BİLGİ GÜVENLİĞİ FARKINDALIK EĞİTİM ÖRNEĞİ

Ender ŞAHİNASLAN
Bilgi Güvenliği Yöneticisi
BANK ASYA, İstanbul
ender@bankasya.com.tr

Dr.Rembiye KANDEMİR
Bilgisayar Mühendisliği
Trakya Üniversitesi, Edirne
rembiyeg@trakya.edu.tr

Önder ŞAHİNASLAN
Bilişim Bölüm Başkanı
Maltepe Üniversitesi,İstanbul
onder@maltepe.edu.tr

ÖZET

Günümüzde kurumlar ve bireylerin sahip olduğu en değerli varlıkları olan bilginin; gizlilik, bütünlük ve erişilebilirlik nitelikleri bakımından sürekli korunması gerekmektedir. Koruma bir takım fiziksel ve sistemsel önlemlerin yanında bireylerin bilgi güvenliğine ilişkin tehdit ve risklerden, kurum bilgi güvenlik politika yada kurallarından haberdar olması, bu tehditlere nasıl karşı koyabileceği, olası riskleri mümkün olabilecek en düşük risk düzeyinde nasıl tutabileceği konusunda bilgilenmesiyle mümkün olabilir.

Güvenliğin en zayıf halkası olarak da kabul edilen insan faktörü üzerinde çeşitli farkındalık programları uygulanması gerekmektedir. Bu programların en başında ise bilgi güvenliği farkındalık eğitimi yer alır.

Bu çalışma; bilgi güvenliği temel farkındalık eğitimi için yer alması gereken ana konuları içeren temel bir eğitim programı hakkında bilgilendirme ve temel bir bilgi güvenliği farkındalık eğitim örneğini sunmayı amaçlar.

Anahtar Kelimeler: Bilgi Güvenliği, Farkındalık Eğitimi, Güvenlikte İnsan Unsuru, Risk Önleme.

ABSTRACT

Today, the information that is the most valuable asset of the individuals and institutions invariably should be secured in terms of confidence, integrity and attainability features. Protection that is threats and risks in terms of individual's information safety alongside certain physical and systematic precautions. The protection provides to be aware institution's information safety policy or its rules, potential risks, how to protect these threats. It can be determined how to decrease potential risks through notification.

The various awareness programs should be implemented about human factor that is also accepted as the most weakness circle of security. The most significant of these programs is information security awareness training.

This study aims to present notification and a basic information security awareness training sample about a basic education program that includes main topics required for information security basic awareness education

Key Words: Information Security, Awareness Training, Human Factor of Security, Risk Prevention.

1. GİRİŞ

Teknolojik dönüşüm ve hızlı bir evrimin yaşandığı günümüzde daha çok bilgi daha küçük aygıtlar üzerinde saklanabilir, taşınabilir, çoğaltılabilir hale gelmiştir. Uygulama yazılımları ve internet tarafında ki gelişmelerle de bilgilerin işlenmesi bir değere dönüşmesi daha pratik hale gelmiştir. Tüm bu insan hayatını kolaylaştıracak teknolojik gelişmeler diğer yanda uygunsuz kullanım, bireylerdeki risk algısının zafiyeti, bilgi güvenliği tehditlerinden habersizliği karşısında bir takım olumsuzlukları, kötü amaçlı kullanımları ve bir takım telafisi güç bilgi güvenliği risklerini de bünyesinde taşımaktadır.

Yapılan bir takım araştırmalar bize bilgi güvenliği risklerini gidermede insan faktörünü göz ardı ederek oluşturulacak sistemsel bir takım güvenlik çemberlerinin çok etkili ve yararlı olmadığını göstermektedir.

Bilgi teknolojileri alanında yapılan yatırımlar sonucunda yazılımsal veya donanımsal açıklar üzerinden bilginin sömürülmesi, uygunsuz kullanımı çok zorlaşmıştır. Bu açıklar yerine insan faktörünü kullanarak bilgiler üzerinde bir takım çıkarlar elde etme gayreti yoğunlaşmış durumdadır.

