T.C. İSTANBUL TİCARET ÜNİVERSİTESİ

DIŞ TİCARET ENSTİTÜSÜ

WORKING PAPER SERIES

Tartışma Metinleri

WPS NO/ 43/2016-06

SİBER SUÇLARIN TESPİTİNDE İÇ DENETİM UYGULAMA ÖRNEĞİ

Rengin KAVCI*

* rkavci@teknosa.com, İstanbul Ticaret Üniversitesi, Sosyal Bilimler Enstitüsü, İşletme Tezli Yüksek Lisans Öğrencisi

Siber Suçların Tespitinde İç Denetim Uygulama Örneği

Özet

Yaşam şartlarının gün geçtikçe zorlaşması; az zaman harcayarak ihtiyaçların karşılanması gereksinimini giderek arttırmaktadır. Bilgi ve iletişim teknolojilerinde hızla meydana gelen gelişmeler ile günlük işlerin mekan değişikliğine ihtiyaç duyulmaksızın yapılmasına imkan sağlayarak hayatı kolaylaştırmaktadır. Aynı zamanda kötü niyetli kullanıcılar tarafından bilgisayar ağları yoluyla çeşitli suçlar işlenmesine, suç mağdurlarının oluşmasına ve şirketler açısından da yeni tehditlere de sıkça rastlanmaktadır. Bu durum şirketler bakımından özellikle finansman kaybı, itibarın zedelenmesi gibi risklere sebep olmaktadır. Yaşam koşullarını olumsuz etkileyen bu suçlarla mücadele edebilmek adına yasal düzenlemeler geliştirilmiş ve güvenlik anlamında standartlar getirilmiştir. İşletmeler ise bu kayıpları ortadan kaldırılabilmek ya da risklerini en aza indirilebilmek için çözümler geliştirmekte ve yatırımlar yapmaktadır.Çalışmada gerçekte yaşanmış bir olay ele alınmıştır. Online satış yapmayan fakat internet sitesini sadece ürünlerin tanıtımları amacıyla kullanmakta olan bir şirketin internet sitesi taklit edilerek dolandırıcılık olayının gerçeklemesi sonucu oluşan kayıplar, müşteri mağduriyeti ve şirketin bu olaya yaklaşım yöntemi incelenmiştir. Bu süreçte yaşanan risklerin nasıl değerlendirildiği, ne tür önlemlerin alındığı ve iç kontrol sisteminin yeterliliği irdelenmiştir.

Anahtar Kelimeler: Bilişim Teknolojileri, Siber Suçlar, Online Satış, İç Kontrol.

Abstract

Life standart and conditions are getting difficult day by day. Necessity of satisfy the needs are decreasing in the same direction. Development of information and communication systems play a big role doing this quick and pratically. In the same time, these improvements occur cyber crime, new company threats and new victims. This situation causes financial loss and bad reputation especially in companies. The goverment created specific legal rules and security standarts in order to tackle them and companies make investments for none or minimum loss.In this study, examined approach of the firm which doesnt sell as online and just display products on website, when facing fraud by imitating. And also examined way of risk evaluation measures taken and sufficiency of internal audit system.

Keywords: IT Technologies, Cyber Crimes, Online Shopping, Internal Audit

Giriş

Gün geçtikçe artan oranda gelişme gösteren bilişim teknolojileri internet kullanımını gün geçtikçe yaşamın vazgeçilmezi haline getirmektedir. Online işlem yapan kullanıcı sayısı da aynı oranda artmaktadır. Bu durum şirketlerin büyümesi ve gelişmesi açısından büyük fırsat olarak değerlendirmekte ve internet aracılığıyla az maliyetle yeni pazarlara açılma olanağı sağlamaktadır. Bu durum şirketler açısından tamamen dışa açık bir sistem gerektirmekte ve bilgisayar ağları arasındaki bağlantıları arıttırmaktadır. Böyle bir işleyiş şirketlerin internet ile dış dünyaya açılmaları ve online olarak faaliyetlerini sürdürmeleri sadece şirket içinden değil şirket dışından da hırsızlık, dolandırıcılık gibi tehditlerin oluşmasına sebep olmaktadır. Artan bu tehditler güvenlik boyutunda yeni kaygıların ortaya çıkmasına sebep olmaktadır. Bu yüzden şirketler bilgi sistemlerini tehdit eden iç ve dış tehditlere karşı güvenlik önlemleri almaları alınan güvenlik önlemlerinin de gelişen teknoloji ile geliştirmeleri gerekmekte ve kendi iç kontrol sistemini yapılandırarak siber suç risklerini azaltmak adına bu alandaki yatırımlara öncelik vermek zorunda kalmaktadır.

