

Kurumlarda Bilgi Güvenliği Farkındalığı,

Önemi ve Oluşturma Yöntemleri

Ender Şahinaslan¹, Arzu Kantürk², Önder Şahinaslan³, Emin Borandağ⁴

¹ Bank Asya, Bilgi Güvenlik Yöneticisi, İstanbul

² Bank Asya, Bilgi Güvenlik Uzmanı, İstanbul

³ Maltepe Üniversitesi, Bilişim Bölüm Başkanı, İstanbul

⁴ Maltepe Üniversitesi, Bilişim Uzmanı, İstanbul

ender@bankasva.com.tr, akanturk@bankasya.com.tr, onder@maltepe.edu.tr, eminb@maltepe.edu.tr

Özet: Kurumların sahip olduğu en değerli varlıkları olan bilginin; gizlilik, bütünlük ve erişilebilirlik nitelikleri bakımından sürekli korunması gerekmektedir. Bu durum ISO Bilgi Güvenliği Standartlarında da açıkça tariflenmiştir. Bilgiye olabilecek yetkisiz erişimlerin engellenmesine gizlilik, yetkili erişim sonucunda kendine özgü bilgi mahremiyetinin korunmasına bütünlük, ihtiyaç halinde kolay ulaşılabilir olması erişilebilirlik denir. Bu bileşenler korunacak bir bilginin üç temel özelliğini teşkil eder. Bu, temel niteliklerin korunabilmesi için sistem üzerinde sadece teknik açıdan önlem almakla yetinilmemelidir. Güvenliğin en zayıf unsuru sayılan insan faktörün de dikkate alınması ve komple bir bütünlük içerisinde farkındalık oluşturulmalıdır. Bu çalışma; kurumlarda bilgi güvenliğine yönelik risklerin önlenmesinde, bilgi güvenliği farkındalığının önemi ve farkındalık oluşturma yöntemlerini kapsamaktadır.

Anahtar Kelimeler: Bilgi Güvenliği, Güvenlikte İnsan Unsuru, Risk, Farkındalık ve Farkındalık Oluşturma Yöntemleri

Abstract: Information that is the most valuable asset of the organizations invariably should be secured in terms of confidentiality, integrity and availability features as it is also described on information security standards. Confidentiality that blocks unauthorized access to information, integrity that secures distinctive features of information as a result of authorized access, availability that is reachable and utilizable in case of necessity comprises three basic feature of information that should be secured. It is, should'nt contented with take precautions in terms of only technical on systems to secure these basic features. Human factor that is thought as the weakest element of security by considering and completely inside of integrity should be created awareness. This bulletin, mentions to prevent information security risks in the organizations, information security awareness, its significance and awareness creation methods.

Key Words: Information Security, Human Factor in Information Security, Risk, Awareness and Awareness Creation Methods.

1. Giriş

Bilgi teknolojilerinde yaşanan gelişmeler, daha çok bilginin depolanmasına ve taşınmasına imkân verebilir hale gelmiştir. Çok fonksiyonlu, küçük ama marifeti büyük teknolojik cihazlar sayesinde her geçen gün daha fazla

bilgi elektronik ortama aktarılmakta, depolanmakta, işlenmekte, hizmete sunulmakta ve taşınabilmektedir. Bilginin elektronik ortamlar üzerinde yoğun kullanımı ve hareketliliği günümüzde bireyler, şirketler ve kurumlar açısından çeşitli güvenlik risk ve sorunlarını da beraber getirmektedir. Bu durum her geçen

gün artış göstermekte, teknolojik ilerlemelere paralel olarak; kurumlarda bilgi güvenliđinin sađlanması kurumun imajı, güvenilirliđi ve faaliyetlerinin devamı ađısından oldukça önemli bir hale gelmiřtir.

Bir kurum, maliyetine bakmaksızın paranın alabileceđi en ileri güvenlik teknolojilerini kullanabilir, sistemleri tasarlayabilir ve adeta kendisini bir güvenlik çemberinden geçirebilir. Bu řekilde sadece en son teknolojiyi kullanarak üst seviyede güvenlik önlemleri alabilen bir kurumda bilgi güvenliđinin tamamen (%100) sađlanmış olduđundan bahsedilemez.