Tüm bu riskler göz önünde tutulduğunda riskleri gidermek yada olası en düşük düzeyde tutmanın yolu bireyler üzerinde bir farkındalık oluşturmadan geçmekte. Bunun en temel yolu ise özellikle kurumlarda yeni başlayan çalışan başta olmak üzere tüm çalışanlara, paydaşlara, tedarikçileri kısaca kurum bilgi güvenliği politikasında yer alan tüm bireylere gereksinimlere göre farklı kategorilerde eğitim programlarının hazırlanması ve bireyler üzerinde bir farkındalık bilincinin oluşturulması gerekmektedir.

Farkındalık eğitimleri bireylerin bilinç düzeyleri ve beklentiler dikkate alınarak temel bir eğitim programına ek olarak farklı kategorilerde hazırlanarak sunulmalıdır. Bir kurumda yeni başlayan ve bilgi teknolojilere yabancı olan bir çalışana verilecek eğitim ile BT alanında çalışan bilgi teknolojileri alanında donanımlı bilgiye sahip bir çalışanın beklentisi ve verilecek eğitim farklı planlanmalıdır. Yine bir birim müdüründen ya da üst yönetiminin sorumlulukları ve bilgi güvenliği alanında kendilerinden beklenenler ile bu yöneticilerin eğitimden beklentileri farklılık arz etmekte. Bu da farkındalık eğitiminden beklenen katkıyı maksimum seviyede tutabilmek için eğitim programlarının farklılaştırılması zorunludur.

Bu çalışmada kurumlarda verilecek temel bir bilgi güvenliği farkındalık eğitim içeriğine yönelik kurumlara örnek bir eğitim sunmak, bu konuda arayış ve gereksinim içerisinde olan kurum ve bireylere yol göstermektir.

2. EĞİTİMİN ANA BAŞLIKLARI

Temel bir bilgi güvenliği farkındalık eğitiminde bireylere temel bilgi kavramları, bilgilerin bulunduğu ortamlar, bilginin korunacak nitelikleri, bilgi güvenliğine ilişkin güncel tehditler ve saldırılar, sosyal mühendislik, dikkat edilmesi gereken kurallar ve temiz masa kuralları, fiziksel güvenlik, şifre güveliği, yasal düzenlemeler, kurum politika ve prosedürleri, bireyin sorumlukluları ve kendisinden beklenenler örneklerle zenginleştirilerek aktarılmalı, eğitimi alan bireylerin aktif katılımı sağlanarak etkileşimli bir şekilde sunulmalıdır. Bunlar kurum ve bireylerin beklentileri dikkate alınarak çeşitlendirilerek farklılaştırılabilir.

2.1. Temel Bilgi Kavramları

2.1.1. Veri/Bilgi kavramları

Veri ve bilgi kavramları bazen karıştırılabilmektedir. Bu konuda kısa bir bilgi vermenin yararlı olabileceği düşüncesiyle bu konuda bilgilendirme yapılmalıdır.

Sayısal veya mantıksal her bir değerin bir veri olduğu, bilgi'nin ise verinin işlenmiş, anlamlı hale gelmiş, açıkça tariflenmiş haline dendiği örneklerle de desteklenerek aktarılmalıdır. Akabinde eğitim alan bireylerden sahip oldukları bir takım bilgilerin neler olduğu yönünde onları düşünmeye sevk etmek ve bazı örnek bilgileri beraberce ele alıp değerlendirerek, bireyler üzerinde sahip oldukları yada olacakları temel bilgiler konusunda farkındalık oluşturulmalıdır.

2.1.2. Bilgi'nin bulunduğu ortamlar

Bilgiler pek çok ortamlarda bulunabilir, iletilebilir ve işlenebilir. Sahip olunan bilgilerin temelde hangi platformlarda bulunduğuna ya da bulunacağına yönelik çalışanlara bilgilendirmeler yapılır.

Bilginin yer aldığı belli başlı ortamlar;

- Fiziksel ortamlar; Kâğıt, tahta, pano, faks, Çöp/Atık kağıt kutuları, Dolaplar vb
- Elektronik ortamlar; Bilgisayarlar, mobil iletişim cihazları, e-posta, USB, CD, Disk, Disket vb manyetik ortamlar.
- Sosyal ortamlar; Telefon görüşmeleri, muhabbetler, yemek araları, toplu taşıma araçları vb sosyal aktiviteler.
- Tanıtım platformları; internet siteleri, broşürler, reklamlar, sunular, eğitimler, video yada görsel ortamlar.

