Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 6(2): 223-240
Cankiri Karatekin University Journal of Institute of Social Sciences, 6(2): 223-240

E-İşletme Güvenliği ve Siber Saldırılar Üzerine Bir Araştırma

Hakan ÇETİN[1], İbrahim GUNDAK[2], Hasibe Hande ÇETİN[3]

Özet

Teknolojinin gelişmesiyle işletmelerin birimleri arasındaki iletişim hızlanmış, büyüyen işletmelerin tek merkezden idaresi ile yöneticilerin karar vermeleri daha kolay hale gelmiştir. İşletmelerin sanal ortama taşınması, işletmelere hem kendi verilerinin güvenliğini sağlamak hem de müşteri verilerini korumak gibi bir sorumluluk da yüklemiştir. Böylece işletmenin fiziki güvenliği yanında birde sanal güvenliği eklenmiştir. Bu çalışmada e-ticaret ve e-işletme kavramları ele alınarak, çeşitli alanlardaki etkileri incelenmiş, Türkiye'de ve Dünya'da gerçekleşen siber güvenlik tehditleri ortaya konularak, siber saldırı sonuçları ve maliyetleri üzerinde durulmuştur.

Anahtar Kelimeler: E-İşletme, E-Ticaret, Siber Saldırı, Siber Güvenlik

A Research on E-Business Security and Cyber Attacks

Abstract

Communication among the business units has been accelerated through the use of technology and decision-making processes of the managers have become easier as a result of the centralized administration of growing businesses. Businesses in virtual platforms have taken on the responsibility of protecting their own data and the customers' data. Therefore, virtual security issues have been added on to the businesses' physical security issues. This study examines the e-commerce and e-business concepts, their influences on various fields, and also focuses on the outcomes of the cyber-attack and its costs by looking into the cases of the cyber security threats that occurred in Turkey and in the world.

Keywords: E-Business, E-Commerce, Cyber Attack, Cyber Security

[1] Akdeniz Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Antalya-TÜRKİYE
E-posta: hakanc@akdeniz.edu.tr
[2] Akdeniz Üniversitesi, AyşeSak Yüksek Okulu, Antalya-TÜRKİYE
E-posta: igundak@akdeniz.edu.tr
[3] Antalya Bilim Sanat Merkezi, Antalya-TÜRKİYE
E-posta: hasibehandecetin@gmail.com

Giriş

Bilgi ve iletişim teknolojilerindeki gelişmeler insan hayatının yaşam standartlarından, işletmelerin işleyiş süreçlerine kadar birçok alanı etkilemiştir. Planlama, pazarlama ve örgütleme gibi temel işletme fonksiyonları işletmeler için ne ifade ediyor ise günümüz işletmeleri için de bilgi onu ifade etmektedir. Ağ teknolojilerinin yaygınlaşması, bilginin toplanmasını, saklanmasını, yayılmasını hızlandırmış ve bilginin önemini daha çok artırmıştır.

Günümüzde bilgiyi elde bulundurma ve etkili bir şekilde kullanma, işletmenin bilgi ve iletişim teknolojilerini hangi oranda ve nasıl kullandığı ile ilgili hale gelmiştir. Bu doğrultuda yöneticiler işletmelerini teknolojiye uyumlu hale getirmiş ve ağ teknolojilerinin kullanılması ile birlikte işletmeler elektronik işletmelere (E-işletmelere) dönüşmüştür. E-işletme, işletmelerdeki iş döngülerini ve iş döngüsüne dahil olan bütün yapıyı bilgi teknolojileri ve internet teknolojileri kullanarak düzenleyen sisteme denilmektedir (Kovacich, 1998: 129, Damanpour, 2001: 18).

Bilginin önemli bir varlık olduğu günümüzde işletmenin hem kurum içi hem de kurum dışı bilgilerinin başka şahısların eline geçmesi istenmeyen bir durumdur. İşletmelerin bilgi ve iletişim teknoloji alt yapıları kurulurken dikkat edilmesi gereken en önemli unsurlardan biriside güvenliktir. Güvenlik problemlerinin oluşmasında siber saldırılar ve kullanıcı kaynaklı eksiklikler önemli başlıklardan sayılabilir. Son yıllarda yapılan araştırmalar işletmelerin siber saldırılar sonucu parasal kayıplarının yüksek miktarlara ulaştığını göstermektedir. Parasal kayıpların azaltılması ve önemli bilgilerin istenmeyen şahısların eline geçmesinin engellenmesi için çeşitli çalışmalar yürütülmektedir. Siber olaylara müdahale ekibinin kurulması, akıllı ve biyometrik doğrulama sistemlerinin hayata geçirilmesi bu önlemlerden bazılarıdır. Siber güvenlik risklerinin önümüzdeki yıllarda işletmeler, ülkeler ve küresel ekonomi için sorunlar ortaya çıkarabileceği tartışılmaktadır.

Çalışmada e-işletme kavramı tüm yönleriyle ele alınmış, çeşitli alanlardaki etkileri açıklanmış, güvenlik politikaları, siber saldırı türleri, işletmeyi tehdit eden unsurlar, siber saldırı sonuçları ve maliyetleri üzerinde durulmuştur.

E-Ticaret ve E-İşletme Kavramları

Teknolojinin gelişimi ile birlikte ticaretin yapılış türü değişmiştir. Teknolojinin yaygınlaşmasından önceki ticarette işletmenin etki alanı ve faaliyet düzeyi çok sınırlı ve işletme sahibine bağımlı iken, teknolojinin gelişiminden sonra ticari faaliyetler daha seri, daha optimum ve daha genel yapılmaya başlanmıştır (Özmen, 2013: 10-11). Yeni dönemde ortaya çıkan elektronik ticaret (e-ticaret) alış veriş yapılış şeklini tamamen değiştirmiştir.

Elektronik ticaret, ağ teknolojileri kullanılarak hem kuruluşları hem de bireyleri kapsayan her türlü işlemin gerçekleştirilmesi olarak tanımlanmaktadır (OECD, 1997).