Güvenlik teknolojileri geliřtirildikçe, olası teknik açıkları kullanmak/sömürmek zorlařacağı için saldırganlar insan unsurunun zayıflıklarından faydalanma yoluna yönelmiřlerdir. Bundan dolayı kurumlarda güvenliđin en zayıf halkasını insan unsuru oluřturmaktadır. Güvenlik; teknolojiden önce insana yatırım yapılmasıyla, kurum çalışanların/bireylerin en tepeden en alt çalışanına, hatta bilgi alış verişinde yaptıđı varsa tedarikçileri, müşteri ve ziyaretçilerini bilgilendirmesi, onlar üzerinde bir bilgi güvenlik farkındalıđı oluřturması, kendini geliřtirmesi, bilgi güvenlik faaliyetlerinin benimsenmesi, önemsenmesi ve desteklemesi ile anlamlı hale gelebilir.

Bilgi güvenliđi risklerinden korunmanın en iyi yolu bilgi teknolojilerine çok para harcamak ve korunma amaçlı teknolojileri daha çok kullanmaktan önce insanların bilinçlenmesi ve ihtiyaç duyulan güvenlik teknolojisinin dođru yer ve zamanda kullanmakla mümkün olabilir.

İnsan faktörüne bađlı bilgi güvenlik riskleri hiçbir zaman tamamen ortadan kaldırmak mümkün olmasada iyi planlanmış bir farkındalık faaliyeti ile güvenlik risklerinin kabul edilebilir bir seviyeye çekilmesini sađlanabilir.

2. Kurumlarda Bilgi Güvenliđi Farkındalıđının Önemi

Kurumlarda bilgi güvenliđi farkındalıđı çalışanlarının ana hedefi; bařta çalışanları olmak üzere bilgi alışveriři yaptıđı bireylere kurumu için deđerli bir varlık olan bilgi ve bilgi varlıklarının koruması konusunda üzerlerine düşen sorumlulukları anlamalarını sađlamak olmalıdır. Kurum için bu durum kritik bir öneme sahiptir.

Kurumun bilgi güvenliđinden sadece bilgi güvenliđi çalışanları deđil kurumun tüm çalışanları hatta paydařları, tedarikçileri kısaca kurum bilgi güvenliđi politikasında yer alan tüm bireyler sorumludur. Farkındalık ile çalışanlar üzerinde güvenlik bilinci oluřturulurken hangi bilgilerin korunması gerektiđi, bunların ne tür tehditlere karřı nasıl korunması gerektiđi konusunda bilinçlendirme yapılır.

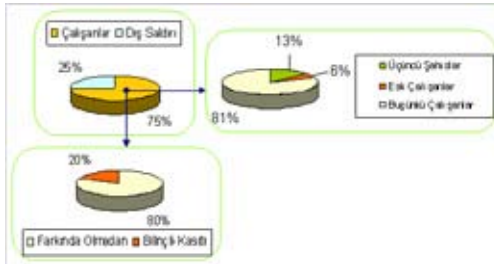
Kurumlarda Bilgi Güvenliđini, çalışanların düşünce ekseninde tutmanın en etkili yollarından biri çalışanın bilgi güvenliđi sorumluluklarını aynı zamanda bir iş sorumluluđu olarak görmesini sađlamaktan geçer. Ancak bunu çalışanlar üzerinde bir farkındalık oluřturmadan tek başına görev tanımlarına yazmakla sađlamayı ummak bir beklentiden öteye gidemez.

Kurum bilgi güvenlik risklerini kabul edilebilir seviyeye indirgemedi yararlanılan bilgi güvenliđi farkındalıđı oluřturmada ki asıl amaç; bilgi eksikliđinden kaynaklanabilecek insan hatalarını ve teknolojinin yanlış kullanılması risklerinin azaltmak, bireylerin bilgi güvenliđi tehditleri ve sorunlarından haberdar edilmesi, normal çalışma zamanları içinde kurumun güvenlik politikasını desteklemek üzere donanımlı bir hale getirebilmeyi sađlamak olmalıdır.

