Muhasebe Bilgi Sistemlerinde Bilgi Güvenliği

Yrd. Doç. Dr. Berna DEMİR
Anadolu Üniversitesi, Bozüyük M.Y.O.

Özet

Küreselleşen dünyada yaşanan yoğun rekabet ortamı ve teknolojik gelişmeler muhasebe bilgi sistemlerinde bilgilerin bilgisayarlı ortamlarda üretilmesini ve sunulmasını gerekli kılmıştır. İşlemlerin bilgisayarlı ortamda yürütülmesi, sağladığı avantajlar yanında çeşitli güvenlik sorunlarını da beraberinde getirmiştir, İşletmelerin Internet'le dış dünyaya açılmaları, on-line olarak faaliyetlerini sürdürmeleri sadece işletme içinden değil işletme dışından da tehditlerin oluşmasına sebep olmaktadır. Bu nedenle işletmelerin muhasebe bilgi sistemlerini tehdit eden iç ve dış unsurlara karşı güvenlik önlemleri almaları gerekmektedir. Ayrıca bu konuda gerekli "bilgi güvenlik politikaları" oluşturulmasında büyük yarar bulunmaktadır.

Anahtar Sözcükler: Muhasebe bilgi sistemi, bilgi güvenliği.

Abstract: (Information Security in the Accounting Information Systems)

High competition and technological developments in today's world have caused accounting system use computer aided applications. Besides having many advantages, using computer aided applications have many security problems as well. In particular on-line processing and internet have many threats originating internal and external sources of the managements. Therefore managements must take safety precautions. Furthermore establishing ali necessary security policies would provide considerable benefits.

Key Words: Accounting information systems, information security.

1. Giriş

İşletmeler günümüzde küreselleşen bir dünyada ve yoğun rekabet ortamında yaşamlarını sürdürmek zorundadırlar. Bu zorunluluk işletmelerin daha hızlı, güvenilir ve doğru bilgiler temelinde kararlar almalarını gerekli kılmaktadır. Bu bağlamda işletmelerin muhasebe departmanlarına ve yönetime Önemli görevler ve sorumluluklar yüklenmektedir.

Muhasebe işletmenin dili olarak ifade edilmektedir. Dolayısıyla muhasebe bilgisi, etkin bir işletme yönetimi için temel bilgi niteliğini taşımaktadır. Bu bilginin olmaması, işletme faaliyetlerinin planlanmasını, yürütülmesini ve kontrol edilmesini olanaksız duruma getirmektedir[1].

Muhasebe, ilgili grupların bilgi gereksinimlerini karşılayabileceği ölçüde başarılı ve faydalı olabilecek bir sistemdir. Bu nedenle, muhasebe bir bilgi sistemi olarak düşünüldüğünde, bu sistemin temel amacı bilgi kullanıcılarının etkili karar almalarını sağlayacak verilerin toplanması, işlenmesi ve iletilmesinden oluşacaktır. Muhasebe bu kararlara esas oluşturacak biçimde işlet-

[1] Fevzi Sürmeli, Melih Erdoğan, Nurten Erdoğan, Kerim Banar ve Saime Önce, Muhasebe Bilgi Sistemi, Açık Öğretim Fakültesi Yayınları No: 532, Ünite 1-17, 1. Baskı, Kasım 1996, s.55.

menin mali nitelikteki bilgilerini toplamalı, bunları işleyerek elde ettiği bilgileri zamanında, yerinde, tam ve doğru olarak gereksinim duyanlara iletmelidir[2].

Muhasebe bilgi sistemlerinde daha önceleri elle (manuel) olarak üretilen muhasebe bilgileri çağın gelişimine paralel olarak bilgisayarlı ortamlarda üretilmeye ve raporlanmaya başlamıştır. Bilgisayarlı ortam muhasebe işlemlerini hızlandırma, kolaylaştırma ve güncelleme ile bilgi iletiminde kolaylık ve hız kazandırması yanında birçok güvenlik sorununu da beraberinde getirmiştir. İşletmenin bütün departmanlarındaki bilgisayarların iletişim ağlarıyla birbirlerine bağlanması ve Internet ile dış dünyaya açılması ile de güvenlik sorunu daha çok artmıştır. Bu nedenle işletmeler yaşamları için çok Önemli olan muhasebe bilgilerinin bilgisayarlı ortamdaki güvenliğini sağlamak için gerekli önlemleri almak zorunda kalmaktadırlar.

Muhasebe bilgi sistemlerinde güvenliği tehdit eden unsurlar bilgisayarlı ortamla sınırlı olmamakla beraber, bu çalışmada bilgisayarlı ortamdaki muhasebe bilgilerinin güvenliğinin sağlanması üzerinde durulacaktır.

2. Güvenlik ve Bilgi Güvenliği Kavramı

Güvenlik genel anlamda *"toplum yaşamında kanuni düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu*[3]*"* olarak tanımlanmaktadır. Güvenlik kavramının kapsamı çok geniş olup, bu kapsam içinde ulusların güvenliğinden en küçük birimlerin güvenliğine kadar geniş bir yelpaze söz konusudur. Güvenlik konusuna işletmeler açısından bakıldığında "veri/bilgi güvenliği" kavramı ön plana çıkmaktadır.

Bilgi güvenliği; bir değer yüklenen ve önemi bilinen, gizli tutulması gereken verinin kaynaklarına ulaşılma hakkının yetkisiz kişilerden uzak tutulması ve bu bilgilerin koruma altına alınması demektir. Bir zincire benzetebileceğimiz güvenliğin gücü en zayıf halkaya bağlıdır. Güvenliğin kendisi bir ürün değil bir süreçtir. Bu süreç yazılım ve donanım güvenlik çözümlerinin alınmasıyla başlamakta, kullanıcıların bu çözümler üzerinde oluşturulan güvenlik politikalarını uygulamasıyla devam etmektedir[4].

