Son Kullanıcılarda Bilgi Güvenliği Farkındalığı Oluşturma Yöntemleri

Faruk YAKARYILMAZ

1. Giriş

Bilgi, bugüne kadar yapılmış bütün tanımların dışında: İnsanların nesneler ve olaylar arasındaki birbirlerini etkileyen ve tetikleyen ilişkilerini anlamalarına hizmet eden ve insanoğlunun nesneler ve olaylar üzerindeki baskı ve gücünü arttıran bir unsurdur.

Emile Brehiere göre, "bilgi eşyanın yüzeyinde dolaşmaz; bilgi, varlığın içerisinde ve derinliklerindedir" (Brehiere, 1948). 21.YY' da bilgi; insan-doğa mücadelesinde veya insan-insan, devlet-devlet arasındaki mücadelelerde hâkimiyeti temsil eden yegâne unsur haline dönüşmüştür.[1]

Francis Bacon ve Auguste Comte, bilgiye sahip olmanın önemini "egemen olmak için bilmek" (Bacon, 1626) şeklinde ifade etmişlerdir.[2]

2. Farkındalığın Ana Başlıkları

2.1 Kurumlarda Bilgi Güvenliği

Bir kurum için en değerli varlık "bilgi" olarak bilinmektedir. Kurumlarının birinci derecede önceliği: bilginin kaybolmasını, zarara uğramasını, yok edilmesini, yetkisiz ve kötü niyetli kişilerin eline geçmesinin engellenmesi yönünde politikalar belirlemek olmalıdır.

2.2 Bilgi Güvenliği Nedir?

McCumber'in "Bilgi ve bilgi sistemlerinin yetkisiz erişim, kullanım, ifşa edilmesi, bozulması, değiştirilmesine veya bilginin gizlilik, bütünlük ve kullanılabilirliğine zarar vermek için yapılan kötü niyetli girişimlere karşı sağlanacak koruma" şeklinde yapmış olduğu tanım, en kapsamlı ve bugünün koşullarını içine alan bilgi güvenliği tanımlarından biridir. (McCumber, 2005)[3]

3. Tehdit ve Riskler

Bilgi güvenliği ve mahremiyeti tehdit eden unsurlar hakkında belirlenmiş zaman dilimlerinde bilgilendirmeler yapılmalıdır. Bu konuyla ilgili yaşanmış örnekler, bilgilendirilen kişilere aktarılmalıdır. Personellerinize, çalışanlarınıza ya da bilgilendirme yaptığınız topluluğa, bilgi güvenliği kavramının sadece bilgi teknolojilerini ilgilendirmediğini iyi anlatabiliyor olmanız gerekmektedir.

3.1 Tehdit Unsurları

3.1.1 Sosyal Mühendislik
3.1.2 Zararlı Yazılımlar
3.1.3 Fiziksel Güvenlik
3.1.4 Güvenlik Açıklıkları
3.1.5 Doğa Tehditleri
3.1.6 Erişim İhlalleri

---

[1] http://edergi.atauni.edu.tr/ataunikkefd/article/viewFile/1021004004/1021003828

[2] https://ebooks.adelaide.edu.au/b/bacon/francis/b12n/

[3] http://www.bby.hacettepe.edu.tr/yayinlar/dosyalar/Henko%C4%9Flu.pdf

Tehdit unsurları, yukarıdaki maddeler karakteristik olacak şekilde, farkındalık oluşturulacak kitleye ve meslek gruplarına göre değişiklikler gösterebilir.

3.1.1 Sosyal Mühendislik

Eski bilgisayar korsanı Kevin Mitnick'in popüler hale getirdiği sosyal mühendislik terimi, insanları istemedikleri bir şeyler yapmaya ya da gizli bilgilerini elde etmek için kandırma eylemidir. [4] Kullanıcıların kendilerini bu tehditlere karşı korumalarının en etkili yolu, bilgi sahibi olmaktır. Nelere karşı tetikte olacaklarını, nelerden kaçınacaklarını ve nelere dikkat edeceklerini bilmeleri gerekmektedir.[5]

3.1.2 Zararlı Yazılımlar

Bilgisayar sistemlerine zarar vermek, bilgi çalmak veya kullanıcıları rahatsız etmek gibi amaçlarla hazırlanmış yazılımlara genel olarak verilen ad. Bu yazılımlara örnek olarak virüsler, solucanlar, truva atları, rootkitler verilebilir. Genellikle yazılım (software) olarak tanımlanmalarına rağmen bazen basit kodlar halinde de olabilirler

3.1.3 Fiziksel Güvenlik

İşyerine yetkisiz erişimlerin engellenmesi ve bilgi varlıklarının hırsızlığa veya tehlikeye karşı korunmasıdır.[6] Bilginin, bilgi varlıklarının güvenliğini sağlamak için bir çok yöntem olsa da çoğu zaman fiziksel koruma yeterli olmamış ve bilgilerin çalınması ve başka kişilerin eline geçmesi engellenememiştir. Bu durum, verileri korumak için fiziksel güvenliğin tek başına yeterli olmadığını göstermektedir. Örneğin, bina etrafına yüksek duvarlar ya da demirler yapılması, bina girişinde özel güvenlik ekiplerinin bulundurulması, önemli verilerin tutulduğu odaların kilitlenmesi ya da bu odalara şifreli güvenlik sistemleri ile girilmesi gibi önlemler kullanılması gerekmektedir.