1. Bilişim Teknolojileri ve E-ticaret

Bilişim teknolojisi; bilginin toplanması, depolanması, üzerinde çalışılması, saklanması, ağlar aracılığıyla bir yerden bir yere aktarılması gibi işlemlerin kullanıcıların hizmetine sunulmasında kullanılan iletişim araçları ile bilgisayarlar dâhil bütün teknolojileri kapsamaktadır (Soysal, 2015, s. 6).

Günümüz dünyasında bilgi teknolojilerindeki gelişme ve değişim ticaret hayatını da etkilemiştir. İşletmelerin istikrarlı büyüme göstererek kalıcı olabilmesi için gelişen teknolojilere ayak uydurarak pazar payını arttırması ve rekabet koşullarına uyum sağlamak adına ticareti internet üzerinden yapılmaya başlama gereksinimi doğmuştur. Bu doğrultuda şirketlerin bilişim teknolojisine duyduğu ihtiyaç artmaktadır. İşletmelerin internet aracılığıyla yeni tüketici kitlelerine ulaşmak adına internet üzerinden satış yapmaya başlayarak e-ticaret hizmeti vermeye başlamıştır (Kul, 2009, s. 233-234).

E-ticaret, tüm dünyada ticaretin serbestleştirilmesi ile birlikte özellikle, son yıllarda yaşanan ve bilgi iletişimini kolaylaştıran teknolojik gelişmelerin bir ürünü olarak ortaya çıkmaktadır (Torlak, 2013, s. 1).

E-ticaretin şirketlere fiziki mağaza ortamından sıyrılarak kısıtlayıcı zaman problemini ortadan kaldırmış ve 7/24 online satış imkanı sağlaması, müşterilere ulaşma konusunda coğrafik sınırları ortadan kaldırması, insan unsurunu en aza indirdiği için maliyetleri azaltması vb. gibi avantajlarının yanı sıra bazı tehditleri de barındırmaktadır. Bu tehditler; şirketlerin finansal verilerinin çalınması, sisteme virüs bulaştırılması, ticari gizlilik içeren dosyaların çalınması, müşteri kredi kart bilgilerinin çalınması vb. olarak sayılabilmektedir (Büyükyıldırım, 2014, s. 4).

2. Siber Suç ve Siber Güvenlik

Bilişim teknolojilerindeki gelişmeler sonucunda, merkezi yapılar yerlerini internet ve ağlar üzerinden erişilebilen elektronik uygulamalara bırakmıştır. İnternetin kullanımının artması ve yaygınlaşmasına paralel olarak güvenlik tehditleri ve riskleri aynı oranda artmıştır. Teknik güvenlik önlemlerinin gelişmesine rağmen bilişim teknolojilerine karşı yapılan saldırıların sayısının artması ve yüksek boyutlarda etki yapan hasarlar oluşturması, teknik yöntemlerin bilgi güvenliğinin sağlanmasında yetersiz kaldığını göstermektedir. Bilgi güvenliğinin sağlanabilmesi için teknik önlemlerin yanında idari önlemler yani kurallar, cezalar vb., standartlar ve insan faktörü göz önüne alındığında bilgi güvenliği karmaşık çözümler içeren ve yönetilmesi mecburi hale gelen bir süreç olmuştur (Tekerek, 2008, s. 132).

Herhangi bir suçun elektronik ortam üzerinden işlenebilme imkanı bulunuyorsa ve bu ortam içerisinde gerçekleştirilen eylem hukuka aykırı veya suç olarak tanımlanabiliyorsa bu suçlara siber suçlar denilmektedir (Yıldız, 2014, s. 4).