Bilgisayarların ve iletişim ağlarının işletmelerde yoğun bir şekilde kullanılması ile de günümüzde önemli bir olgu olarak "teknolojik güvenlik" ve "bilgisayarlı ortamdaki bilgilerin güvenliği" konuları önem kazanmıştır.

Bilişim teknolojisi hızla gelişmekte ve değişmektedir. İşletmeler, bu gelişmelere kayıtsız kalamamışlar ve sağladığı avantajlar sebebiyle bilgisayar teknolojisini, Intranet ve Internet'i yoğun olarak kullanmaya başlamışlardır. Bu teknolojilerin kullanımı işletmelerde etkinlik ve verimliliği önemli ölçüde arttırmıştır. Ancak sağladığı yararlar yanında pek çok güvenlik sorununu da beraberinde getirmiştir.

Internet'in yaygınlığının ve kulanımı-nın artması, gittikçe üzerinden daha fazla kritik veri dolaşması kurumların iş süreçlerini elektronik ortama taşıyarak Kurumsal Kaynak Planlaması-KKP (Enterprise Resource Planning-ERP) ile e-iş fonksiyonlarını birleştirme çabaları, bunun sonucunda daha fazla işlem yapmaları ve dolayısıyla ürün ve hizmetlerine rekabet üstü değerler kazandırmaları giderek tüm bu unsurlara temel teşkil eden güvenlik teknolojilerinin önemini arttırmaktadır[5].

3. Muhasebe Bilgi Sistemlerinde Bilgi Güvenliğini Tehdit Eden Unsurlar

İşletmelerde muhasebe bilgileri bilgisayarlı ortamlarda üretilmekte ve kulanıcılara bilgisayarlı ortamlarda sunulmaktadır. İşletme ölçeğine bağlı olarak muhasebe kayıtları tek bir bilgisayarda tutulabileceği gibi işletmeler kendi özel ağlarını kurmakta muhasebe bu ağda bir departman olarak yerini almaktadır.

Bilgi teknolojilerinin işletmenin çeşitli departmanlarında ve muhasebede kullanıl-

[2] Münevver Yılancı, "Muhasebe Bilgi Sistemi ve Kontrol", Kütahya İ.İ.B.F. Yıllığı, 1991, S.103. [3] Türkçe Sözlük, T.D.K. Basımevi, 1998, s.915.

[4] http://www.ssm.gov.tr/lihratT/doc5/tr/teskilat/ dosyalar/bim/kur_gu v_pol. pdf.

[5] Altay Onur, "Kurumsal Bilgi Güvenliğine Bakış", http ://www.bilgiyonetimi. org/cm/.

masıyla birlikte, birbiriyle bağlantısız geliştirilen yazılımlar bugünün bilgi ihtiyacını karşılamada yetersiz kalmış, bu nedenle işletmeler gelişen donanım ve iletişim teknolojilerinin desteği ile işletme genelinde tam entegrasyonu hedef almışlardır. Bu yaklaşım Kurumsal Kaynak Planlaması-KKP sistemlerinin geliştirilmesine yol açmıştır. KKP bir organizasyonun bilgi işleme sistemleri ve onunla ilgili bütün verilerin tamamının entegrasyonunu sağlamak için geliştirilmiştir. Muhasebede bu gelişmeden etkilenmiş, önceleri muhasebe yazılımları bağımsız iken, KKP sisteminde tümleşik yapı içinde bir modül haline gelmiştir. KKP sisteminde muhasebeden insan kaynaklarına kadar bütün işletme departmanları modüler sistemle tek bir veritabanında toplanmaktadır ve eş zamanlı olarak bilgi paylaşımını sağlamaktadır[6]. İşletmelerde KKP sisteminin kullanılması üretkenliği önemli ölçüde arttırmıştır. Ancak tüm bölümlerin Internet'e ve Intranet ile birbirlerine bağlanması ve verinin/bilginin tek bir yerde toplanması bilgisayarlı ortamdaki bilgilerin güvenlik riskini daha da arttırmıştır. Muhasebede iletişim ağlarının kullanılması ile sadece işletme içindeki yetkili kişiler değil işletme içindeki ve dışındaki yetkisiz kişilerde muhasebe bilgilerine ulaşabilmektedirler.

Teknolojik gelişmeler muhasebe bilgi sistemlerinde yeni güvenlik tehditleri yaratmıştır. Bunlar[7]:

- Bilgi gizliliğinin/mahremiyetinin kaybı,
- Bilginin çalınması,
- Onaylanmamış bilgi kullanımı,
- Bilginin ve bilgisayarların hileli kulanımı,
- Onaysız (kasti) değiştirme yada veri manipülasyonunun sonucu olarak bilgi bütünlüğünün kaybı,
- Onaylanmamış yada kasti, kötü niyetli hareketlere bağlı işlem hatası şeklinde sıralanabilir.

OECD Konseyi muhasebe bilgi sistemlerindeki güvenlik tehditlerinin kasıtlı yada kasıtsız hareketlerden kaynaklanabileceğini ve iç veya dış kaynaklardan gelebileceğini onaylamıştır[8]. Doğal felaketlerde muhasebe bilgi sistemi için güvenlik tehdidi oluşturmaktadır.

Kasıtlı veya kasıtsız tehditler işletme içindeki kişilerden (işletme personeli) veya işletme dışındaki kişilerden gelebilir. Bu kişiler;

- Donanım,
- Yazılım,
- Veri (girdi),
- Sistem,
- İletişim ağı
- Bilgi (çıktı)'ye zarar verebilirler.