3.1.4 Güvenlik Açıklıkları

Yazılımlarda zaman zaman hatalar veya eksiklikler keşfedilir. Bilgisayar sistemlerini dışarıdan gelecek açık hale getiren bu zaaflara **güvenlik açıklığı** denir ve ancak yazılımlar **güncellenerek** kapatılabilir.

3.1.5 Doğa Tehditleri

Deprem, sel, toprak kayması, fırtına, yıldırım düşmesi gibi tehditler doğa tehditlerine örnek verilebilir. Örnek olarak, bilişim sektöründen bir firmanın karşılaşabileceği tehditler ve tehdit unsurları ile tehdit kaynakları aşağıdaki Tablo-1'de gösterilmiştir.

Tablo 1: Tehdit ve Tehdit Kaynakları

Tehdidin kaynağı bölümünde kullanılan kısaltmalar B: İnsan kaynaklı ve bilerek, K: İnsan kaynaklı ve kazayla, D: Doğal, Ç:Çevresel

Tehdit	Tehdit Kaynağı
Deprem	D
Sel	D
Fırtına	D
Yıldırım	D
Endüstriye Bilgi Sızıntısı	B,K
Bombalama ve Silahlı Saldırı	B

[4] http://en.wikipedia.org/wiki/Social_engineering_(security)
[5] http://www.trendmicro.com.tr/media/resource_lib/social/5-reasons-why-social-engineering-tricks-work-tr.pdf
[6] http://www.cagataycebi.com/security/fiziksel_ve_cevresel_guvenlik.pdf

Yangın	B,K
Güç Kesintisi	B,K,Ç
Su Kesintisi	B,K,Ç
Havalandırma sisteminin arızalanması	B,K,Ç
Donanım arızaları	K
Güç dalgalanmaları	K,Ç
Tozlanma	Ç
Elektrostatik boşalma	Ç
Hırsızlık	B
Saklama ortamlarının izinsiz kullanılması	B,K
Saklama ortamlarının eskiyip kullanılmaz duruma gelmesi	B,K
Personel hataları	K
Bakım hataları/eksiklikleri	K
Yazılım hataları	B,K
Lisanssız yazılım kullanımı	B,K
Yazılımların yetkisiz kullanılması	B,K
Kullanıcı kimlik bilgilerinin çalınması	B,K
Zararlı yazılımlar	B,K
Yetkisiz kişilerin ağa erişimi	B
Ağ cihazlarının arızalanması	K

[7]

3.1.6 Erişim İhlalleri

Erişim ihlali, bilgisayar sisteminin tamamına veya bir bölümüne, bu eylem için hazırlanmış programlar, çeşitli virüs programları, casus yazılımlar yolu ile ulaşılmasıdır. Kişilerin özel hayatının gizliliğinin korunması çerçevesinde, dinleme, izin alınmaksızın kişisel veya şirket bilgisayarına erişim hukukende suçtur. Bu durum Türk Ceza Kanunu'nun Bilişim Alanında Suçlar Başlığı altındaki 243. maddesinde tanımlanmıştır.

4. Yöntem ve Usul

Bilgi güvenliğine yönelik tehditlerin seviyesini azaltmak, kurumda bütün çalışanların katılımını sağlamak ve basit ya da değersiz görülen önleyici tedbirlerin uygulanmasını sağlamak gerekmektedir.

4.1 Temiz Masa-Temiz Ekran Kuralı

Firmaların bilgi güvenliği politikasının bir parçasıdır ve maksadı, ilgisiz kişilerin firmaya ait bilgileri ele geçirme çalışmalarını etkisiz kılmaktır. Ayrıca, etrafa özensiz olarak bırakılan eşyaların ofis içi kazalara sebep olma riski de azalacağından personel güvenliği riskini de minimize eder. Temiz Masa Kuralı, **uygulanması en basit** güvenlik tedbirlerinden birisi olmasına rağmen, aynı zamanda **uygulama seviyesi en düşük** olanıdır. Temiz masa politikası ile ilgili uygulanması gereken maddeler;

• Çalışma sonunda kâğıt ortamında ya da elektronik cihazlar üzerinde tutulan "gizli ya da çok gizli" bilgiler güvenlikli ortamlarda (çelik kasa, kilitli güvenli ortamlar vb) saklanmalı,