1994 yılından 2013'e kadar geçen süreçte e-ticaretin hacmi PayPal ve Nielsen küresel sınır ötesi online alışveriş harcama ve davranış modellerini araştırdığı "Modern Baharat Yolları: Sınır Ötesi Alışverişin Kültürel Etkisi" adlı raporunda ABD, Birleşik Krallık, Almanya, Avustralya, Çin ve Brezilya alışveriş pazarının 105 milyar dolara ulaştığı ve bu rakamın 2018'e kadar %200 oranında artacağına dair önemli veriler sunulmaktadır (Paypal, 2014). E-Marketer'in dünya çapında yaptığı (B2C) iş modeliyle gerçekleşen ticari faaliyet araştırma sonucuna göre ise dünyada gerçekleşen elektronik ticaret işlem hacminin 2014 yılında 1,500 trilyon dolar seviyesinde olduğu rapor edilmiştir (E-Marketer, 2014).

Teknolojik gelişmelerin bir diğer etkisi ise işletmelerin işleyiş yapılarını değiştirmesi olmuştur. Değişimin sürekli yaşandığı ve rekabetçi ortamın arttığı çağımızda işletmelerin varlıklarını devam ettirebilmesi, iş süreçlerini, ürünlerini ve örgütsel yapılarını sürekli yenilemesine bağlı hale gelmiştir. İşletmelerin değişim sürecinde bilgi ve iletişim teknolojileri önemli rol oynamış ve işletmeler dijital işletmeye yani e-işletmeye dönüşmüştür.

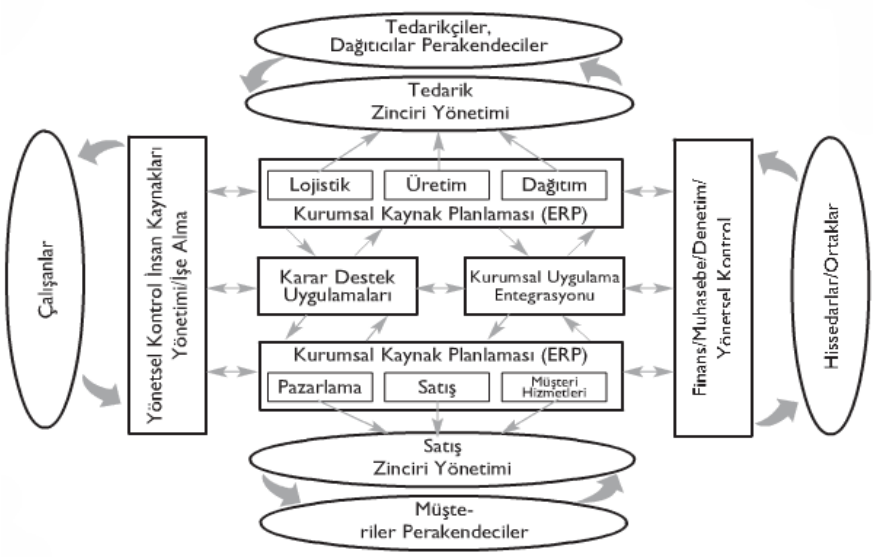
O'Brien ve Marakas (2008: 250) e-işletmeyi, hem kurum içi ağda, hem de müşteri ve işletme ortaklarıyla, elektronik ticareti, kurum iletişimi ve işbirliğini desteklemek için internetin, diğer ağların, bilgi teknolojilerinin ve web-tabanlı işletme süreçlerinin kullanılması olarak tanımlamaktadır. Başka bir tanımda ise işletmenin müşterileri, tedarikçileri ve diğer paydaşlarıyla örgütsel iletişim ve işbirliğini, işletme süreçlerini güçlendirmek için bilgisayar ve ağ teknolojisinin kullanılması olarak ifade edilmektedir (Combe, 2006: 1).

Teknolojik gelişmelerin getirdiği değişim ve ticaret yapış şekillerine göre işletmeler yapı olarak kendi alanında üçe ayırılabilir.

- *Tam E-işletme:* İşletmelerin ürün veya hizmeti, fiziksel erişilebilirlikle değil sanal erişilebilirlikle muhatabına ulaştırdığı işletme türüdür (hepsiburada.com, ebay.com gibi).
- *Kısmi E-işletme:* İşletmelerin ürün veya hizmetlerinden bir tanesinin elektronik olduğu işletmelerdir (teknosa.com gibi).
- *Normal İşletme:* İşletmelerin ürün veya hizmetlerinin hiçbirisinin elektronik olmadığı işletmelerdir.

Bütün işletme fonksiyonlarının birbirinden ayrı yürütüldüğü geleneksel işletmelerin aksine e-işletmelerde işletmenin tüm fonksiyonları (üretim, insan kaynakları yönetimi, tedarik zinciri yönetimi, müşteri ilişkileri

yönetimi, finansal tedarik zinciri) bir veri tabanı ve ağ teknolojileri (internet, intranet veya ekstranet) uygulamalarıyla eşzamanlı olarak yürütülmektedir (Sevim ve Gül, 2012). Şekil 1'de görüldüğü gibi e-işletme uygulaması iç ve dış tüm etkenleri içine alacak şekilde bütünleştirilmiştir.



Şekil 1: E-İşletme Uygulama Mimarisi (Çağlar, 2010).

E-İşletmelerde Güvenlik Politikaları

İşletmeler için en önemli olan detaylardan birisi de güvenliktir. Yapılan işlemlerin fiziksel ortamdan sanal ortama taşındığı ve bilgiyi korumanın daha da zorlaştığı günümüzde şirket verileri veya şirket ile bağlantılı kişilerin bilgileri korunmaya muhtaçtır. E-işletmelerde güvenlik, alışveriş verilerinin, depolanan bilgilerin, yazılım ve donanım bileşenlerinin saldırılara karşı korunmasını kapsamaktadır (Özmen, 2013: 485).

Geleneksel işletmelerden farklı olarak e-işletmelerde yapılan işlemlerin sanal olması riskleri daha da artırmakta ve farklı güvenlik önlemlerinin alınması gerekmektedir. İşletmelerdeki güvenlik konusu bütün çalışanları ilgilendiren bir konudur, bu konuda yeterli düzeyde bilinçlendirme ve güvenlik kültürü oluşturulmalıdır. Güvenlik kültürü işletmenin kârlılık prensibi gibi aynı derecede önemli bir prensiptir. Şu unutulmamalıdır ki işletme ne kadar iyi teknoloji ile donatılırsa donatılsın güvenlik kültürü yerleştirilmemişse o işletmenin her an bir güvenlik tehdidi ile karşı karşıya olduğu bilinmelidir.