Bu bölümde yukarıda yer alan genel bilgilendirmenin yanında bireylere sahip oldukları ya da olacakları bilgilerin kurumda hangi platform ve ortamlarda yer aldığı konusunda da bilgi verilmeli. Bu onlara o bilgilere erişmek istediklerinde nasıl erişebilecekleri hakkında da bilgilenmelerini sağlanır. Burada, bilgi güvenliğinden beklenenin sadece "gizlilik" ve korumadan ibaret olmadığını gizliliğin yanında "bütünlük" ve "erişilebilirlik" niteliklerini de unutmamak gerekir.

2.1.2. Bilgi'nin Korunması

ISO bilgi güvenliği standartları tabiriyle; "Bilgi, bir kurumun en önemli değerlerinden biridir ve sürekli korunması gerekir". Eğitimde, önceki bölümlerde tanımlaması yapılan değerli varlıkların bu bölümde ise korumanın nasıl ve bilginin hangi niteliklerini, kısacası neyini korumak gerektiği konusunda bilgilendirmeler yapılır.

Bilginin korunacak temel nitelikleri(ISO 27001);

- Gizlilik: Bilginin yetkili olmayan kişiler, varlıklar ve süreçler tarafından erişilemez ve ifşa edilemez niteliği
- Doğruluk, Bütünlük ve Özgünlük: Bilginin doğruluk, bütünlük ve kendisine has özelliklerinin korunması,
- Kullanılabilirlik(erişilebilirlik): Bilginin yetkili kişiler(görevi gereği) tarafından istenildiğinde ulaşılabilir ve kullanılabilir olma özelliğine denir.

2.2. Bilgi Güvenliği ve Tehditler

Bu bölümde günün şartlarına göre bilgi güvenliğini tehdit eden unsurlar hakkında bilgilendirmeler yapılmalı, eğitime katılan kişilerden yaşadıkları, gördükleri ya da duydukları çeşitli bilgi güvenliği tehditleri, olayları hakkında varsa örnekler alınarak aktif katılımları sağlanmalıdır.

Bilgi güvenliğine yönelik belli başlı tehditleri Şekil-1'de de gösterildiği gibi aşağıdaki başlıklar altında toplayabiliriz.

Şekil 1: Bilgi Güvenliği ve Tehditler

- Doğal tehditler; yangın, sel, yıldırım vb doğal afetler ve bunların bilgiler üzerinde oluşturabilecekleri tehditler.
- Zararlı yazılımlar; virüsler, trojan'lar, truva atları, casus yazılımlar(spyware, spyware cookie), spam, exploit, keylogger, botnet, sniffer, phishing vb
- Sosyal mühendislik
- Güvenlik açıkları ve Fiziksel Güvenlik
- Korsanlar ve Erişim; Korsanlar ve bilgiye erişime yönelik tehditler

Bilgi güvenliğine ilişkin tehditler eğitim verilecek kesime ve beklentilerine göre çeşitlendirilmeli ve detaylandırılmalıdır.

2.3. Temiz Masa Kuralları

ISO/IEC 17799 standardında da yer aldığı şekilde kurumlar çalışanların mesai saatleri içi veya dışında kendilerine görevleri gereği paylaşılmış olan bilgilerin yetkisiz erişimler veya uygunsuz kullanımı sonucunda başına gelebilecek riskleri ortadan kaldırabilmek için temiz masa temiz ekran politikaları oluşturmasını ve bunu çalışanlara aktarmasını istemektedir. Masalarda ya da çalışma ortamlarında korumasız bırakılmış bilgiler yetkisiz kişilerin erişimleriyle gizlilik ilkesinin ihlaline, yangın, sel, deprem gibi felaketlerle bütünlüğü'nün bozulmalarına ya da yok olmalarına sebep olabilir.

Tüm bu veya daha fazla tehditleri yok edebilmek için ilgili standartta tavsiye edilen ve aşağıda yer alan belli başlı temiz masa kurallarına ilişkin politikalar geliştirilmeli ve bu politikaların çalışanlar tarafından haberdar olunması sağlanmalıdır.