İşletme içindeki veya dışındaki kişiler aşağıdaki yolları kullanarak kasıtlı veya kasıtsız olarak güvenliği tehdit edebilirler. Bunlar;

- Bilgisayar virüsleri
- Bilgi hackerları/Yetkisiz erişimler
- Hırsızlık
- Teknik problemler
- Yetkili erişimleri kasıtlı veya kasıtsız olarak kötüye kullanma
- Bilgisayar hileleri şeklinde sıralana bilir.

3.1. İşletme İçinden Gelen Tehditler

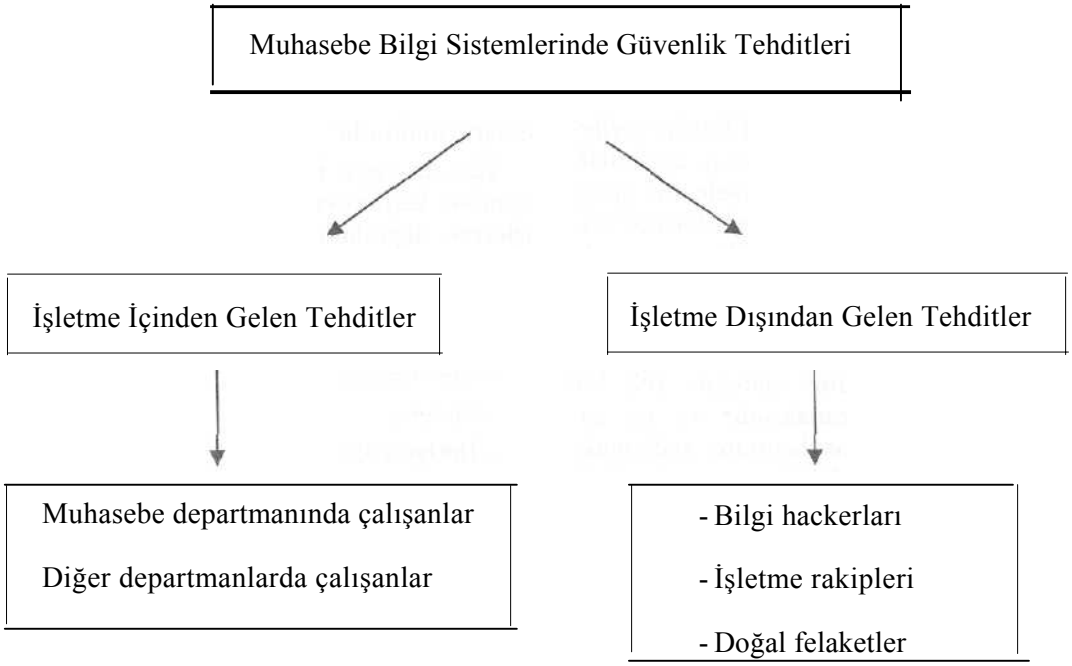
Genelde saldırıların işletme dışından olacağı düşünülür. Ancak işletmede çalışan personelde güvenliği tehdit eden önemli bir unsurdur. Bu kişiler kasıtlı veya kasıtsız olarak (hata ile) muhasebe bilgilerinin güvenliğini tehdit edebilirler. Bilgisayarları iletişim ağları ile birbirlerine bağlı olan işletmelerde sadece muhasebe personeli değil diğer departmanlarda çalışan personelde muhasebe bilgi sistemlerinde güvenlik tehdidi oluşturmaktadırlar.

Personelin kasıtsız olarak bilgi güvenliğini tehdit etmesinin ana sebepleri arasında yaptıkları iş ile ilgili yeterli eğitime

[6]Abdullah Tekin ve Raif Parlakkaya, "Tümleşik Bilgi Sistemleri ve Muhasebe Bilgi Sistemi", http: //www. bilgiyonetimi. org/cm/-[7] Ahmad A. Abu-Journal of American Academy of Business, Cambridge, Holywood, Sep. 2003, Vol.3, Iss. 1/2, s.9.

[8] Ahmad A. Abu-Musa, a.g.m., s.10.

sahip olmamaları, işletme içinde iç kontrolün olmaması veya yetersiz olması, yorgunluktan dolayı dikkatini tam toplayamaması gibi sebepler sayılabilir. Bu kişiler hata ile yanlış veri girebilir veya kaza ile bu verilere zarar verebilirler. Gereksiz yere ağı meşgul edebilirler. Fiziksel olarak donanıma zarar verebilirler (vandalizm) veya sistem ve uygulama yazılımlarını bozabilirler.



Şekil 1. Muhasebe Bilgi Sistemlerinde Güvenlik Tehditleri

İşletme personeli kasıtlı olarakta muhasebe bilgi sistemine zarar verebilir. Bu kişiler aldıkları ücretten memnun olma-

bilgilerine zarar verebilirler. Sadece yetkisiz (izinsiz) kişilerin güvenlik tehdidi oluşturduğu düşünülmemelidir. Yetkili (izinli) personelde tehdit oluşturabilir. İş-

bilgiyi çalabilirler.

Örneğin; bankalarda zimmetine para geçirme içerden bilgiye erişim yetkisine sahip olan personel tarafından yapılmaktadır. Bu kişiler kasıtlı olarak sadece veri/bilgiye değil, donanım ve yazılıma da zarar verebilirler.

Sisteme veya verilere maksimum zararı vermek için planlanacağından kasıtlı hareketler daha önemlidir. Örneğin; muhasebe verilerini yok eden bilgisayar operatörü, back-up (yedek) dosyalarını da yok edebilir.

3.2. İşletme Dışından Gelen Tehditler

İşletme dışından gelen tehditler kasıtlı olmaktadır. Bu kişiler bilinçli olarak muhasebe verilerine zarar vermek istemektedirler. Bu kişilere karşı önlem almak işletme içinde çalışan personele karşı önlem almaktan daha kolaydır. Çünkü potansiyel olarak bu tehditler tahmin edilebilir.