Güvenliği sağlamak sadece giriş-çıkışların kontrolü değil, yetkilendirilmiş kişilerin yetkisi dâhilinde işlemler yapmasını sağlamaktır. İşletmelerde güvenlik ilkesi en fazla saldırıya uğrayan birim olduğundan dolayı sürekli dikkatli olunmalı ve yeni teknolojilerin kullanılmasına özen gösterilmelidir.

E-işletmenin kuracağı güvenlik sistemi ihtiyaçlara cevap verebilecek nitelikte, esnek ve sızıntılara karşı sürekli sistemi kontrol eden bir yapıda olmalıdır. E- işletmelerde güvenlik mimarisi oluşturulurken üç temel noktaya dikkat edilmelidir. Birincisi müşterinin kullandığı yazılımların güvenliği, ikincisi verilerin depolandığı veri tabanlarının güvenliği ve üçüncüsü ise işletmenin kendi güvenliğidir (Karabacak, 2008: 68).

B2B International ve Kaspersky Lab. tarafından gerçekleştirilen "Global Kurumsal BT Güvenlik Riskleri 2014" araştırmasına göre Türkiye'de işletmelerin kurum içi tehditler dolayısı ile %37'sinin hasas veri kaybına uğradığı ve bu veri kayıplarının sebeplerinde %43'nün yazılımsal güvenlik açıklarından, %17'sinin personelin yanlışlıkla sızdırmasından, %18'nin ise kasıtlı olarak yapılan sızıntılardan kaynaklandığı rapor edilmektedir. (Kaspersky Lab., 2014).

İşletmelerin saldırılara karşı strateji geliştirebilmeleri ve korunabilmeleri için güvenlik tedbirlerini bir politika haline dönüştürmeleri gerekmektedir. Güvenlik politikası, işletmenin bilgisayar ağının, bilginin gizlilik derecesinin ve kullanıcı haklarının bir bütün olarak ele alındığı kurallar bütünüdür (Can ve Akbaş, 2014).

Güvenlik politikaları işletmeye özgü belirlenmelidir. Ama genel çerçevede olması gerek ana başlıklar gizlilik politikası, bütünlük politikası, kullanılabilirlik politikası, yönetimsel güvenlik politikası ve ticari güvenlik politikası olmalıdır (Sınav, 2014).

E-İşletmelerde güvenlik sistemleri kurulurken dikkat edilmesi gereken kurallar şu şekilde sıralanabilir (Özmen, 2013: 511-512);

- *Sisteme giren kullanıcıların tanımlanması;* Günümüzde hemen hemen bütün işletmeler sistem kullanıcılarının üye olmasını istemektedirler. Üyelik sistemi ile kullanıcıların tanımlanması amaçlanmaktadır.
- *Girişlerin kontrol edilmesi;* Sistemi kullanan kullanıcılar hakkında bilgileri bir veri tabanında tutarak girişlerin kontrolü amaçlanmaktadır.
- *Alternatif sunucuların kullanılması;* Kullanıcılar web üzerinden bir ürün veya da hizmeti satın aldığı zaman alternatif sunuculara bağlanarak farklı güvenlik işlemlerinin sağlanması amaçlanmaktadır.
- *Kullanıcıların takibi;* Web sitesine giren ve kullanan kişilerin yaptıkları işlemleri kontrol etmeyi amaçlamaktadır.

- *Kanun ve yönetmelikler;* Kamu ya da kişi haklarının korunması bağlamında yapılan işlemlerin IP adreslerinin tutulması gerekmektedir. Adli ya da idari bir talep gelmesi durumunda bilgilerin yasa ve yönetmelik koyucularla paylaşılması gerekmektedir.

Güvenlik politikası kurallarının belirlenmesi noktasında kuralların birbiriyle çakışmaması gerekmektedir. Kuralların birbirini kesmesi sistemde açıklara sebep olacak ve sistemin güvenliği tehditlerle karşı karşıya kalacaktır. Saldırı türleri ve şekillerinin sürekli değiştiği günümüzde güvenlik politikasının aktif yaşayan bir anlayışla yani bir yaşam döngüsü şeklinde ele alınması gerekmektedir.

İşletmelerde Güvenliği Tehdit Eden Unsurlar ve Saldırı Türleri

İşletmelerin internet, intranet ve ekstranet gibi teknolojileri kullanması ve çalışanların birçoğunun internete bağlantılı işlemler yürütmesi işletmeleri elektronik saldırıların hedefi haline getirmiştir. E-işletmelere yönelik olarak kullanılan birçok saldırı yöntemi ve modeli bulunmaktadır. Saldırganlar para, itibar kazanmak ve yeteneklerini sergilemek için bu işleri yapmaktadırlar. Bu kişi veya kişilere karşı alınan güvenlik önlemleri, işletmede maliyetlerin artmasına ve işlem hızının yavaşlamasına sebep olmaktadır (Özmen, 2013: 489-490).

2015 Symantec İnternet Güvenlik Tehdidi Raporu verilerine göre 2014'de gerçekleşen saldırıların %60'ının KOBİ'leri hedef aldığı belirtilmektedir. Aynı raporda 2014 yılı içerisinde 317 milyon zararlı yazılım tespit edilmiş ve fidye yazılımlarının bir önceki yıla göre %113 oranında artış gösterdiği belirtilmiştir (Symantec, 2015). Son zamanlarda üretim sektörü saldırganların yeni gözdesi olarak öne çıkmaktadır. Bu yükselişte en önemli unsur üretim tedarik zincirinde yer alan üstlenici ve taşeron firmaların artması gösterilmektedir. Tedarik zincirindeki üstlenici ve taşeron firmalara yapılan saldırılarla ana hedefteki büyük işletmeye varılmak istenmektedir.

