgi güvenliği,bilginin izinsiz kullanılması veya yetkisiz bir biçimde erişime açık olunması bu erişimden kaynaklanan kulanım,degiştirilme,ortadan kaldırılma,el degiştirme ve hasar verilmesi gibi bilginin gizlilik,bütünlük ve sürekliliğinin degiştirilmesi gibi husulardan meydana gelir.Bu temellerden herhangi biri zarar görürse güvenlik zaafiyeti meydana gelir. Bu kısımda ISO 27001 Bilgi Güvenliği Yönetim Sistemi devreye girmektedir.Bu standart ISO tarafınan 14 Ekim 2005 tarihinde yayınlanmış ve ISO/IEC 27000 standart serisi altında yerini almıştır[2].Aynı zamanda ISO 27001 VE ISO 27002 Bilgi Güvenliği Yönetim Sistemi'nin en temel standardıdır.BGYS'nin planlanmasının gerçkleştirilmesini,iyileştirilmesini ve sürdürülmesi için uygulama işlemlerini ISO 27002 içerirken belgelendirme için gereken standartlar ise ISO 27001 içerisinde yer almaktadır. Bu standart aynı zamanda kurumsal bilgi güvenliğinin

saglanmasında insanları, süreçleri ve bilgi sistemlerini içine alan ve üst yöntim tarafından desteklenen bir yönetim sistemidir[3].

2008 tüm saldırı tipleri Dünya Sıralaması	2007 tüm saldırı tipleri Dünya Sıralaması	Ülke	2008 Yılı Tüm Saldırı Tipleri içinde oranı	2007 Yılı Tüm Saldırı Tipleri içinde oranı	Zararlı Kod	Spam Yayıcı Sistem	Phishing Web Siteleri	Bot Sistemler	Tüm Saldırılar Geneli
1	1	A.B.D.	23%	20%	1	3	1	2	1
2	2	Çin	9%	11%	2	4	6	1	2
3	3	Almanya	6%	7%	12	2	2	4	4
4	4	İngiltere	5%	4%	4	10	5	9	3
5	8	Brezilya	4%	3%	16	1	16	5	9
6	6	İspanya	4%	3%	10	8	13	3	6
7	7	İtalya	3%	3%	11	6	14	6	8
8	5	Fransa	3%	4%	8	14	9	10	5
9	15	**Türkiye**	**3%**	2%	15	**5**	24	8	12
10	12	Polonya	3%	2%	23	9	8	7	17

Şekil 2. 2007 ve 2008'de dünya genelinde zararlı kodların tiplerine göre sıralamalar ve genel sıralamalar (Symantec, 2009: 18).

2.GELİŞME

Bilgi güvenliğinin yalnızca teknik yönetemlerle degil aynı zamanda bir takı standart ve denetimler altında sağlanması gerektir.Bu yüzden kullanılan bu standartlar kuruluşlar açısından gerekli bir güvenlik politikası haline gelmektedir.Fakat burda ana husus bu politikaya üst yönetim ve digger tüm çalışanların destek vermesi gerekmektedir.Bu sayede işbirliği içinde bulunan tüm kuruluşlar bu politikalara uygun davranarak bilgi güvenliğini arttırabilmektedir.Temel olarak bu sistemin faydaları ise;bilginin dogru,güvenilir ve geçerli olmasının sağlanması,güvenlik risklerinin azaltılması,bilginin daha korunumlu hale getirilmesi,kuruluş içerisinde bilgi güvenliginin farkındalığının arttırılması ve bunun gibi birçok faydayı yasal tarafların zorunlu kıldığı kriterler dahilinde sağlanabiliyor olması.

3. SONUÇLAR

Ernst & Young›ın yıllık anket sonuçlarına göre, şirketler bilgi güvenliği hakkındaki risk ortamının değiştiğinin farkında. Ankete yanıt verenlerin yüzde 80'i dış tehditlerin artmasıyla risk faktörünün de yükseldiği konusunda hemfikir. Buna ek olarak katılımcıların yüzde 31'i bilgi güvenliklerini tehdit eden vakaların geçen yıla göre artış gösterdiğini, yüzde 59'u aynı oranda kaldığını, yüzde 10'u da düşüş gösterdiğini belirtti. Bilgi güvenliğine yönelik tehditlerin sıklığı ve güvenlik vakalarının artması bu konuda şirketlerin görebileceği potansiyel zararın da

arttığına işaret ediyor.ABD›nin resmi rakamları da kişisel tanımlanabilir bilgilerin izinsiz paylaşımı, 2011 yılında yüzde 19 arttığını belirterek bilgi sızıntısının vardığı boyutu ortaya koymaktadır[5].

Günümüz dünyasında her geçen gün bireyler, şirketler, kurumlar ve devletler için "bilgi = daha çok güç" haline geldiği gibi, bilgi teknolojileri geliştikçe güvenlik sorunları da artmaktadır[4].ISO 27001 Bilgi Yönetim Sistemi kuruluşlar açısından bilgi güvenliğini bir standart ve yasal yükümlülük çeçevesine taşıyarak bu konuda alınması gereken temel bir yükümlülük haline gelmiştir.Kurumlar BGYS ile herşeyden önce bilgi varlıklaırnın farkına varmaktadır.Bu sayede farkına vardıkları bu varlıkların öneminin anlaşılması ve riskleri belirleyip bunları yöneterek iş sürekliliğini sağlayabileceklerdir.Ayrıca temel standartlar dahilinde ISO 27001 sertifikasına sahip olmak bu kuruluşa blgi güvenliği risklerini bildiği,bu riskleri yönetebildiği ve bunları ortadan kaldırmak için kaynak ayırdığı şeklinde bir farkındalık yaratacaktır.

4.KAZANIMLAR

Bu araştırma ödevi kapsamında bilgi güvenliğinin şirketler açısından önemi ve ISO 27001 standardı ile bilgi güvenligi farkındalığının kurum ve kuruluşlar açısından arttırılmasının gerekliliği hakında bilgi sahibi oldum.Var olan istatistk ve anketler ile de güvenlik zaafiyetinin günümüz teknolojisinde nedenli gerekli olduğunu bilimsel olarak da görüntüleyebildim.

5.KAYNAKÇA

Makaleler:

[1] TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı kapsamında bilgi güveniği yönetim sisteminin kurulması ve bilgi güvenliği risk analizi Hasan Yılmaz İç Denetçi, İstanbul Üniversitesi 2014/2015

[2] ISO 27001 Kurumsal Bilgi Güvenliği Standardı Şenol Şen

[3] Eminağaoğlu, M., Gökşen, Y. DEÜ SBE Dergisi Cilt11, Sayı:4

[4] ERNST&YOUNG, 27/12/2012 tarihli Basın Bülteni, http://www.ey.com/Publication/vwLUAssets$FILE/Bilgi Guvenligi%20BB_EB.pdf Erişim tarihi:28/05/2014, s.1

Elektronik Kaynaklar:

[5] http://belgelendirme.ctr.com.tr/iso-27001.html