İşletmelerin iletişim ağları ile işletme dışına da açılması işletme dışından gelen tehditleri de arttırmıştır, İşletmenin rakipleri, bilgi hackerları gibi kişiler yetkisiz olarak işletmenin bilgisayarlarına girebilir ve muhasebe bilgilerine zarar verebilirler. Bu kişiler sisteme virüs bulaştırarak sistemi işlemez hale getirebilirler. Doğal afetlerde işletme dışından gelen tehditler arasında yer almaktadır.

4. Muhasebe Bilgi Sistemlerinde Bilgi Güvenliğinin Sağlanması

Günümüzde işletmelerin, globalleşen dünyada faaliyetlerini en iyi şekilde devam ettirebilmeleri, artan rekabet ortamında rekabet edebilmeleri ve kararlar alabilmeleri için özellikle muhasebede üretilen "bilgi" çok önemli hale gelmiştir. Bu nedenle işletmeler için çok önemli olan bu bilgilerin güvenliğini sağlamak için işletme içinde ve dışında oluşan tehditlere karşı gerekli güvenlik önlemlerini almak gerekmektedir.

Doğru, tam ve güvenilir muhasebe bilgileri elde edebilmek için sadece bilgi oluştuktan sonra değil, verinin bilgisayara girilmesi, işlenmesi ve bilgiye dönüşüm süreçlerinde de gerekli önlemler alınmalıdır. Bu nedenle bilgisayarlı ortamdaki muhasebe veri/bilgilerinin güvenliği için;

- Ağ güvenliği (Intranet ve Internet)
- Sistem güvenliği,
- Veri güvenliği sağlanmalıdır.

Bunlardan birisinde gerekli güvenlik önlemlerinin alınmamış olması, diğerlerini de etkilemektedir. İşletmelerde bilgisayarlar ağ yoluyla birbirlerine bağlı oldukları için bilgisayar sisteminin güvenliğini ve uygulama güvenliğini sağlamak, özellikle ağ güvenliğinin sağlanmasına bağlıdır.

Ağ güvenliğinin sağlanması için her şeyden önce kurumsal bir güvenlik politikasının oluşturulması gerekmektedir. Doğru, etkin ve dokümante edilmiş kurumsal bir güvenlik politikası oluşturulmadan güvenlik çalışmalarının başarıya ulaşması olanaksızdır[9]. Ağ yöneticileri veya birimleri, başkaları tarafından bu ağların zarar görmemesi için gerekli önlemleri almakla sorumludurlar.

4.1. İşletme İçinden Gelen Tehditlere Karşı Alınacak Güvenlik Önlemleri

İşletme dışındaki tehditler için ağ güvenliğinin sağlanması büyük ölçüde yeterli olmaktadır. Çünkü bu kişiler işletmenin donanımına, sistemine, yazılımına, veri ve bilgiye ağ yolu ile ulaşabilmektedirler. Verinin işlenerek bilgiye dönüşümünü sağlayan, sistemi, uygulama yazılımlarını, bilgisayar donanımlarını ve yerel alan ağını kullananlar işletme içindeki personel olduğu için bu kişilerin oluşturacakları tehditlere karşı daha geniş kapsamlı önlemler alınmalıdır.

Muhasebe verisinin işlenip bilgiye dönüşmesi aşamasında oluşacak olumsuzlukları (Şekil 2)[10] önlemek ve yerel ağ güvenliğini sağlamak işletme içinden gelen tehditlere karşı güvenliği büyük ölçüde sağlayacaktır.

Muhasebe bilgi sistemlerinde verinin doğru ve geçerli olarak yaratılması büyük önem taşımaktadır. Kasıtlı veya kasıtsız olarak geçersiz verinin yaratılması, değiştirilmesi, silinmesi ve kopyalanması sistemin Çıktısı olan bilgininde doğru ve güvenilir olmasını engelleyecektir. Örneğin, hayali fatura düzenlenmesi, irsaliyede müşteriye gönderilen mallarların adetinin kasıtlı olarak değiştirilmesi, müşterinin borç bilgilerinin hata ile silinmesi gibi durumlarda oluşturulan muhasebe kayıtları ve raporlar gerçek bilgileri vermeyecektir.

Muhasebe bilgi sistemlerinde bilgi işlem bölümü dışında çalışan personelin (muhasebe personeli veya diğer departmanlardaki personel) yapacakları hata ve hileler özellikle muhasebe verilerinin oluşturulması aşamasında olmaktadır.