Mobil teknolojilerin yaygınlaşması ile işletmeye yönelik tehditler mobil cihazlar üzerinden gelmeye başlamıştır. Cyren (2015) firmasının yayınladığı 2015 Cyberthreat Yearbook Report verilerine göre android tabanlı zararlı mobil yazılımlar bir önceki yıla göre %61 oranında artmıştır. Symantec (2015) raporuna göre ise 2014 yılı içerisinde 46 yeni kötülcül yazılım keşfedilerek 2014 yılı içerisinde aktif olan kötülcül yazılım sayısı 277'ye çıkmıştır. Mobil teknoloji kaynaklı gelen tehditlerin %32'sini e-posta ve telefon numaralarını hedef alan saldırılar oluşturmaktadır (Symantec, 2015).

İşletme veya herhangi bir kuruma yönelik oluşabilecek siber tehditler, sisteme yetkisiz erişim, sistemin bozulması veya engellenmesi, bilgilerin değiştirilmesi, yok edilmesi, ifşa edilmesi ve çalınması başlıklarında

toplanabilir (Atalay, 2014). Siber tehditlerde öne çıkan bazı tehdit türleri şunlardır:

- *Meşru sitelere verilen zararlı içerik bulunduran reklamlar;* meşru sitelerin reklam alanlarını satın alarak saldırı kodlarını bu alanlarda saklayıp reklamlar aracılığı ile yapılan saldırı türüdür.
- *Fidye yazılımlar (Ransomware);* Saldırganlar tarafından güvenliğine zarar verilmiş web siteleri aracılığıyla kullanıcılarının bilgisayarlarını kilitleyip fidye karşılığında kilidi açma mantığı ile hareket edilen saldırı türüdür. Türkiye'de "Sahte Fatura" gönderimiyle gerçekleştirilen saldırı aslında bir oltalama (phishing) yöntemidir. Sahte fatura ile kişiler farklı bir sayfaya yönlendirilir ve kişinin tıkladığı link bir programı çalıştırarak kişinin bilgisayarında bulunan Pdf, Word, Excel vs. tarzındaki doyaları şifreler (*Cryptolocker)* ve bu şifrenin çözümlenmesi için kişilerden bir ücret talep edilir. Trend Micro (2015) 2014 verileri üzerinden yaptığı araştırmıya göre *Cryptolocker'dan* en fazla etkilenen ülkeler arasında Türkiye %22,19 ile ikinci sıradadır.
- *DDoS (Distributed Denial of Service);* Dağıtık servis engelleme saldırısı olarak ifade edilmektedir. Saldırının temel ilkesi birçok makinadan belirlenen hedef veya hedeflere istek gönderimi yolu ile özellikle hedefin band genişliği işgal edilerek hedefin devre dışı bırakılmasıdır. İlk olarak Haziran 1998 yılında rastlanılan bu saldırı türüne günümüzde sıkça rastlanılmaktadır (Lin ve Tseng, 2004).
- *HeartBleed;* Apache ve Nginx gibi popüler sunucularda Mart 2014 yılında bulunan açık şifreli iletişimde yaygın olarak kullanılan OpenSSL kütüphanelerinde yer almaktadır. Buradaki açıktan yararlanılarak dünya çapında yaklaşık 500.000 websitesinin içerisine girilmiş ve burada yer alan kullanıcı isimleri ve parolaları ele geçirilmiştir (Durumeric vd. 2014).
- *Shellshock;* Unix ve Linux tabanlı işletim sistemlerinin kullandığı BASH (Bourne-Again Shell) uygulamasından kaynaklanan bir açıktır. Bu açıktan yararlanılarak sisteme uzaktan erişim yapılıp istenen komutun çalıştırılması sağlanmaktadır (Altundal, 2014).
- *Veri Hırsızlığı;* Veri hırsızlığı 2014 yılında en çok konuşulan konu haline gelmiştir. Bu yöntemle Sony Picture, Ebay, Apple, Turkcell, J.P.Morgan Chase gibi firmaların verileri çalınmıştır (Altundal, 2014).
- *APT (Advanced Persistent Thereat);* Devlet kuruluşları, kritik altyapılar, bankacılık ve finans sektörü, askeri kuruluşlar ve savunma sanayi gibi belli bir hedefe yönelmiş uzun süreli saldırı anlamına gelen APT için en iyi örnekler Stuxnet, Duqu, Flame'dir. Stuxnet ile İran nükler programı hedef alınmış ve sisteme erişilerek makinaların yüksek hızda çalıştırılıp devre dışı kalması sağlanmıştır (Gücüyener, 2015: 19).

Siber Saldırı Analizi

Symantec İnternet Güvenlik Tehdidi Raporu 2014 sonuçlarına bakıldığında her geçen yıl tehdit sıralamasında Türkiye üst sıralara çıkmaktadır. Tablo 1'de görüldüğü gibi Türkiye siber suçlar sıralamasında dokuzuncu sırada yer almaktadır (Symantec, 2014).

Dünya Siber suçlar sıralamasında Amerika Birleşik Devletleri %23 ile en fazla siber suçun gerçekleştiği ülke olurken Türkiye dünya ülkeleri arasında siber suçların %3'nün gerçekleştiği 9. ülke olmuştur.

Tablo 1: Siber Suçlar Dünya Sıralamasında Türkiye'nin Durumu

	2011	2012	2013
Genel Siber Saldırılar	21	18	9

Kaynak: İnternet Security Threat Report, 2014, Fortinet -2014 Threat Landscape Report

Türkiye'nin Dünya'da siber suç sıralaması belirlenirken kullanılan başlıklar/sıralamalar Tablo 2'de verilmiştir. Türkiye siber suçların gerçekleştirildiği yöntemlerde Spam ve Zombi sıralamasında ilk beşe girmektedir.

Tablo 2: Türkiye Siber Suç Sıralaması

Siber Suç Sıralama Başlıkları	
Kötü Niyetli Bilgisayar Aktivitesi	%3
Kötü Niyetli Kod Sıralaması	15
Spam Zombi Sıralaması	5
Oltalama Web Site Sıralaması	24
Bot Sıralaması	8
Saldırı Başlangıç Noktası Sıralaması	12

Kaynak: Enigmasoftware (2014)

2014 yılı içerisinde yedi önemli APT (gelişmiş kalıcı tehdit) olayı rapor edilmiştir. 55 ülkeden 4400'ün üzerinde kurumsal sektör üyesinin etkilendiği saldırılarda milyonlarca dolar kaybedilmiştir. (UITSEC, 2015). McAfee firmasının 2015 yılı ilk yarıyılı Ağustos ayı tehdit raporuna göre Malware (Kötü amaçlı yazılım) olayları 2015 yılı ilk çeyreğe göre ikinci çeyrekte %12 büyüyerek 433 milyon vakaya çıkmıştır.