2.1. Siber Suçların İşleniş Şekilleri

Siber suçlar klasik suçlara amaç açısından benzerlik göstermekle beraber yöntem olarak büyük ölçüde farklılıklar göstermektedir. Siber suçlar fiziksel olarak herhangi bir hareket eylemi gerçekleştirmeden bir bilgisayar ve internet ağı kullanarak herhangi bir yerde suçu işleyebilmekte ve suçun gerçekleşmesi sonucunda büyük zararlar oluşabilmektedir. Siber suç sürekli değişen ve hızla artan bir suç türü olup zaman ve mekan kavramı olmadan her an gerçekleşme riski vardır (Akarslan, 2011, s. 15). Aşağıda bugüne kadar sıkça karşılaşılan başlıca siber suç işleniş şekilleri sıralanmıştır:

- Zararlı Yazılımlar
- Salam Tekniği
- Sistem Güvenliğinin Kırılarak İçeri Girilmesi
- İstem Dışı Alınan E-postalar
- Süper Darbe
- Gizli Kapılar
- Eş Zamansız Saldırılar
- Yerine Geçme
- Web Sayfası Hırsızlığı ve Yönlendirme
- Yanlış Yazanları Yakalama
- Klavye İşlemlerini Kaydeden Programlar
- IP Adresi Gizleme
- SQL Enjeksiyonu
- İnternet Dolandırıcılığı
- Oltaya Gelme

2.2. Siber Güvenlik

Birçok ülke güvenlik politikalarının içerisinde önemli bir başlık olarak siber güvenliğe yer vermeye başlamıştır. Bu ülkelerin bazıları ekonominin, sosyal yaşamın vb. sanal dünya ile giderek iç içe girmesi sebebiyle siber güvenlik alanına büyük yatırımlar yapmakta ve bu alanda önemli maliyetlere katlanmaktadır (Yıldız, 2014, s. 58).

Siber güvenlik; şirketlerin ve kullanıcıların bilgi varlıklarını korumak amacıyla kullanılan yöntemler, politikalar, risk yönetimi yaklaşımları, faaliyetler ve kullanılan teknolojilerin bütünlüğünü, gizliliğini ve elde edilebilir olmasını kapsamaktadır (Tıngöy, 2009, s. 78).

E-ticarette özel bir kodlama sistemi temeline dayanan SSL ve SET olmak üzere iki güvenlik sistemi bulunmaktadır (İçli ve Aslan, 2008, s. 3).

SSL (Secure Sockets Layer): SSL hem gizli anahtarlar ve hem de ortak anahtar teknolojilerini kullanan güvenlik protokolüdür (Barışık ve Temel, 2007, s. 140-141). İnternet sitesine SSL protokolü ile ulaşıldığında, tarayıcı ve sunucu arasında şifreli bir

oturum başlar ve bu şifreli oturum başkalarının izlemesine olanak tanımayan bir seviyeye getirilmektedir (Diker ve Varol, 2013, s. 32).

Bu işlemler yapılarak kredi kartı ve kişisel bilgilerin gizliliği ve bütünlüğü korunmuş olmaktadır (Dondurmacı ve Çınar, 2014, s. 175).

SET (Secure Electronic Transaction): E-Ticarette güvenli bilgi aktarımını sağlamak, özellikle de kredi kartı işlemlerini güvenli hale getirmek amacıyla oluşturulmuştur (Büyükyıldırım, 2014, s. 28).

3. Bir Online Tanıtım Firmasının İç Denetim Uygulaması ve Suistimal Vakası Örneği

Çalışmamızda ele alınan internet sitesi örneğinde; sadece bayi ve şube kanalıyla satışını gerçekleştirdiği ürünlerin tanıtımını yapmak amacıyla kullanan bir kurumsal şirketin sistem güvenliği kırılarak sistemdeki müşteri bilgilerine erişim sağlandığı ve oltaya gelme yöntemi kullanılarak gerçekleştirilen bir siber suç olayı ele alınmıştır. Oltaya gelme yöntemi kullanılarak oluşturulmuş olan sahte internet sitesinin sadece tasarımı değil internet adresi de aynı şekilde gerçek adrese çok benzemektedir. Bu sebeple aynı zamanda internet üzerinden bu şirketin sayfasına erişim sağlamak isteyen diğer kullanıcılar arasından yanlış yazanları yakalama yolu ile de dolandırıcılık olayı gerçekleşmiştir.