Gartner Datapro Research şirketi tarafından yapılan araştırmanın sonuçları, kurumsal bilgilerin nasıl, kimler tarafından tehdit edilebileceđi ve zarar verilebileceđi hakkında ilginç sonuçlar

vermektedir. Genel olarak ilk baslarda saldırıları yapanların yaşça oldukça genç ve kendilerine ün sağlamak isteyen bilgisayar saldırganları olduğu ancak son zamanlarda bunların yerlerini daha çok maddi gelir sağlamayı amaçlayan organize örgütlerin aldığı yönündedir.

Bu ve benzeri araştırma sonuçları doğrultusunda oluşturulmuş aşağıdaki grafiklerde güvenlikte insan unsurunun önemi ve farkındalık oluşturulması zorunluluğunu açık bir şekilde sergilenmektedir.



Şekil 1: Bilgi Güvenlik İhlallerinde İnsan Faktörü

Kurumlar her geçen gün gelişen teknolojiden biraz daha fazla faydalanır hale gelmişler ve pazarlarda kendilerine rekabet üstünlüğü sağlamak amacıyla süreçlerini güçlendirmektedirler.

İnternet'in çok yaygın olarak kullanılmasına paralel olarak güvenlik açıklarının artması, davranış temelli güvenlik açıklarını oluşturan sosyal mühendislik, kimlik hırsızlığı gibi tehditlerini ortaya çıkartmıştır.

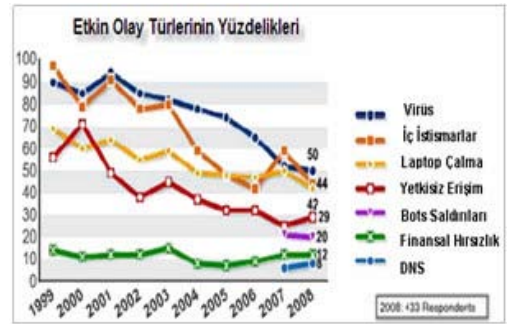
Araştırmalar gösteriyor ki, etkili atak modelleri arasından ilk ikisi, bilgilere yetkisiz erişim ve kurum bilgilerinin çalınması üzerine gerçekleşmiştir. Yapılan araştırmaların ikinci yönü ise günümüz dünyasında geçmiş yıllara göre atakların artık yıkıcı yönünün geride kaldığını; yerine bilgi sızdırma, hırsızlığı ve istihbarat çalışmaları yönünün daha ön planda olduğunu gösterir.

2008 SANS ISC raporuna göre saldırganların güvenlik duvarını, antivirüs hatta saldırı tesbit

sistemlerini asmada kullandığı ilk hedefin kolayca kandırılabilen insan faktörü olduğudur.

Bilgisayar Güvenlik Enstitüsünün, 2008 bilgisayar suçu ve güvenlik araştırmasına göre; virüs, iç istismarlar, bilgisayar hırsızlığı ve yetkisiz erişim en çok rastlanan güvenlik olaylarıdır.

Bu rapora; güvenlik olaylarının yıllara göre gösterdikleri değişimler aşağıdaki grafikte gösterilmektedir. Bu grafikte genel olarak 1999 yılından 2008 yılına kadar bazı tehditlerin gerekli farkındalık çalışmaları ve kullanılan güvenlik teknolojileri sayesinde büyük bir düşüş yaşandığı gözlemlenmektedir. (2008 CSI Computer Crime & Security Survey)