Trendmicro (2015) şirketinin 2014 yılı raporunda Malware çeşitlerinden sıklıkla karşılaşılan tiplerinin Sality, Downad ve Gamarue olduğu

belirtilmiştir. Ev kullanıcıları ve şirketlerin bilgisayarlarına ençok bulaşan malware çeşitleri ise Tablo 3'de gösterilmiştir.

Tablo 3: Bilgisayarlara Ençok Bulaşan Malware Çeşitleri

Küçük İşletmeler		Büyük ve Orta İşletmeler		Ev	
Downad	11K	Downad	59 K	Gamarue	40 K
Sality	8K	Dunihi	35 K	Sality	39 K
Vobfus	5K	Sality	33 K	Virux	23 K

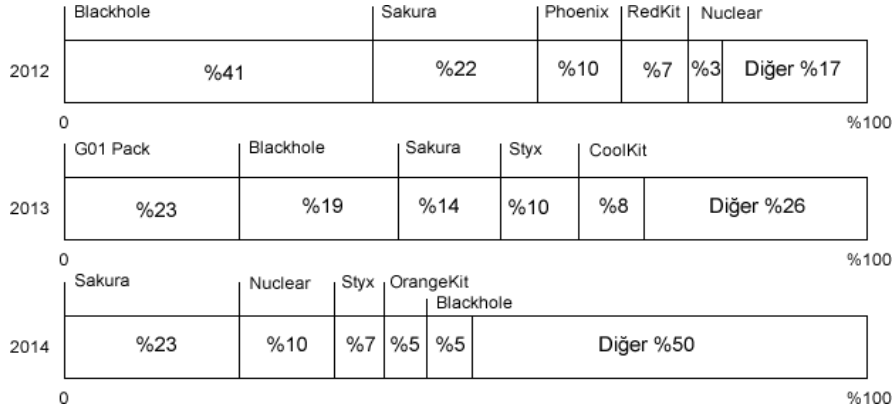
Aynı raporda ransomware (fidye yazılımları) tehditlerinde 2015 yılı ikinci çeyreğinde ilk çeyreğine göre %58'lik bir artış meydana gelirken bir önceki yıla göre %127'lik bir artış meydana gelmiştir. Böylelikle fidye yazılım tehdidi ikinci çeyrekteki artışı ile dört milyon bandının üzerine çıkmıştır.

Tablo 4: Fidye Yazılımın Ülkelere Göre Dağılımı (%)

	Ülke	2013	Ülke	2014
1	ABD	35,93	ABD	41,81
2	Japonya	19,94	Japonya	16,11
3	Almanya	6,39	Avustralya	6,42
4	Avustralya	5,67	Almanya	3,98
5	Türkiye	3,19	Türkiye	3,35
6	İtalya	2,49	Hindistan	2,51
7	Fransa	2,00	Kanada	2,24
8	Kanada	1,87	Fransa	2,19
9	Filipinler	1,70	İngiltere	1,95
10	İngiltere	1,64	İtalya	1,85
	Diğerleri	19,18	Diğerleri	17,58

Trend Micro şirketinin 2014 yılı verileri için yayınladığı yıllık güvenlik raporunda fidye yazılımın ülkelere göre dağılımı Tablo 4'de gösterilmiştir. Fidye yazılımına maruz kalan kesimlere bakıldığında %69,75 ile ev kullanıcıları, %11,66 ile Küçük boyutlu işletmelerin ve %18,59 ile orta ve büyük boyutlu işletmelerin olduğu rapor edilmektedir (Trend Micro, 2015).

Nisan 2015 Symantec Internet Security Threat Report verilerine göre ilk beş web saldırı araçlarının yıllara göre kullanım oranları Şekil 2'de gösterilmiştir. Şekil 2'de yıllara göre web saldırı araçlarının farklılaştığı ve 2014 yılı ile %50'lere ulaştığı görülmektedir. Blackhole saldırı aracı %41'lerden %5'lere kadar düşmüştür (Symantec, 2015).



Şekil 2: Yıllara Göre İlk 5 Web Saldırı Araçları (Symantec, 2015)

Elektronik Saldırıların Sonuçları

E-İşletmelere düzenlenen saldırıların genel amacı, işletmenin internet üzerinden hizmet sunmasını engellemek ve işletmenin itibarını yıpratmaktır. Tablo 5'de gerçekleştirilen saldırı çeşitleri ve sonuçları yer almaktadır.

ABD siber güvenlik kuruluşu Arbor Networks (2015)'ün 2014 verilerine göre Türkiye'ye yönelik siber saldırıların diğer ülkelere göre daha fazla olduğunu rapor etmektedir. 2014'ün ilk yarısında dünya genelinde siber saldırılar %68 oranında hız keserken Türkiye'de %6 oranında artış göstermiştir. Siber saldırılarda Türkiye'yi sırayla Rusya, ABD ve İsviçre takip etmektedir (BThaber, 2014).

Siber saldırılar devlet kuruluşlarını, partileri, politikacıları, sanatçıları, finans sektörünü (bankalar, borsa, kredi kart merkezleri, para transfer merkezleri), sporcuları, şirketleri vb. kişi veya kuruluşları hedeflemektedir. Bu hedeflere yapılan siber saldırılarda amaç hedef şaşırtma, banka bilgilerini ele geçirme ve veri hırsızlığı gibi işlemlerdir. 2014 yılı ikinci yarısında elde edilen verilere göre dünyada siber saldırıların nedenleri yüzdelik dilimler ile ifade edilmiştir (BThaber, 2014).