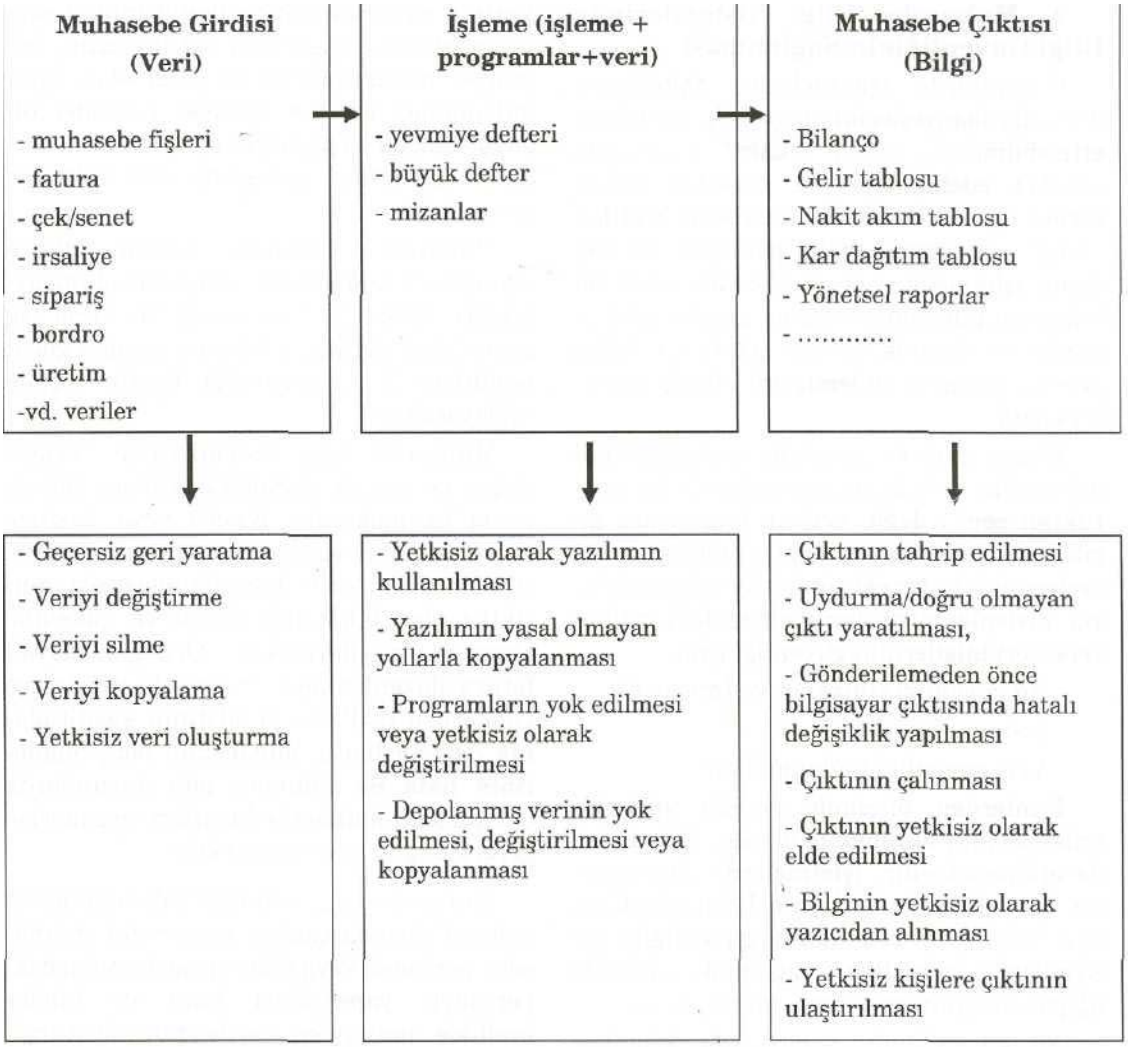
Bilgisayarlı ortamdaki muhasebe verilerinin girişine izin verilmiş kişiler dürüst ve iyi niyetli olabilirler. Fakat yorgunluğa, yetersiz eğitime ve ihmale bağlı olarak veriyi silen kasıtsız hareketlerde bulunabilirler[11]. İşletme içindeki yetkili (izinli) erişime sahip olan kişilerin muhasebe verilerine kazara verecekleri zararları önlemek için bu kişiler yaptıkları iş ve bilgi güvenliği konusunda eğitilmelidir. Ayrıca işletme içinde etkin bir iç kontrolün olması veri (girdi) üzerinde hem kasıtlı hem de kasıtsız olarak oluşan tehditleri önleyecektir.

---

[9] "Ağ Güvenliği", tr/agguvenligi. htm http://www.tepum.com.

[10] Ayrıntılı bilgi için bkz; Ahmad A. Abu-Musa, a.g.m., s.16.

[11] Ahmad A. Abu-Musa, a.g.m., s.14.



Şekil 2. **Muhasebe Bilgi Sistemlerinde Veri/Bilgi Akış Sürecinde Oluşan Güvenlik Tehditleri**

Ağa bağlı olmayan bilgisayarlarda yetkisiz erişim olmayacağı için güvenlik sorunu da daha az olacaktır. Çünkü veri girişini yapan, yazılımı ve donanımı kullanan kişiler bellidir. Yetkisiz erişim ağa bağlı bilgisayarlarda önemli bir sorundur. Ağa bağlı bilgisayarlarda tüm departmanlar ortak veritabanını kullandıkları için veriler ortak havuzda toplanmakta ve ilgili kişiler tarafından gerekli veriler kullanılmaktadır. Bu sistemlerde muhasebe verilerine erişenler ve muhasebe verilerini girenler sadece muhasebe personeli olmadığı için güvenlik sorunu daha da artmaktadır. Bu nedenle işletme içindeki yetkisiz kişilerin muhasebe verilerine ulaşmalarını ve sisteme zarar vermelerini önlemek gerekmektedir. Örneğin, Muhasebe bilgi sistemi içinde finansal muhasebe ve maliyet muhasebesi servisinde çalışanların birbirlerinin bilgisine ulaşımını engelleyecek kullanıcı kodu ve şifre girme yöntemiyle izinsiz erişimler engellenebilir. Ayrıca, geliştirilecek bir uygulamayla, bilgilere kimin ve hangi bilgisayar aracılığıyla ulaştığı ağ üzerinden izlenebilir. Böyle bir kontrol mekanizması muhasebe bilgilerinin güvenliğini sağlama açısından caydırıcı bir etki yapabilir. Diğer yandan muhasebe bilgi sistemi dışındaki bilgi sistemlerindeki kişilerin gereksinim duydukları bilgiler sadece onların erişimine izin verecek şekilde

kullanıma açık tutularak yetkisiz erişimler engellenebilir. Böylece bu kişiler yetkili olmadıkları için sadece veriye erişebilecekler, veri girişi, değiştirme ve silme işlemlerini yapamayacaklardır.