Şekil 2: Etkin Bilgi Güvenlik Olayları

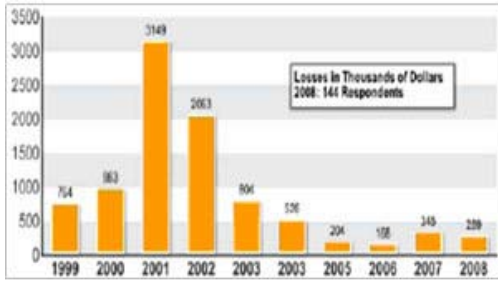
Saldırı Türleri	2004	2005	2006	2007	2008
DOS Atakları	39%	32%	25%	25%	21%
Laptop Çalma	49%	48%	47%	50%	40%
Telekom Dolandırıcılığı	10%	10%	8%	5%	5%
Yetkisiz Erişim	37%	32%	32%	25%	29%
Virüs	78%	74%	65%	52%	50%
Finansal Sahtekarlık	8%	7%	9%	12%	12%
İç Sistemler	59%	48%	42%	59%	44%
Sistem Sızma	17%	14%	15%	13%	13%
Sabotaj	5%	2%	3%	4%	2%
Çalma/ Özel bilgi kayıpları	10%	9%	9%	8%	9%
Kablosuz Ağ Sistemleri	15%	16%	14%	17%	14%
Web Site Saldırıları	7%	5%	6%	10%	6%
Web Uygulamaları kötüye kullanma	10%	5%	6%	9%	11%
Bots (DDoS, Spam, Sniffer)	-	-	-	21%	20%
DNS Atakları	-	-	-	6%	8%
Atık Mesajlaşma Sistemleri	-	-	-	25%	21%
Parola dinleme	-	-	-	10%	9%
Çalma/Müşteri bilgileri kayıpları	-	-	-	17%	17%

Tablo 1: Bilgi Güvenlik Olayları Yüzdelerinin Dilimleri

2007 yılındaki kurum içinde bilinçli ya da bilinçsiz bir şekilde yapılan güvenlik istismarları %59' den 2008 yılında bu durum bilgi güven-

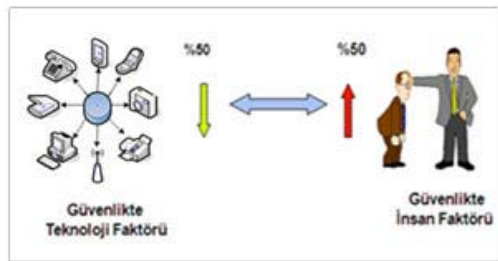
liği farkındalık çalışmaları ile %44'de kadar düşürülebildiği gözlemlenmektedir. Yine etkin bilgi güvenlik olaylarına ait yüzdelik dilimler incelendiğinde en büyük tehdit unsurunu iç tehditler olduğu görülmektedir. Bu durumda insan faktörünün kurum için önemini açık bir şekilde göstermektedir. (2008 CSI Computer Crime & Security Survey)

Aşağıdaki grafik de yukarıdaki tablolarda gösterilen güvenlik olaylarının kurumlar bazında 1999-2008 ortalama maddi zarar dağılımı gösterilmektedir. En yüksek maddi zarar 2001 yılında vuku bulmakla birlikte 2001'den 2008 yılına kadar belirli oranlarda düşüşler yaşanmıştır (CSI Computer Crime & Security Survey 2008)



Sekil 3: Yıllara Göre Ortalama Zarar Kaybı

Tüm bu grafiklerden çıkarılabilecek sonuca göre, aşağıdaki resimde güvenlikte teknoloji ve insan faktörünün etkisinin yüzdelik oranı %50 olarak verilmiştir fakat bu değer önümüzdeki günlerde ilerleyen teknolojiye paralel olarak daha da artacağı düşünülmektedir.



Sekil 4: Güvenlikte Teknoloji ve İnsan Faktörünün Yönü

Bütün bunlardan çıkartılması gereken sonuç güvenliğin bir teknoloji sorunu olmaktan çok süreç ve iş yönetimi sorunu olduğunun kabul edilmesinden geçer.

Bu nedenle günümüz koşullarında kurumların esas değerini oluşturan insan varlığı ve onun bu süreçlere göre performansından ödün vermeden güvenli şekilde yönetmek, kurumun olduğu kadar çalışanlarında yararınadır. Bunu sağlamanın yolu kurumsal bir farkındalık programı oluşturmak ve bunu belirli dönemlerde veya farklı yöntemlerle çalışan zihinlerde aktif bir şekilde tutacak şekilde bilinçlendirme çalışmalarını yapmaktan geçmektedir.

Kurumlarda bilginin paylaşıldığı bireylerin yapabilecekleri çok küçük hatalar, dikkatsizlikler, bilinçli ya da bilinçsiz yapılabilecek her türlü suistimler teknik anlamda alınan tüm güvenlik önlemlerini boşa çıkaracaktır. Bu nedenle kurumlar, günümüz şartlarına uygun bir farkındalık oluşturmak zorundadır.