Şirketin internet site ile birebir aynı tasarıma sahip sahte bir internet sitesi yapılarak online satış kısmı eklenmiştir. Sonrasında ilgili şirketin sistem güvenliği kırılarak elde edilmiş olan müşteri e-posta adreslerine sahte internet sitesinin linkinin bulunduğu ve ilgili şirketin logosunun yer aldığı satış kampanya duyurusunu içeren bir e-posta eşzamanlı olarak gönderilmiştir. Bu e-posta aracılığı ile çok sayıda kullanıcı internet sitesini ziyaret ederek bayi ve şube üzerinden alamayacağı avantajlı fiyatlarda olan ürünleri satın almıştır. Bu aşamaya kadar kullanıcılar bu internet sitesinin sahte olduğunu anlayabileceği herhangi bir şüphe uyandıracak eksiklik gözlemleyememiştir. Satın alma işlemi yapan kullanıcılar ürünlerinin kendilerine ulaşmadıklarını fark ettikleri zaman şirketin müşteri hizmetleri departmanına ulaşmıştır. Müşteri hizmetleri ile yapılmış olan görüşmelerde şirketin online satış yapmadığını ifade etmiştir. Müşteri hizmetleri kendilerine ulaşan bu şikayetleri baz alarak konuyu bilgi sistemleri direktörlüğü, iç denetim başkanlığı ve hukuk müşavirliğine aktarmıştır.

Bu çalışmada iç denetim başkanlığının iç kontrol sistemi kapsamında konuyu ele alış biçimi, riskleri değerlendirme yöntemleri ve şirket içi ne tür aksiyonlar alınması gerektiği konusunda nasıl bir yol izlediği anlatılmıştır.

3.1. İç Denetim Başkanlığı'nın İnceleme Çalışması

İç denetim ekibi; bir kıdemli denetçi ve iki denetçi tarafından yürütülmüştür. İnceleme öncesi müşteri hizmetleri departmanı, hukuk müşavirliği, bilgi sistemleri departmanı, internet sitesinin yazılım ve tasarımından sorumlu personelin katılımıyla beraber toplantı düzenlenmiştir. Yapılan toplantı neticesinde; ilgili departmanlardan inceleme kapsamında bilgi ve belgeler talep edilmiştir.

Müşteri hizmetleri departmanından,

- Kendilerine ulaşan şikayet sahiplerinin şirket müşteri veri tabanında yer alan müşterilerden olup olmadığının incelenebilmesi için şirket müşteri listesi ve şikayette bulunan kişilerin bilgileri,
- Şikayet sahiplerine ulaşan e-posta örneği,
- Müşteri veri tabanında yer alan müşterilere reklam amaçlı e-posta gönderimi yapılıyor mu? Yapılıyor ise şirketin göndermiş olduğu e-posta örneği,
- Daha önce kendilerine benzer ulaşan bir şikayetin olup olmadığı bilgileri talep edilmiştir.

Bilgi sistemleri departmanından,

- İnternet sitesinin güvenlik ve gizlilik sertifikaları,
- İnternet sitesinde yer alan kullanıcı giriş arayüzünde sanal klavye, kullanıcı kimlik doğrulama gibi önlemlerin neler olduğu?
- İnternet sitesinin tasarımında kullanılan içeriğe personel tarafından erişiminin nasıl sağlandığı, bu dosyaların güvenliği konusunda herhangi bir şifreleme işleminin uygulanıp uygulanmadığı?
- Şirketin sunucusundaki internet sitesi dosyalarına erişim yetkilerinin kimlerde olduğu ve şirket dışında erişim sağlanıp sağlanmadığı?
- Olayın gerçekleştiği tarihten itibaren sunucudan dosyaların kimler tarafından indirildiği, kopyalandığı ve/veya yükleme yapıldığı?

- Şirketin internet sitesinin tasarım ve içeriği üzerinde çalışan personelin dışında herhangi bir danışman firmadan hizmet alınıp alınmadığı, alınıyor ise bu kişilerin kullanıcı yetkilerinin ne durumda olduğu ve bu firmalar ile yapılan sözleşme örnekleri talep edilmiştir.
- Ayrıca müşteri e-posta adreslerine nasıl ulaşıldığı konusunda teknik bir araştırma yapılarak sebeplerinin bildirilmesi talep edilmiştir.