Geleneksel olarak güvenlik duvarları kurum ile dış dünya arasına yerleştirilir. Ancak büyük bir organizasyon, iç (internal) ateş duvarlarına da ihtiyaç duyabilir. İç ateş duvarları kurmak için pek çok neden vardır. Bunlardan en Önemlisi, bir işletmede çalışanların tamamının, şirket içindeki tüm bilgilere erişiminin istenmemesidir. Bu gibi durumlarda iç ateş duvarları, farklı yetkilerdeki kişilerin, erişmesi gereken verilerinde farklı olacağı düşüncesinden hareketle kullanılmaktadır[12].

Verinin doğru olarak yaratılması üretilecek bilginin doğru olacağı anlamına gelmemelidir. Örneğin; muhasebe fişleri doğru olarak girilse de programın hileli olarak yanlış işlem yapması sonucu oluşturulan yevmiye kaydı da hatalı olacaktır. Bu nedenle veri/bilgi işleme sürecinde de gerekli önlemler alınmalıdır. Programların yetkisiz olarak değiştirilmesi, depolanmış verinin yok edilmesi, değiştirilmesi ve kopyalanması engellenmelidir. Fiziksel olarak donanımın korunması da önem taşımaktadır. Ayrıca bu veriler yangın, hırsızlık, çalınma gibi tehlikelerden de korunmalıdır. Sistem içinde etkin bir kontrol mekanizmasının oluşturulması bilgi işleme sürecinin de güvenilir bilgiler üretmesine katkıda bulunacaktır.

Bilgisayarlı ortamdaki muhasebe verilerinin güvenliğini sağlamak için kaydedilen verilerin düzenli olarak yedeklenmesi (back-up) gerekmektedir. Yedekleme yapılan diskler çok sıcak ve elektriğin fazla yüklü olduğu ortamlarda bulundurulmamalıdır. Yetkisiz erişimlerin önlenmesi verinin yetkisiz olarak değiştirilmesini ve kopyalanmasını önleyecektir. Ayrıca sistemin zarar görmesini önlemek için donanım fiziksel olarak korunmalıdır.

Sistem doğru çıktılar üretebilir. Ancak çıktı üretildikten sonra da çıktıların yetkisiz olarak elde edilmesi, kopyalanması, çıktı üzerinde değişiklik yapılması ve tahrip edilmesi önlenmelidir. Örneğin; Bilanço rakamlarında değişiklik yapılarak işletmenin mali durumu farklı gösterilebilir, gelir tablosu ilgili olmayan kişilere ulaştırılabilir. Bunları önlemek içinde etkin bir kontrol oluşturulmalıdır.

Özetle işletme yönetimi tarafından işletme içinde iyi bir iç kontrol sistemi kurularak, bilgi güvenlik politikası oluşturularak, erişim kontrolleri sağlanarak, donanım fiziksel olarak korunarak ve personel eğitilerek işletme içinden gelen kasıtlı veya kasıtsız tehditlere karşı önlemler alınabilir. Güvenilir bir muhasebe bilgi sistemi için eğitimli ve güvenilir muhasebe personeli istihdam edilmelidir.

4.2. İşletme Dışından Gelen Tehditlere Karşı Alınacak Güvenlik Önlemleri

Muhasebe bilgilerinin güvenliğini tehdit edici önemli bir unsur da dışarıdan gelen tehditlerdir. İşletmeye zarar vermek isteyen kişiler ve/veya kurumlar artık günümüzde bilgisayar sistemlerine Internet yoluyla yetkisiz olarak çok rahat girebilmektedirler. Muhasebe bilgilerine yetkisiz erişilmesi işletmeleri güç durumlara sokmaktadır. Kasıtlı olarak muhasebe bilgilerine zarar vermek isteyen bu kişiler Internet'i saldırı yolu olarak kullanmaktadırlar. Bu nedenle dış tehditlere karşı Internet güvenliğini sağlamak gerekmektedir.

Dış tehditlere karşı Internet güvenliğini sağlamak için şunlar yapılabilir[13];

- Güvenlik duvarı (firewall) kurularak internet ile işletmenin özel ağı arasında bağlantı kurulur.
- Internet ortamında e-posta ve elek tronik dosyalar aracılığıyla bulaşabilecek virüsler ciddi bir tehlike oluşturmaktadır. Virüslere karşı koruyucu yazılımlar (antivirüs yazılımları) yüklenmelidir.

[12] Umut AL, "Internet'te Veri Güvenliği", Oluşum/38, http://yunus.hacettepe.edu.tr/~umutal/publications/datasecurity.pdf, s.47.

[13] "İnternet Güvenliği", http://www.tepum.com.tr/internetguvenlik.htm

Şekil 3. Güvenlik Duvarı (Firewall)

Internet üzerinden iletilen bilgiler üçüncü kişiler tarafından ulaşılma riski taşımaktadırlar. Internet üzerinden güvenli özel bilgi alışverişi için dijital şifreleme (encryption) ve kimlik kontrol (authentication) çözümleri sağlanmalıdır. Internet bağlantısının çalışanlar tarafından doğru kullanımı çok önemlidir.

Erişim kontrolü (authorization) sağlanarak Web erişimi ve mail içeriklerini kontrol eden çözümler geliştirilmelidir.

Dış tehditlere karşı, güvenlik duvarı, muhasebe verilerinin güvenliği açısından işletmelerin alacakları önemli önlemlerden birisidir.Bunlar ağın Internet'e çıkışının sağlandığı noktada kurulmakta ve bir güvenlik duvarı oluşturmaktadır. Ve ağa yapılacak saldırılar burada engellenmektedir. Güvenlik duvarı, Intranet'i dış ağdan (internetten) ayıran bir duvar olarak düşünülebilir (Şekil 3). Temel işlevi güvenlik gediği olan uygulamalara ait veri paketlerinin iç ağa ulaşmasını engellemektir. Böylelikle, iyi veya kötü niyetli olduğuna bakılmaksızın hiç kimse ağ dışından ağ içine izin verilen uygulamalar dışındaki uygulamalara ulaşamayacaktır[14].