3. Bilgi Güvenliği Farkındalığı Oluşturma Yöntemleri

Bilgi Güvenliği çalışanları bu konuda yeteri kadar donanıma sahip olmalı veya gerekiyorsa bu anlamda bir danışmanlık hizmeti de alınabilir.

Bilgi güvenliği farkındalığını oluşturmanın ana yolu kurumda en üst seviyedeki yönetimden en alt seviyedeki çalışana hatta tedarikçilere kadar çalışanların görev ve pozisyonları da dikkate alınarak ihtiyaç ve beklentilere göre farklı eğitim ve farkındalık programları hazırlanmalı ve eğitimler düzenlenmelidir.

Bu eğitimler bir çalışan ise başladığında verilen oryantasyon eğitimlerinin ayrılmaz bir parçası olarak düşünülmeli ve mutlaka her çalışana en az bir kez verilmelidir. Daha sonraki dönemlerde ise çalışana planlanmış varsa alması gereken diğer eğitimler düzenli olarak verilmelidir.

Kurumlarda çalışanlar/bireyler üzerinde farkındalık oluşturmada sınıf içi eğitimler yanında pek çok farklı yöntemler de bulunmaktadır. Bunlar;

- İnternet tabanlı interaktif sanal eğitimleri verilebilir.
- E-Learning eğitimleri; zorunlu bilgi güvenliği eğitimleri ya da pozisyona göre özel interaktif sanal eğitimler hazırlanabilir.
- Çalışanlara yönelik masaüstü bilgi güvenliği (el kitabı) kitapçığı ve renkli broşürler, posterler hazırlanabilir.
- Kurumdaki birimler bazında aylık etkinlikler düzenlenip, ilgili birimlerin güvenlik konusundaki eksiklikleri ve dikkat edilmesi gereken güvenlik unsurları açıklanarak, bir farkındalık oluşturulabilir.
- LCD'lerde çeşitli animasyonlar hazırlanabilir.
- Film gösterileri (Multimedya) hazırlanabilir.
- Bilgi güvenliği e-posta bülteni hazırlanabilir.
- Ekran koruyucu ile mesajlar iletilebilir. Bu mesajlar bilgisayar güvenliği ve kurumun bilgi güvenliği politikasını yansıtacak şekilde parola güvenliği, e-posta güvenliği vs. gibi konuları içerebilir.
- Bilgi güvenliği mesajlarını iletme için farklı küpler hazırlanabilir. Her çalışanın masasına konur ve bunlar günlük olarak bir biriyle değiştirilebilir.
- Bilgi Güvenliği konusunda oyunlar hazırlanabilir. Son kullanıcının seviyesine göre simülasyonlar hazırlanabilir. Bu oyunlarda kullanıcıya güvenlik açıklarının bulunması yönünde bir strateji ile farkındalık oluşturulabilir. Bilgi Güvenliği oyunu ile hedeflenen ana nokta, kurum çalışanlarına kurum için önem ve gizlilik taşıyan bilgi varlıklarının neler olduğu ve bunların saklanması konusunda bilgilendirilmesi, kurumsal bilginin kolayca savunmasız kalabileceği, gereksiz görülen şeylerin izinsiz erişime neden olabileceği hakkında bilinirliğin artırılması ve kurumsal bilgi güvenliğinin sağlanmasının kurum için ne kadar önemli olduğunun çalışana farkettilmesidir.

- Karikatürlerle, insanlara hoş eğlenceli gelecek şekilde kullanıcıyı bilinçlendirecek bir kurgu üzerinden gidilerek sunular hazırlanabilir.
- Belirli aralıklarla kurumda çalışanlara yönelik yazılar ya da yukarıda ifade edilen şekilde sunular hazırlanıp, yayınlanabilir.
- Kullanıcıların masaüstü arkaplanları bilgi güvenliği farkındalığına uygun şekilde tasarlanabilir.
- Güvenliği hatırlatan sisteme giriş mesajları, mousepad, anahtarlık, not kağıtları logo veya sloganlar hazırlanabilir.
- Çalışanlara güvenlikle ilgili sesli e-posta ve video görüntüleri gönderilebilir veya bir portal üzerinden yayımlanabilir.
- Çalışanların güvenlik hassasiyetleri değerlendirilip ödüllendirme yoluna gidilebilir.
- Farkındalık amaçlı bulmacalar hazırlanıp kurum bazında periyodik olarak yayımlanabilir, bulmacayı doğru çözen ilk üç çalışan ödüllendirilebilir.
- Bu anlamda kurumda etkinlikler oluşturulup, çeşitli skeçler, oyunlar hazırlanabilir.
- Bilgi güvenliği oyun turnuvaları düzenlenebilir.
- Yapboz türü oyunlar geliştirilebilir.