- Politik/ideolojik anlaşmazlıklar %33
- Nihilizm/vandalizm %27
- Servislerinin potansiyel müşterilere demosu %24
- Sosyal networking ile ilgili %22
- Kişiler ya da gruplar arası rekabet %20

- Hata %17
- İşletmeler arası rekabet %15
- Hedef şaşırtma yoluyla veri hırsızlığı %15
- Fidye/gasp amaçlı %14
- Flaş kalabalık %12
- Finans sektörü manipülasyonları %12
- Suçlular arası anlaşmazlık %7
- Bilinmeyen %25

Tablo 5: Saldırılar ve Sonuçları

Saldırılar	Sonuçları
Bilgileri yok etmek	Verinin ve bilginin deşifre edilerek gizliliğinin bozulması
Sistemin üçüncü şahıslar tarafından dinlenmesi	
Bilgileri değiştirmek	Bilginin değiştirilerek bütünlüğünün bozulması
Veri, ses, görüntülü iletişimine engel olmak	Sistemin çalışmamasından doğan kayıplar
Şifre, kredi kartı numarası çalmak ya da hileli biçimde elde etmek	İşletmelerin ve müşterilerin maddi ve itibar kaybı
Güvenlik açıkları: Personeli kandırarak içeriden bilgi elde etmek	
İftira atmak	
Hizmetleri engelleme	

Kaynak: Özmen (2013: 491)

E-İşletmelerde Güvenlik Katmanları

İşletmelerde hem fiziki hemde elektronik güvenliğin sağlanabilmesi belirli önlemlerin alınmasına bağlı olduğu gibi mutlak güvenliğin olmadığı da akıldan çıkarılmamalıdır. Güvenliğin sağlanabilmesi için belirli süreç ve prosedürlerin devrede olması gerekmektedir. Bu süreç ve prosedürler (Golchha vd., 2015) ;

- Kullanıcı hesaplarının ve veri dosyalarının şifrelenmesini ve yedeklenmesini gerektirmektedir.
- Sisteme erişen kişilerin kimlik tespitinin ve yetki kontrolünün yapılması gerekmektedir.
- Ağ güvenliğinin sağlanmasında en yaygın kullanılan yöntemlerden biri olan güvenlik duvarları sisteme erişmek isteyen kişileri ve paketleri filtreleme yapması gerekmektedir.

- Saldırı tespit sisteminin (IDS) ve antivirüs yazılımlarının kurulması gerekmektedir.
- Ağ cihazlarının ve kullanılan sistemlerin yazılım güncellemelerinin yapılması gerekmektedir.
- Ağ içerisinde gerçekleşen olayların log kayıtlarının tutulması ve kayıtların merkezileştirilmesi gerekmektedir.

E-işletmelerde sistem güvenliğini sağlamak ve güvenli ortam oluşturmak için sistem güvenliği dört boyut da değerlendirilebilir;

Tablo 6: Sistem Güvenlik Katmanları

İşletim Sistemleri	Altyapı (Ağ) Güvenliği Katmanı
İnternet, Intranet, Ekstranet	
Bilgi Sistemleri Uygulamaları	Uygulama (İşlem) Güvenliği Katmanı
Veri Tabanları	
Hazır Yazılımlar	
Güvenlik Politikası, Standartlar, Personel	Sistem Güvenliği Katmanı
Bina, Donanım	Fiziki Güvenlik Katmanı

Altyapı (Ağ) Güvenliği Katmanı

Ağ sistemleri verilerin ve bilgilerin işletme arasında veya işletmeler arasında elektronik cihazlar kullanılarak iletişimin gerçekleştirilmesi için kurulmuştur. İlk ağ sistemi 1974-76 yılları arasında ABD Savunma Bakanlığı'nca bir Intranet ağı kurularak gerçekleştirilmiştir. 1983 yılında TCP/IP protokolünün kullanıma girmesiyle internet global hale gelmiş ve ticari amaçlarla kullanılmaya başlanmıştır (Kara, 2013: 8).

Ağ sistemlerinin kullanılması ağ güvenliğini beraberinde getirmiştir. Ağ güvenliğinde alınan önlemlerin başında güvenlik duvarları (firewall), Web filitreleme (Web filtering), Uygulama kontrolü (application control) ve Saldırı tespit ve önleme sistemleri (intrusion detection and prevention system, IDS/IPS) gelmektedir (Can ve Akbaş, 2014). Ağ güvenliği için bunun dışında kullanılan uygulamalar ise;

- *Süzülen veriler:* TCP/IP protokolünün ağ katmanında çalışır. Firewall'dan kurallar dahilinde geçişine izin verilmektedir.
- *TCP/IP bağlantılarında Proxy sunucular:* Proxy sunucular, dış dünyada bir "IP" numarasını gösterir. Yerel ağ üzerindeki "IP" adreslerini gizleyerek bunları muhtemel saldırılardan korumaktadır.

- *Sanal Ağlar (Virtual Private Networks-VPN):* "IP" adreslerinin şifrelenmesini sağlamaktadır.

Uygulama (İşlem) Güvenliği Katmanı

E-işletmelerde veri iletişim güvenliği önemli bir husustur. Sanal ortamda tarafların işlem ve iletişim güvenliğinin sağlanması, üçüncü şahıslara karşı önlemlerin alınması, takip edilmesi ve kimlik doğrulama ile işlemlerin sonuçlandırılması işlemlerini ifade etmektedir (Özmen, 2013: 506).

Güvenli alış-verişin yapılması için, verinin bütünlüğünü koruyan ve gizliliğini sağlayan teknolojiler kullanılmaktadır. Kullanılan teknolojiler;

SSL (Secure Sockets Layer) : SSL protokolünde amaç, kişisel gizliliği ve karşılıklı bilgi alış-verişi sırasında güvenliği sağlamak için kullanılır (Freier vd, 2011).

TSL (Transport Layer Security) : İşleyiş olarak SSL benzemektedir. Tercih yapmamız gerekirse TSL kullanmamız daha iyi olacaktır çünkü daha güvenlidir (Özmen, 2013: 508).

Elektronik İmza: E-İşlemlerde kişinin kimliğini belirlemeyi sağlayan bir methotdur. Yasal olarak bağlayıcı olan ve imzalanan evrakların elektronik ortama aktarılarak zaman, işlem hızı ve diğer masraflardan tasarruf sağlamak için geliştirilmiş bir uygulamadır (Turktrust, 2014).