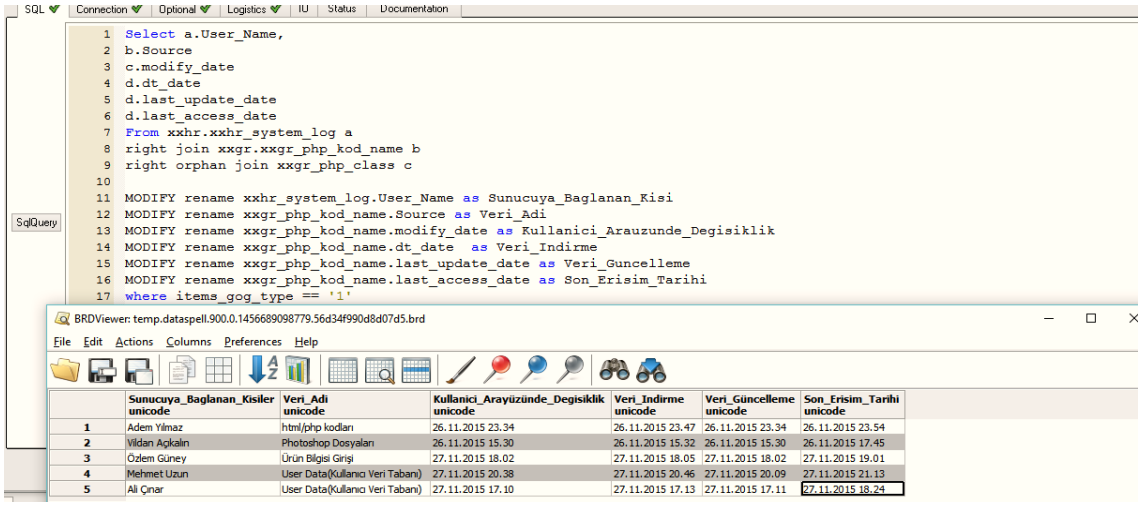
Öncelikli olarak müşteri hizmetleri departmanı tarafında kontroller sağlanmıştır. Şikayette bulunan kişilerin şirket müşteri veri tabanında yer alan müşteriler olduğu görülmüştür. Şirketin müşterilere sadece ürün tanıtımı amacıyla e-posta gönderimi yaptığı tespit edilmiştir. Gönderilen e-posta ve sahte internet sitesi üzerinden gelen e-posta içerikleri karşılaştırıldığında satış linkinin eklenmesi dışında birebir aynı tasarıma sahip olduğu görülmüştür. Geriye dönük bir yıllık şikayet analizi incelendiğinde benzer bir şikayete rastlanmadığı gözlemlenmiştir.

Bilgi sistemleri departmanından internet sitesinin güvenlik ve gizlilik sertifikası anlamında mevcutta herhangi bir sertifikasının bulunmadığı öğrenilmiştir. Şirketin ileri bir tarihte online satışa geçmek üzere uluslararası geçerliliği bulunan bir güvenlik protokolü olan SSL sertifikası, güvenli bilgi aktarımını sağlayan SET sertifikaların alım süreçlerinin devam ettiği bilgisine ulaşılmıştır.

Şirket sunucundaki dosyaların ve internet sitesinin tasarımında kullanılan içeriklerin yazılım ve tasarım ekibi tarafından ortak bir hesap üzerinden erişim sağladığı tespit edilmiştir. Sunucudaki dosyalara tek hesap üzerinden erişim sağlandığı için hangi zaman aralığında kimin giriş yaptığının ancak IP adres üzerinden kontrol yapılabildiği bununda operasyonel bir zaman kaybına neden olduğu için bugüne kadar hiç denetlenmediği bilgisi alınmıştır. Ayrıca tüm yazılım ve içerik geliştirme ekibin sunucuya erişim, dosya kopyalama ve indirme yetkisinin olduğu ve bu işlemi şirket dışında da gerçekleştirebildiği tespit edilmiştir.

Sahte internet sitesi linkinin bulunduğu eşzamanlı e-posta gönderimin 27.11.2015 tarihinde saat 22.17'de yapıldığı bilgisine ulaşılmıştır. Bu tarih ve saat baz alınarak bilgi sistemleri direktörlüğü ile beraber IP adresleri üzerinden geriye dönük bir haftalık ve sonraki bir haftalık süre göz önünde bulundurularak internet sitesi sunucundan dosyaların kimler tarafından indirildiği, kopyalandığı ve yükleme yapıldığı incelenmiştir. Belirtilen tarih aralığında beş personelin sıklıkla sunucuya bağlandığı