Dışarıdan gelip muhasebe bilgilerini elde etmek isteyen kişiler ilk önce güvenlik duvarını aşmak zorundadırlar. Bu nokta bilgilerin güvenliği açısından ilk aşamadır. Ancak bu kişiler güvenlik duvarını açıp işlemenin yerel ağına girebilirler. Bu durumda işletme içinden gelen tehditlere karşı alman önlemler bu kişiler içinde alınmalıdır.

Genel olarak ağ güvenliğinden bahsedildiğinde akla gelen diğer bir sorun da açık kanallarda dolaşan bilginin gizliliği ve bütünlüğüdür. Bilgi gizliliği, verinin alıcısı dışında hiç kimse tarafından okunamaması, bilgi bütünlüğü ise, verinin değişmeden alıcısına ulaşması anlamına gelmektedir. Kimlik kanıtlama sistemleri oluşturdukları oturum anahtarları ile bu sorunları Çözebilmektedirler[15].

Bilgisayar çağının gereği olarak ticaret hayatının da elektronik ortama taşınması ile birlikte bir çok ülkenin mevzuatında, e-ticaretin benimsenebilmesi için açık ağ sistemine kullanıcıların güven duymasını sağlamak amacı ile hukuki düzenlemelerin yapılması gereği doğmuştur. Bu nedenle taraflar arasında iletilen bilginin gizliliği, bütünlüğü ve tarafların kimliklerinin doğruluğun, kurulacak olan teknik ve yasal alt yapı ile garanti edebilmek amacı ile elektronik imza (e-imza) kullanımı başlamıştır[16].

Elektronik imza (e-imza), kimliği ve mesaj içeriğine onay verildiğini göstermek amacıyla bir kimse tarafından (veya onun namına) mesaja eklenen veya mantıksal olarak mesaja bağlı olan elektronik bilgidir. Başka bir tanımla e-imza olaya taraf olmayan üçüncü kişilerin erişimine olanak vermeyen bir ortamda bilginin orijinal biçimiyle ve tarafların yasal kimliklerinin doğrulanarak saklandığının elektronik

[14] Albert LEVI ve M. Ufuk ÇAĞLAYAN, "Elektronik Posta Güvenliği için PGP Kullanımı", http://mercan.cmpe.boun.edu.tr/~-levi/AS97.HTM, s.2.

[15] Albert LEVI ve M. Ufuk ÇAĞLAYAN, a.g.m., s.2.

[16] Melih ERDOĞAN, Arman Aziz KARAGÜL ve Cemal ELİTAŞ, "Elektronik Veri Değişimi Güvenliği ve Elektronik İmza", Prof.Dr. Yüksel Koç Yalkın'a Armağan, SBF Yayın No: 590, TÜRMOB Yayın No: 221, Ankara 2003, s.186.

araçlarla garanti edildiği simgelerden oluşan bir kümedir[17].

Teknolojik gelişmeye paralel olarak işletmeler muhasebede ürettikleri mali raporları ilgili kesimlere gazete ve benzeri iletişim araçları yanında Internet ortamında da sunmaya başlamışlardır. Ancak Internet ortamında sunulan bilgilerin güvenli bir şekilde ilgililere ulaşması gerekmektedir. Hacker'ların Internet ortamında kamuoyuna sunulan mali raporları değiştirerek, kamuoyunu yanlış bilgilendirmeleri dolayısıyla işletmeyi zor durumlarda bırakabileceği düşünüldüğünde, Internet ortamındaki bilgilerin güvenliği özel bir önem taşımaktadır.

Bu öneme istinaden Sermaye Piyasası Kurulu (SPK), bildirimlerin kağıt ortamında gönderilmesine devam edilmesi suretiyle, elektronik imza ile de Kurul'a iletilmesini sağlamak üzere "Elektronik İmzalı Bildirim" esaslarını belirlemiş ve Internet sitesinde yayınlamıştır. IMKB'de işlem gören anonim ortaklıklar ve aracı kurumlar mali tablo ve özel bildirimlerini kağıt ortamında ve elektronik imza yoluyla imzalayarak bu esaslara uygun olarak elektronik ortamda gerçekleştireceklerdir[18].

Güvenliği sağlamak için alınan bu önlemler güvenliği sağlamanın bir süreç olduğu düşünülerek sürekli izlenmeli ve önlemler gelişmelere bağlı olarak güncellenmelidir. Örneğin; virüs, risklerin içinde gerçekleşme olasılığı en yüksek olanıdır. Dünya üzerinde 50.000'in üzerinde virüs olduğu ve her ay 100 civarında yeni virüsün çıktığı düşünülürse virüs programlarının güncelleştirilmesinin ne kadar önemli ve gerekli olduğu anlaşılır[19].

Güvenlik sisteminin sürekli yenilenmesi ve güvenliğin bir ürün değil bir süreç olduğu unutulmamalıdır. Internet üzerinden dünyanın dört bir tarafından erişilebilir hale gelmiş işletmeler için tehlikeler söz konusu iken bazı işletmeler bu tehlikelerden habersizdirler. Güvenliği sağlamanın bir maliyeti vardır ancak dışarıdan gelecek bir saldırının meydana getirdiği zarar güvenliği sağlamanın maliyetinden Çok fazla olabilir.

Muhasebe bilgi güvenliğini sağlamak için güvenlik hizmetleri sunan şirketler ile de çalışılabilir. İşletmenin güvenlik işini kendisinin yapmasının maliyeti yüksek ise güvenlik işini bu şirketlere devretmesinde yarar olacaktır.