Ayrıca kurum çalışanların yanı sıra müşterilere de bu tür eğitimler verilmelidir.

Örneğin; İnternet bankacılığı konusunda güvenliğin nasıl sağlanacağı, ya da güvenli POS kullanımı, kredi kartı güvenliği gibi konularda müşterilerde eğitimler verilmeli ya da kurumun internet sitesinde bu konularda güncel bilgilendirmeler yapılmalı duyurular aracılığıyla da bilgilendirilmelidir.

4. Sonuç

Güvenlik kuralları; bilgiyi korumak amacıyla, çalışan davranışları için yön gösterici bir rehberdir ve güvenlik tehditlerini bertaraf edebilmek içinde etkili kontrol geliştirilmesinin temel yapı taşıdır.

Etkili güvenlik önlemleri ise iyi düzenlenmiř kurallar ve süreçlerle çalışanları eğitmekle mümkün olacaktır. Bu da ancak etkili bir çerçevede hazırlanmıř farkındalık programları ile olabilecektir.

İyi tasarlanmıř ve kurgulanmıř farkındalık programı güvenlik çemberinin en zayıf halkasının güçlenmesini sağlayacaktır.

En önemli ve en etkili güvenlik önlemi kurumun çalışanlarını mutlaka ama mutlaka eğitmesi ve bilinçlendirmesinden geçmektedir. En basit bir ciddiyetsizlik, dikkatsizlik, sorumsuzluk bilginin yetkisiz kişilerin eline geçmesine ve kurum için maddi manevi çok büyük belki telafisi mümkün olmayabilecek kayıplara sebep olabileceđi hiçbir zaman unutmamalıdır.

Bu tür bir bilinçlendirme çalışmalarında üst yönetimin desteđi ve çalışanların yeterli bilince sahip olması çok önemlidir. Tüm bu farkındalık çalışmaları ya da teknolojik önlemlerin alınması, uygulanması ve bunlardan etkin beklenen sonuçların elde edilmesinde kurum üst yönetimi başta olmak üzere tüm çalışanların aktif katılımları ve destekleri ile mümkün olabilecektir. Son olarak, kurumlarda bilgi güvenliđini sağlamada etkin teknolojik önlemleri almanın yanında, bir yandan çalışana güveni esas alırken diđer yandan çalışanlara bir farkındalık programı uygulamayı ve kontrolü kesin suretle elden bırakmamak gerekir.

5. Kaynakça

- [1] ISO/IEC 27001 Information Security Management System
- [2] 2008 CSI Computer Crime & Security Survey <http://www.gocsi.com/>

[3] CSI Awareness <http://www.gocsi.com/awareness/?jsessionid=5V2UUESUW13GQQSNDLOSKH0CJUNN2JVN>

[4] CERT-In Monthly Security Bulletin July 2008 <http://www.fbi.gov/majcases/fraud/inter-netschemes.htm>

[5] Oyun Tabanlı Eğitim http://www.enocta.com/web2/ContentShowOne.asp?C_Type=1&ContentID=343&T=1

[6] Kurumsal Bilgi Güvenliđi Bilinci <http://www.inflnityteknoloji.com/tr/article.asp?ID=509>

[7] Mitnick D.Kevin, 'Art Of Deception', Jan. 2006

[8] Key Considerations for Developing Effective Information Security Awareness and Training Programs, March 2006

[9] Bilgi Güvenliđi Bilincinin Genele Yayılması <http://www.deloitte.com/dtt/article/0,1002,cid%253D53205%2526pv%253DY,00.html>

[10] <http://www.sans.org/>

[11] <http://www.gartner.com/>

[12] <http://tbd.wmv.gen.tr/>