Sistem Güvenliği Katmanı

E-işletmelerde Sistem güvenliği, çalışan ve uygulanan sistemin doğru şekilde çalışmasını sağlamak, yapılacak ve alınacak güvenlik önlemlerinin düzenlenmesini sağlamayı kapsamaktadır. Değişim ve gelişimle beraber farklı risklerin ortaya çıktığı E-işletmelerde öncelikle bilgi sistemi güvenliği sağlanmalıdır. Bilgi sistemi güvenliği ISO 27001 standardı e-işletmelerin kritik öneme sahip verilerinin korunması için gerekli olan dinamik bir bakış açısını getirmektedir. Mutlaka e-işletmelerin bu standarda sahip olmaları gerekmektedir (Sevim ve Gül, 2012).

Fiziki Güvenlik Katmanı

E-işletme sistemi işletmenin kendi bünye ve kontrolünde ise her türlü fiziki güvenlik şartlarını işletmenin kendisinin yerine getirmesi gerekmektedir. İşletme sanal barındırmayı satın alma şeklinde gerçekleştiriyor ise yükümlülük hizmet satın alınan firmaya aittir. Her iki yöntemde de e-işletmenin alması gereken tedbirler bulunmaktadır. Her hangi bir doğal afet veya acil durumda sistemi güvene alacak bir stratejinin geliştirilmesi

gerekmektedir. Elektrik kesintilerine karşı jenaratör sistemi, bilişim sistemlerinin ve çalışanların rahat çalışabilmesi için havalandırma sistemi, sistemin aşırı ısınmasını önleyecek soğutma sistemi, her hangi bir yangın tehlikesinde yangının büyümesini önleyici yangın söndürme sistemi, hırsızlık olaylarına karşı alarm ve güvenlik sistemleri (kamera, biyometrik kontrol) gibi hayati öneme sahip bileşenlerin kurulu olması gerekmektedir.

Türkiye ve Dünyada Siber Saldırı Maliyet Verileri

Siber saldırıların yol açtığı kayıplar organizasyonlara ciddi mali yükler getirmeye başlamıştır. Oluşan bu mali yükün tespiti ve olayın ne kadar ciddi olduğunu gösteren çeşitli şirketlerin yapmış olduğu araştırmalar bulunmaktadır. Bunlardan bazıları veri ihlalini engellemek üzerine yapılan harcamaları ve siber saldırı oranlarını ön plana çıkarırken bazı araştırmalarda veri sızıntısı ve veri kaybından kaynaklanan maliyeti ön plana çıkarmaktadır.

2015 Global State of Information Security araştırmasına göre bilgi güvenliği alanında raporlanan vaka sayısı %48'lik artış ile 42,8 milyona ulaşmıştır. Aynı raporda yıllık 1 milyar veya daha fazla brüt gelire sahip büyük ölçekli organizasyonlara yönelik olarak bir önceki yıla göre yapılan saldırılarda, %44'lük artış olmuştur. 100 milyon dolar ile 1 milyar dolar arası gelire sahip orta ölçekli organizasyonlarda ise %64'lük artış meydana gelmiştir (Pwc, 2014). Gartner araştırma firmasının IT güvenliği için şirketlerin 2014 yılında 71.1 milyar dolar olarak gerçekleşen harcamalarının 2015 yılı için %8,2 artış ile 76,9 milyar dolara ulaşması tahmin edilmektedir (The Wall Street Journal, 2014). Visiongain şirketinin araştırmasına göre 2015 Temmuz ayına kadar yapılan siber güvenlik harcaması 75 milyar dolara yaklaşırken 2018 yılında 101, 2020 yılında ise 170 milyar doları bulacağı tahmin edilmektedir (Siberbülten, 2015). Küresel pazar araştırma şirketi Vanson Bourne'nun gerçekleştirdiği araştırmaya göre ise dünya genelinde şirketler veri sızıntısını engellemek için aylık ortalama 4129 Euro harcama yaparken, Türk şirketlerinin 3220 Euro harcadığı ifade edilmektedir.

2014 yılında Kaspersky Lab. ve B2B International işbirliğiyle gerçekleştirilen Global Kurumsal BT Güvenlik Riskleri araştırmasına göre, dünyada küçük veya orta ölçekli işletmelerde ortalama veri ihlali maliyetinin 47 000 $ olduğu bilinmektedir. Batı Avrupa'da bu rakam 55 000 $ tutarına kadar çıkmaktadır. Kayıplar sadece mali ve finansal olarak değil şirketin imajı ve itibarının zarar görmesine de olmaktadır. Kayıp veri vakalarında olayların yarısından fazlasının (%56) şirketin itibarına veya güvenilirliğini olumsuz etkilediği araştırmada ifade edilmektedir (Kaspersky, 2014).

McAfee'nin himayesinde Stratejik ve Uluslararası Araştırmalar Merkezi (CSIS) tarafından yapılan araştırmaya göre siber suçların dünyadaki yıllık

maliyetinin ortalama 375 ile 575 milyar $ seviyelerinde olduğu tahmin edilmektedir. 2014 yılında siber suçların dünya ekonomisine vermiş olduğu zararın 160 milyar doları bireysel çapta olmak üzere toplam 400 milyar doların üzerinde olduğu ifade edilmektedir. Aynı araştırmada siber saldırılara en çok maruz kalan sektörlerin başında %68 ile otomobil, %66 ile kimya ve ilaç sektörü, %60 ile finans, %58 ile de sağlık sektörü yer almaktadır (McAfee, 2014). Norton 2013 raporuna göre Türkiye'de siber saldırılardan kaynaklanan toplam maliyet 2 milyar dolar seviyesine ulaşmıştır ve kişi başı yaşanan ortalama maliyet ise bir önceki yıla göre 6 kat artarak 309 dolar seviyelerine ulaşmıştır (Symantec, 2013).