Yalnız teknolojik önlemlerle (anti-virüs, güvenlik duvarı sistemleri, kripto vb.) iş süreçlerinde bilgi güvenliğini sağlama olanağı yoktur. Bilgi güvenliği, süreçlerin bir parçası olmalı ve bu bakımdan bir iş anlayışı, yönetim ve kültür sorunu olarak ele alınmalıdır. Her kurum mutlaka bireysel olarak ve kurum bazında bir güvenlik politikası oluşturmak, bunu yazılı olarak dökümante etmek ve çalışanlarına, iş ortaklarına, paydaşlarına aktarmak zorundadır. Tüm çalışanlar bilgi güvenliği konusunda bilinçli olmalı, erişebildikleri bilgiye sahip çıkmalı, özenli davranmalı, üst yönetim tarafından yayınlanan "Bilgi Güvenliği politikası" şirket açısından bilgi güvenliğinin önemini ortaya koymalı, sorumlulukları belirlemeli, çalışanları bilgilendirmeli ve BG sistemi, iş ortaklarını (müşteri, tedarikçi, taşeron, ortak şirket vb.) da kapsamalıdır[20].

5. Sonuç

Muhasebe bilgi sistemlerinde bilgilerin bilgisayarlı ortamda üretilmesi, raporlanması ve ilgili kişilere sunulması sağladığı avantajlar yanında çeşitli güvenlik sorunlarını da beraberinde getirmiştir. Muhasebe bilgi sistemlerine güvenlik tehdidi, işletme içinden olabileceği gibi, faaliyetlerinde Internet'in kullanımı sebebiyle işletme dışından da olabilmektedir.

İşletme içinden gelebilecek güvenlik tehditlerine karşı etkin bir iç kontrol sistemi oluşturulmalıdır. Muhasebe departmanında çalışan personel itina ile seçilmelidir ve bu konuda eğitilmelidir. Erişim kontrolları sağlanarak yetkisiz olarak

---

[17] Melih ERDOĞAN, Arman Aziz KARAGÜL ve Cemal ELİTAŞ, a.g.m., s.187.

[18] http://www2.dunyagazetesi.com.tr/, Dünya Oıline, 26/04/2004.

[19] "Virüslere Karşı Güvenlik", http://www.tepum.com.tr/virus.htm

[20] Altay ONUR, "Kurumsal Bilgi Güvenliğine Bakış http://www.bilgiyonetimi.org/cm/.

veri/bilgiye ulaşmak ve bunlar üzerinde değişiklik yapmak engellenmelidir.

İşletme dışından oluşacak tehditler genellikle ağ üzerinden olduğu için ağda gerekli güvenlik önlemlerini almak gerekmektedir. Güvenlik duvarının kurulması, virüslere karşı koruyucu yazılımların yüklenmesi, erişim kontrolünün sağlanması, e-imza, kimlik kontrolü gibi uygulamalar dış tehditlere karşı önemli önlemlerdir.

Ancak teknolojik önlemlerle bilgi güvenliğinin sağlanması tam olarak olanaklı değildir. İşletmelerde, bilgi güvenliği, iş sürecinin bir parçası olmalı, her adımda güvenliği sağlayacak önlemler alınmalıdır. Bunun için işletmede bilgi güvenlik politikası oluşturulmalı, işletme çalışanları ve diğer ilgililer bu konuda bilgilendirilmelidir.

Kaynakça

"Ağ Güvenliği", http://www.tepum.com.tr/ agguvenligi.htm.

"Internet Güvenliği", http://www.tepum. com.tr/ internetguvenlik.htm

"Kurumsal Güvenlik Politikaları ve Yapısı", http://www.ssm.gov.tr/library/docs/tr/teskilat/ dosyalar/bim/kur_guv_pol. pdf.

"Virüslere Karşı Güvenlik", http://www. tepum. com.tr/virus.htm

Abu-Musa, Ahmad A., "The Perceived Threats to the Security of Computerized Accounting Information Systems", Journal of American Academy of Business, Cambridge, Holywood, Sep. 2003, Vol.3, Iss. 1/2.

Erdoğan, Melih, Karagül, Arman Aziz ve Elitaş, Cemal, "Elektronik Veri Değişimi Güvenliği ve Elektronik İmza", Prof.Dr. Yüksel Koç Yalkın'a Armağan, SBF Yayın No: 590, TÜRMOB **Yayın** No: 221, Ankara 2003.

Levi, Albert ve Çağlayan, M.Ufuk "Elektronik Posta Güvenliği İçin PGP Kullanımı", http ://mercan .cmpe. boun.edu.tr/~levi/as97 .htm.

Onur, Altay, "Kurumsal Bilgi Güvenliğine Bakış", http://www.bilgiyonetimi.org/cm/.

Sürmeli, Fevzi, Erdoğan, Melih, Erdoğan, Nurten, Banar, Kerim ve Önce, Saime, Muhasebe Bilgi Sistemi, Açık Öğretim Fakültesi Yayınları No: 532, Ünite 1-17, l.Baskı, Kasım 1996.

Tekin, Abdullah ye Parlakkaya, Raif, "Tümleşik Bilgi Sistemleri ve Muhasebe Bilgi Sistemi", http://www.bilgiyonetimi.org/cm/.

Türkçe Sözlük, T.D.K. Basımevi, 1998.

Umut AL, "Internet'te Veri Güvenliği", Oluşum/38, http ://yunus.hacettepe.edu.tr/~umutal/publicati ons/ datasecurity.pdf.

Yılancı, Münevver, "Muhasebe Bilgi Sistemi ve Kontrol", Kütahya İ.İ.B.F. Yıllığı, 1991.