görülmüştür. Olay tarihine yakın sunucuya erişim sağlamış olan beş personelin görev tanımları incelenmiş ve sunucudaki tüm dosyalara erişim sağlayabilme yetkilerinin olduğu ve her türlü değişiklik yapabildikleri tespit edilmiştir. Ancak bu personelden Özlem Güney ve Mehmet Uzun'un sisteme sadece yeni ürün bilgi girişi yapmakla sorumlu olduğu yöneticilerinden öğrenilmiştir.




```
Select a.User_Name,
b.Source
c.modify_date
d.dt_date
d.last_update_date
d.last_access_date
From xxhr.xxhr_system_log a
right join xxgr.xxgr_php_kod_name b
right orphan join xxgr_php_class c

MODIFY rename xxhr_system_log.User_Name as Sunucuya_Baglanan_Kisi
MODIFY rename xxgr_php_kod_name.Source as Veri_Adi
MODIFY rename xxgr_php_kod_name.modify_date as Kullanici_Arauzunde_Degisiklik
MODIFY rename xxgr_php_kod_name.dt_date  as Veri_Indirme
MODIFY rename xxgr_php_kod_name.last_update_date as Veri_Guncelleme
MODIFY rename xxgr_php_kod_name.last_access_date as Son_Erisim_Tarihi
where items_gog_type == '1'
```

	Sunucuya_Baglanan_Kisiler unicode	Veri_Adi unicode	Kullanici_Arayüzünde_Degisiklik unicode	Veri_Indirme unicode	Veri_Güncelleme unicode	Son_Erisim_Tarihi unicode
1	Adem Yılmaz	html/php kodları	26.11.2015 23.34	26.11.2015 23.47	26.11.2015 23.34	26.11.2015 23.54
2	Vildan Açıkalın	Photoshop Dosyaları	26.11.2015 15.30	26.11.2015 15.32	26.11.2015 15.30	26.11.2015 17.45
3	Özlem Güney	Ürün Bilgisi Girişi	27.11.2015 18.02	27.11.2015 18.05	27.11.2015 18.02	27.11.2015 19.01
4	Mehmet Uzun	User Data(Kullanıcı Veri Tabanı)	27.11.2015 20.38	27.11.2015 20.46	27.11.2015 20.09	27.11.2015 21.13
5	Ali Çınar	User Data(Kullanıcı Veri Tabanı)	27.11.2015 17.10	27.11.2015 17.13	27.11.2015 17.11	27.11.2015 18.24

Şekil 1.İnternet Sitesi Sunucusuna Erişim İle İlgili Sorgu

Bu beş personel ile birebir görüşme sağlanmış olup dosyalarda yapmış oldukları değişiklerin görevi gereği yapıldığı anlaşılmıştır. Sadece Mehmet Uzun 27.11.2015 tarihinde User Data dosyasında yapmış olduğu değişikliğin Ali Çınar'ın yapması gerekirken kendisinden rica etmesi üzerine yapmış olduğunu beyan etmiştir.

Bilgi sistemleri direktörlüğü, yazılım ve içerik personeli tarafından sahte site linkinin gönderildiği müşteri bilgilerine nasıl erişildiği konusunda detaylı bir araştırma yapılmıştır. İşletim yazılımını yazan kişilerin gerektiğinde ileride oluşabilecek sorunlara müdahale edebilmek adına yazılımı ve dolayısıyla sistemi korumak amacıyla bıraktıkları açık gizli kapıların port tarama yöntemiyle bulunarak sistem güvenliğinin kırılması sonucu müşteri verilerine erişim sağlandığı bilgisi edilmiştir.

3.2. İç Denetim Başkanlığı Tarafından Yapılan İncelemenin Sonucu

Sahte internet sitesi oluşturulduğuna dair zaman kaybetmeden hukuk müşavirliği tarafından edinilen deliller doğrultusunda suç duyurusunda bulunulması gerektiği bilgisi paylaşılmıştır. Ayrıca bilgi sistemleri direktörlüğü tarafından tespit edilmiş olan port tarama yaparak sistem güvenliğini kırıp sisteme erişim sağlayan yabancı IP adres

bilgilerinin hukuk müşavirliği ile paylaşılarak gerekli yasal işlemlerin başlatılması gerektiği bilgisi verilmiştir.

İnternet sitesinde online satış yapılmadığı için herhangi bir güvenlik önleminin alınmamış olmasının bu olaya sebebiyet veren en büyük etken olduğu, bu nedenle öncelikli olarak veri bütünlüğünün sağlanarak, güvenilirlik ve gizlilik sertifikalarının alınma sürecinin hızlandırılması gerektiği tavsiye edilmiştir. Ayrıca online satış yapmaya başlandığında ödeme aşamasında sanal pos üzerinden yapılan ödemelerin güvenli hale gelebilmesi için Sanal Klavye, 3D Secure gibi güvenlik hizmetinin bulunması gerektiği bilgisi verilmiştir.