• Kullanım ömrü sona eren, artık ihtiyaç duyulmadığına karar verilen bilgiler kâğıt 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) başıboş yetkisiz erişimlere açık bir şekilde konumlandırılmamalı, bu cihazlar üzerinde bilgi ve belge bırakılmamalıdır,

[7] http://www.saglik.gov.tr/TR/dosya/1-101521/h/bilgiguvenligipolitikalarikilavuzu.pdf

• Her türlü bilgiler, şifreler, anahtarlar ve bilginin sunulduğu sistemler, ana makineler(server), bilgisayarlar vb. cihazlar yetkisiz kişilerin erişebileceği şifresiz ve korumasız bir şekilde başıboş bırakılmamalı,

• Hassas bilgiler her tülü yağmur, sel, yangına karşı korunaklı yerlerde saklanmalıdır.[8]

4.2 Parola Güvenliği

Kullanıcıların veya çalışanların güçlü parola oluşturması, parolasını güvende tutması gerekmektedir. Bu bilgiler çerçevesinde öncelikle güçlü parola oluşturmak gerekmektedir. Tahmin edilmesi kolay olmayan ya da deneme yanılma yolu ile **ele geçirilmesi oldukça zor olan** parolalara **güçlü parola** denir.

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

Bu kurallara uygun parola oluştururken genelde yapılan hatalardan dolayı saldırganların ilk olarak denedikleri parolalar vardır. Bu nedenle parola oluştururken aşağıdaki önerileri de dikkate almak gerekir.

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

Güçlü gibi görünse de çok kullanılan ve çok kolay tahmin edilebilen parolalardan kaçınmak gerekmektedir. Bu parolalar klavyedeki harf sırası, alfabedeki harf sırası gibi popüler kurallardan oluşturulmaktadır.

Örnek Olarak:

- "123qwe", "qwe123", "123qweasd", "qwer1234", ...
- "qweasd", "123QweAsd", "asd12345", "Asd123", ...
- "qwerty", "qwerty123", "qazwsx123", ...
- "abc123", "123abc", "1234abcd", ...
- "123456", "987654321", "1234qqqQ", ...[9]

Kullanımlarının güvenlik zafiyeti yaratacağı düşünülmektedir.

4.3 Sistem Güvenliği

Donanım ve Yazılım güvenliği kapsamında kullanıcılara veya çalışanlara;

- Donanım veya yazılımların güvenlik açığına sebep olabileceği,
- Donanım veya yazılımların sistemin çalışmasını engelleyebileceği veya durdurulabileceği,
- Kopya veya lisanssız yazılımların hukuki problem oluşturabileceği,
- İnternetten indirilen kırılmış (crack) yazılımların güvenlik açığına sebep olabileceği,
- Kırılmış (crack) yazılımların zararlı yazılım, Truva yazılımı ve arka kapı (malware, trojan veya backdoor) taşıyabileceği bildirilmelidir.

Ayrıca kullanıcılara veya çalışanlara virüs kavramı ile ilgili bilgilendirmelerin zaman zaman yapılması gerekmektedir. Virüslerin indirilen dosyalardan, usb ya da harici belleklerden, korsan yada lisanssız

[8] http://ab.org.tr/ab09/bildiri/117.pdf
[9] http://www.bilgimikoruyorum.org.tr/?b222_guclu_parola_olusturma

yazılımlardan ve e-posta yoluyla bulaşabileceği ve barındırdıkları riskler, kullanıcılara\çalışanlara bildirilmesi ve bu bilgilerin güncelliğini koruyarak iletiminin sağlanması gerekmektedir.[10]

5. Herkes İçin Farkındalık

Kurumlarda, üniversitelerde, kişisel kullanım alanlarında kısacası toplumun her kesiminden her insanda farkındalık oluşması için sosyal hayatın her noktasında kullanılabilecek bilgilendirme afişleri ve broşürler kullanılmalıdır.

Örnek olarak;

Resim 1 : Bilgisayarını Kilitlemeyi Unutma

Resim 2: Bilgisayarınızı Terk Ettiğinizde Kilitleyin.

[10] http://slideplayer.biz.tr/slide/1925082/

Resim 3: Kişisel Bilgilerinizi İsteyen E-Postalara Dikkat Edin.

5.1 Farkındalık Günü

Farkındalık bilincinin oluşturulması ve farkındalık kültürüne katkı sağlamak için organizasyonlarda her ayın bir gününün seçilerek farkındalık günü oluşturulması olumlu anlamda bir katkı sağlayacaktır.

6. Kaynakça

[1] Bacon F. "The New Atlantis", 1620, S:13.
[2] Brehiere E. " Science et Humanisme", 1948,S :54.
[3]Mccumber J. "Assessing and managing security risk in IT systems",2005, S:23