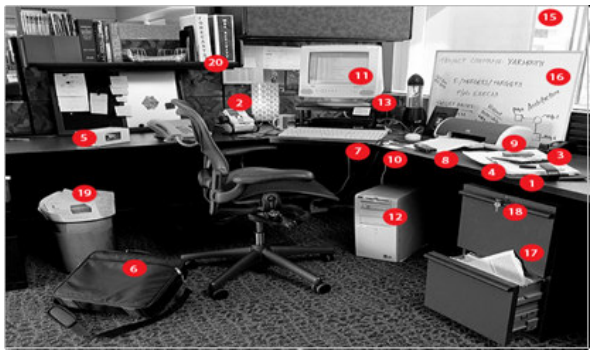
Belli başlı temiz masa kuralları;

- Çalışma sonunda kağıt ortamında yada elektronik cihazlar üzerinde tutulan "gizli yada çok gizli" bilgiler güvenlikli ortamlarda (çelik kasa, kilitli güvenli ortamlar vb) saklanmalı,
- Kullanım ömrü sona eren, artık ihtiyaç duyulmadığına karar verilen bilgiler kağıt öğütücü, disk/disket kıyıcı, yakma vb metotlarla imha edilmeli, bilginin geri dönüşümü ya da yeniden kullanılabilir hale geçmesinin önüne geçilmelidir,
- Her türlü haberleşmede kullanılan cihazlar (telefon, faks, fotokopi makineleri) başı boş yetkisiz erişimlere açık bir şekilde konumlandırılmamalı, bu cihazlar üzerinde bilgi ve belge bırakılmamalıdır,
- Her türlü bilgiler, şifreler, anahtarlar ve bilginin sunulduğu sistemler, ana makineler(server), pc'ler vb. cihazlar yetkisiz kişilerin erişebileceği şifresiz ve korumasız bir şekilde başıboş bırakılmamalı,
- Hassas bilgiler her tülü yağmur, sel, yangına karşı korunaklı yerlerde saklanmalı,

Şeklinde özetleyebiliriz.

Bu temel bilgiler aşağıdakine benzer bir örnek üzerinden bireylerin katılımını da sağlayacak şekilde etkileşimli bir biçimde verilerek, bilgilerin çalışanların zihninde daha canlı tutulması sağlanabilir.

Burada önemli husus çalışanın kurumdaki hangi bilginin hangi güvenlik sınıfında olduğunu önceden biliyor olması ya da bu bilgilere erişebiliyor olmasının gerekliliğidir. Aksi takdirde çalışan hangi bilgiyi hangi güvenlik seviyesinde koruması gerektiğini karıştırabilir.



Şekil 2: Temiz masa ve bilgi güvenlik ihlalleri

Pek çok bilgi güvenlik ihmali olan ve olması gereken "temiz masa temiz ekran kuralları"nı ihlal eden unsurlar Şekil-2'de gösterilmektedir.

2.4. Şifre güvenliği

Elektronik ortamlarda yada kasalarda korumalı bir şekilde tutulan bilgilere erişmede kullanılan şifrelerin korunması, bilgi güvenliği risklerini önlemede hayati öneme sahiptir. Bu bakımdan kurumlar şifrelerin korunmasına yönelik çeşitli kurallar ve politikalar geliştirilmeli ve bunları çalışanlarıyla paylaşmalıdır.

Şifre güvenliğini sağlamaya yönelik kurallardan bazıları aşağıda şekilde özetlenebilir;

- Şifre Seçimi; şifreler başkaları tarafından kolayca tahmin edilemeyen, kullanıcı hakkında özel bilgileri(doğum tarihi, çocuk bilgisi, araç plaka numarası vb) içermeyecek, içerisinde büyük küçük harflerin, sayıların ve özel karakterlerin karışımından oluşmalı. Şifre karakter boyutu en az 8 karakter olarak belirlenmeli.
- Koruma; Şifreler kağıt ortamlar üzerine yazılmamalı, başkalarıyla paylaşılmamalı, şifrelerin tutulduğu ortamların güvenliği sağlanmalı, güvenliğinden şüphe edilen durumlarda yetkililer bilgilendirilmeli ve gerekiyorsa şifre değiştirilmeli,
- Gizlilik; Kullanıcılar şifrelerini gizli tutulmalı ve kimseyle paylaşmamalı, şifre güvenliğinden şüphelendiği durumlarda derhal şifrelerini değiştirmeli, gerekiyorsa yetkililere haber vermeli,
- Düzenli Gözden Geçirme; Şifreler düzenli olarak kritiklik durumuna göre en fazla üç ayda bir düzenli olarak gözden geçirilip değiştirilmeli,