Şirket sunucusundaki tüm dosyalara; ilgili departmanlardaki kişilerin ortak bir hesap üzerinden erişim sağlamak yerine kimin ne sıklıkla ne işlem için sunucuya erişim sağladığının izlenebilirliğini kolay hale getirebilmek adına kişisel şifreleme/kimlik sınaması yöntemi ile erişimin sağlanması gerektiği iletilmiştir.

Ayrıca bilgi sistemleri direktörlüğü, yazılım ve içerik personelinin görev tanımlarının yeniden gözden geçirilmesi ve yapılacak işlerin net olarak yazılı hale getirilmesi gerektiği iletilmiştir. İlgili personelin yaptığı iş ile bağlantılı olarak sunucuda ihtiyacı olan gerekli dosyalara erişim hakkının verilmesi ve kalan dosyalara erişim kısıtlamasının getirilmesi gerektiğine raporda yer verilmiştir.

Sistem güvenliğinin kırılarak sisteme erişim sağlanması neticesinde yaşanacak olan benzer tehditlere karşı olası senaryolar geliştirilerek, bilgi güvenliğine etki eden faktörlerin bir bütün olarak bilişim korsanı gözüyle değerlendirilmesi ve sistemde mevcut olan gizli açık kapıların kapatılması, gerekli görülenlerin ise sürekli kontrol altında tutulacak şekilde yapılandırılmasının daha doğru olacağı kanaatine varılmıştır.

Bu olay sonucunda tespit edilen kendi görevi olmadığı halde sistem üzerinden farklı personelin yapması gereken bir işlemi kendisi yaptığı için Mehmet Uzun'a, kendi yapması gereken işlemi görev sorumluluğunda olmayan başka bir arkadaşına yaptırdığı için Ali Çınar'a yazılı uyarı verilerek gözlem altında tutulması gerektiği tavsiye edilmiştir.

Yaşanan bu olumsuz olay neticesinde öncelikli olarak müşterilere ve kamuoyuna bilgilendirme ve özür yazısının ulaştırılması marka imajının güvenilirliği açısından faydalı olacağı konusunda mutabakata varılmıştır.

Sonuç

Hızla artan siber suçlar neticesinde şirketlerin de ciddi oranda para ve itibar kaybına uğradıkları görülmektedir. Birçok şirket güvenlik politikalarının içerisinde önemli bir başlık olarak siber suçlara yer vermeye başlamıştır. Bu şirketlerden bazıları sanal dünya ile beraber büyümesi sebebiyle, siber suçlar alanına büyük yatarım yaparak bu alanda çalışacak kişiler istihdam etmektedir. Nitekim yaşanan kayıpların büyüklüğü Türk ceza yargısında da "Bilişim Suçu" kavramının ön plana çıkmasına sebep olmuştur.

Çalışmaya konu olan şirket ise sanal dünyayı sadece reklam amaçlı kullandığı ve online hizmet vermediği için internet sitesi üzerinden önlem almayı ihmal etmiş ve bu sebeple yaşanan siber suç sonucunda şirketin marka imajı ve itibarı zedelenmiştir.

Günümüzde bilginin saklanması, paylaşılması açısından büyük kolaylıklar sağlayan bilişim teknolojileri, şirketler için önemli maddi ve itibar kaybına neden olabilecek bazı güvenlik tehditlerini de beraberinde getirmektedir. Şirketler maliyetlerine bakmaksızın en üst düzey güvenlik teknolojilerinden faydalanarak sistemler geliştirse de bu tür teknik güvenlik önlemleri yeterli olmamaktadır. Çünkü güvenlik teknolojilerinin geliştirilmesi saldırganları teknik açıdan zorlaşan yapıdaki insan faktörünün zayıflıklarından yararlanmaya yöneltmiştir. Bu durum ise insan faktörünü güvenlik anlamında en zayıf halka haline getirmektedir. Şirket içerisinde insan faktörüne bağlı oluşabilecek bilgi güvenliği riskleri tamamen ortadan kaldırılamasa da en aza indirilebilmesi için gerekli farkındalık faaliyetlerine önem verilmesi gerekmektedir. Ayrıca sadece dışarıdan gelebilecek saldırılara odaklanmayarak şirket içerisinde gerçekleşebilecek saldırıları da düşünerek insan ilişkilerine de önem verilmesi gerekmektedir.