2.5. Yasal Düzenlemeler

Çalışanları bekleyen ve sorumlu oldukları yasal düzenlemeler hakkında bilgilendirilmelidir. Bu bağlamda kurum ve bireyin bağlı olduğu yasal düzenleyicilerin belirlediği kurallar ve bu kurallarının getirdiği yükümlülükler hakkında bireylere özet bilgilendirme yapılmalı.

Kurum ve bireylerin bağlı olduğu belli başlı yasal düzenlemelere;

- 1951 tarih ve 5846 sayılı Fikir ve Sanat Hakları Kanunu,
- 2004 tarih ve 5237 sayılı Bilişim Suçları Kanunu,
- Kurumların bağlı olduğu yasal düzenleyiciler (BDDK, YÖK, Bakanlıklar, Sayıştay vb) tarafından konulan yükümlülükler,
- 2007 tarih ve 5651 sayılı 'İnternet üzerinden yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkındaki kanun'

Örnek olarak verilebilir.

2.6. Bilgi Güvenlik Politika Beklentileri

Bu bölümde çalışanlar veya eğitime tabi tutulan bireylere kurum bilgi güvenlik politikası ve/veya kuralları, çalışan sorumlulukları ve kendilerinden beklenenler hakkında bilgilendirilmelidir.

3. SONUÇ

Güvenliğin en zayıf halkası olarak da kabul edilen insana yapılacak bilgi güvenlik bilinçlendirme faaliyetleri kurumlara bilgi güvenliğini sağlamada çok büyük katkılar sağlayacağı unutulmamalıdır. Bu eğitim ve farkındalık programları, en üst yönetimlerden başlayarak en alt seviyedeki uç bir kullanıcıya kadar yaygınlaştırılmalı ve sunulmalıdır.

Kurumlar ve bireyler ellerindeki değerli varlık olan bilgiyi korumak, bütünlüğünü ve güvenilirliğini sağlamak, gerektiğinde ise ulaşabilmek için bir bilgi güvenlik politika ya da kuralları etrafında birleşmeli, aynı zamanda kendilerine yol gösterici olan bu kurallardan öncelikle haberdar olmalıdır. Diğer taraftan güncel ne tür bilgi güvenlik risk ve tehditleriyle karşılaşabilecekleri konusunda da bilgi sahibi olmalıdırlar. Bu farkındalığı oluşturmada en temel ve etkili yöntem ilgili bireylerin bir farkındalık eğitim programından geçirilmesiyle mümkün olabilecektir.

Farkındalık eğitimi vermek isteyen kurumlar içerik olarak ne sunacakları konusunda bilgiye ihtiyaç duymakta ve arayış içerisine girebilmektedirler.

Sonuç olarak; bu çalışma ile kurumlara, bu yönde eğitim vermek isteyen ya da bilgilenmek isteyen bireylere, kendi tecrübe ve deneyimlerimizden bir bölümünü, örnek ve yol gösterici olması açısından temel seviyede sunmaya çalışıldı.

Bununla birlikte bunun çok temel bir seviye olduğu, bireylerin seviyeleri, kurumun o kesime yüklediği sorumluluk ve beklentileri dikkate alınarak eğitim farklı kategorilere/gruplara özel hazırlanmalı, gerektiğinde temel seviyenin üzerine dönemsel olarak diğer eğitimler verilerek bilinç seviyesi en üst düzeyde tutulmaya çalışılmalıdır.

4. KAYNAKÇA

[1] ISO/IEC 17799 Information Technology- Code of practice for information security management

[2] ISO/IEC 27001 Information Security Management System

[3] BANK ASYA, Temel Bilgi Güvenliği Eğitim Çalışma Notları

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