Çalışmaya konu olan şirkette iç denetim başkanlığı tarafından yapılan inceleme neticesinde insan kaynaklı bir güvenlik zafiyetinin yaşanıp yaşanmadığı konusunda net bir bilgiye rastlanamamıştır. Ancak insan faktörünün güvenlik konusunda büyük öneme sahip olduğu görülmüştür. Bu aşamada şirketin prosedürleri, görev tanımları, güvenlik önlemleri ve şirket çalışanı kaynaklı oluşabilecek güvenlik ve gizlilik zafiyeti riskinin iyi değerlendirilmesi ve en aza düşürebilecek önlemlerin kapsamlı olarak alınması gerekmektedir. Şirket personeline mutlaka bilgi güvenliği konusunda farkındalıklarını arttırmak adına genel, özellikle sistem üzerinde işlem yapan personele ise siber suçlar

kapsamında detaylı bir eğitim verilmesi ihmal sonucu ortaya çıkacak bir suistimal riskini en aza indirecektir.

Şirketin sistemine ve kullanılan programlara olan erişimlere kimler tarafından niçin ulaşması gerektiğinin yazılı olarak duyurulması, görev tanımındaki işe hizmet etmeyen farklı bir kişinin sorumluluğunda olan ekranlara ve dosyalara erişimlerin kısıtlanması gerekmektedir. Mutlaka kişisel şifreleme/kimlik doğrulama sistemine geçilerek kimlerin hangi dosyalar üzerinde çalıştığı bilgisinin izlenebilirliğinin hayata geçiriliyor olması insan kaynaklı güvenlik zafiyetine rastlanma olasılığını azaltacaktır.

Online satış hizmeti veren şirketlerin güvenlik sertifikalarının olmasının yanı sıra siber suçlara karşı korunması için olası senaryolar hazırlayarak bu alanda sürekli kontrol mekanizması geliştirmesi gerekmektedir. Bu sebeple özellikle bu alanda çalışacak olan bir ekip oluşturması faydalı olmaktadır.

Kaynakça

Akarslan, H. (2011). Bilişim Suçları, Bilişim Yoluyla İşlenen Suçlar ve Adli Bilişim Ayrımı. Yayınlanmamış Yüksek Lisans Tezi. Polis Akademisi Güvenlik Bilimleri Enstitüsü.

Barışık, S. ve Temel, H. (2007). İnternet Bankacılığı Kullanımında Güvenlik Unsurlarının Bilinilirliği (Anket Uygulamasına Dayalı SPSS Çözümlemesi). Karamanoğlu Mehmetbey Üniversitesi Sosyal ve Ekonomik Araştırma Dergisi, (2), 119-135.

Büyükyıldırım, Ü. (2014). Yeni Başlayanlar İçin E-ticaret. Şubat 5, 2016 tarihinde http://www.umityildirim.com/dosyalar/Yeni-Baslayanlar-Icin-E-Ticaret.pdf adresinden alındı

Diker, A. ve Varol, A. (2013). E-Ticaret ve Güvenlik. 1st International Symposium on Digital Forensics and Security-Proceding Book, 29-33.

Dondurmacı, G. A. ve Çınar, A. (2014). Yönetim Bilişim Sistemleri. Papatya Yayıncılık.

İçli, G. E. ve Aslan, B. (2008). İnternette Ödeme ve Güvenlik. Kırklareli Üniversitesi Lüleburgaz Meslek Yüksekokulu.

Kul, H. (2009). İşletmeciler İçin Bilişim Sistemleri Temelleri ve Uygulamaları İstanbul: Papatya Yayıncılık.

Soysal, E. (2015). Bilişim Teknolojilerinin Eğitimde Ölçme Aracı Olarak Kullanılması ve Örnek Uygulama Olarak "Moodle" Kullanımı.Yayınlanmamış Yüksek Lisans Tezi. Zirve Üniversitesi Sosyal Bilimler Enstitüsü.

Tekerek, M. (2008). Bilgi Güvenliği Yönetimi. Kahramanmaraş Sütçü İmam Üniversitesi Fen ve Mühendislik Dergisi, 11 (1), 132-137.

Tıngöy, Ö. (2009). Bilişim Çağında Etik. İstanbul: Avcıol Basım Yayım.

Torlak, M. (2013). E-Ticaret El Kitabı. Şubat 5, 2016 tarihinde http://melihtorlak.com/wp-content/uploads/2010/09/E-T%C4%B0CARET-EL-K%C4%B0TABI-28.11.2013.pdf adresinden alındı

Yıldız, M. (2014). Siber Suçlar ve Kurum Güvenliği. Yayınlanmamış Uzmanlık Tezi. Ulaştırma Denizcilik ve Haberleşme Bakanlığı.