NetDiligence (2014) şirketinin veri ihlali olayları üzerine yaptığı araştırmada, finansal kayıplara neden olan veri kayıplarının %74'nün hackerlar ve %23'nün zararlı yazılımlar yüzünden meydana geldiğini ortaya koymaktadır. Bu kayıpların en düşüğü 1000 $ ile en yükseği 13,7 milyon $ arasında gerçekleşmiştir. Olay başına ortalama kayıp bir önceki yıla göre %23 azalarak 733,109$ olarak gerçekleşmiştir (NetDiligence, 2014).

Sonuç

İnternet ve bilişim teknolojilerinin gelişmesi hem işletme içi hemde işletme dışı iş süreçlerini yeniden şekillendirerek, ticaret yapılış şeklini de değiştirmiştir. Bu yeni şekillenmede E-işletme ve E-ticaret kavramları hayatımızın içerisine girmiş ve yeni bir ekonomi doğmuştur.

Değişim yeni sektörlerin ve şirketlerin doğmasını sağlarken bazı sektör ve firmalarında yok olmasına sebep olmuştur. Rekabeti en üst seviyeye taşıyan bilişim teknolojileri işletmelere bazı avantajlar sağlarken bazı tehdit unsurlarını da beraberinde getirmektedir. Bu tehditlerden en önemlisi siber tehditlerdir. Özellikle üretim ve hizmet sektörlerinde faaliyet gösteren organizasyonlar bu tür tehditlerle sıklıkla karşılaşmaktadırlar.

Tehditlerden korunmak için işletmeler güvenlik politikalarını gözden geçirmeli yaşayan bir organizma gibi canlı tutmalıdırlar. Yapılan araştırmalar tehdit çeşitlerinin ve türlerinin yıllara göre farklılaştığını ortaya koymaktadır. 2014 yılı için web sitelerine yapılan saldırı türlerinin %50'sinin çok farklı saldırı araçlarından oluştuğu rapor edilmektedir. Başka bir araştırmada ise son yıllarda işletmelere büyük sıkıntılar yaşatan fidye yazılımlarında Türkiye 2013 ve 2014 yıllarında bu tehdite en çok maruz kalan ülkeler sıralamasında ilk onda yer almaktadır. Araştırmalardan elde edilen sonuçlara göre işletmelerin güvenlik problemlerine karşı yeni sistemler ve çözümler getirmesi zorunluluk haline gelmiştir. Eğer gerekli tedbirler alınmaz ise işletmeler prestij kaybından, maddi ve manevi zararlara kadar hatta işletmenin batmasına sebep olabilecek bir sürece gidebilirler.

Siber saldırıların düzenlenme nedenlerine bakıldığında, politik ve ideolojik sebeplerin en üst sırada yer aldığı ve genel amacın karşı tarafın bilgilerini ele geçirmek veya sistem çalışmasına zarar vermek olduğu görülmektedir. Siber saldırıların etkisini azaltmak veya hasar görmeden kurtulabilmek için organizasyonların önleyici, tespit edici ve müdahale edip önlem alıcı yetkinliklerini kurumsal iş süreçleriyle bütünleştirmesi gerekmektedir. Ayrıca şirket çalışanlarının bilinç düzeylerini artıracak gerekli çalışmaların belirli periyodlarla yapılması gerekmektedir.

Araştırmalar siber saldırılardan dolayı oluşan maddi kayıpların arttığını ortaya koymaktadır. 2014 yılı içerisinde işletmelerin siber saldırılardan dolayı uğradığı zararın 260 milyar dolar civarında olduğu, bireysel kayıplarla beraber 400 milyar doların üzerine çıktığı tahmin edilmektedir. Saldırıların işletmelere vermiş olduğu zararın azaltılması ve siber saldırılardan korunmak için alınabilecek tedbirleri içten ve dıştan gelen tehditler olmak üzere iki boyutta incelenebilir. İçeriden gelebilecek tehditleri engelleyebilmek için kişi yetkilendirmesi çok iyi tasarlanmalı ve şirket çalışanlarının dijital verileri sürekli kontrol altında tutulmalıdır. Dışarıdan gelen tehditler için ise firewall (ateş duvarı) ve Proxy sunucular gibi çeşitli donanımsal ve yazılımsal yapılar sisteme kurulmalı ve yazılım güncellemeleri aksatılmadan yapılmalıdır.

KAYNAKÇA

Altundal, Ö.F. (2014). Siber Güvenlik Raporu'14, http://www.siberguvenlik.org.tr/2015/01/2014-Siber-Guvenlik-Raporu-Yayinlandi.html.

Arbor Network (2015). 2014 Infrastructure Security Survey.

Atalay, A. H. (2014). Siber Güvenlik ve Siber Suçlar. Erişim Tarihi: 08.04.2015. http://www.slideshare.net/ahatalay/sber-gvenlk-ve-sber-sularahaaralk2014-43135183.

BThaber, (2014). Siber Saldırılar. Erişim Tarihi: 22.12.2014. http://www.bthaber.com/turkiye-siber-saldirilarin-odaginda-yer-aliyor.

Can, Ö., Akbaş, M.F. (2014). Kurumsal Ağ ve Sistem Güvenliği Politikalarının Önemi Ve Bir Durum Çalışması. TÜBAV Bilim Dergisi, 7(2): 16-31.

Combe, C. (2006). Introduction To E-Business: Management and Strategy. Oxford: Elsevier, UK.

Cyren, (2015). 2015 Cyberthreat Yearbook, Erişim Tarihi: 12.07.2015. https://www.cyren.com/tl_files/downloads/CYREN_2015_CyberThreat_Yearbook.pdf.

Çağlar, O. (2010), Yönetim Bilgi Sistemi. Erişim Tarihi: 22.06.2015. http://notoku.com/elektronik-isletme-e-isletme/.

Damanpour, F. (2001). E-business e-commerce evolution: Perspective and strategy. Managerial Finance, 27(7): 16-33.

Durumeric, Z., Kasten, J., Adrian, D., Halderman, J. A., Bailey, M., Li, F., Paxson, V. (2014). The matter of Heartbleed. IMC'14 Proceedings of the 2014 Conference on Internet Measurement Conference: 475-488.

E-Marketer (2014). Global B2C Ecommerce Sales to Hit $1,5 Trillion This Year Driven by Growth in Emerging Markets, http://www.emarketer.com/Article/Global-B2C-Ecommerce-Sales-Hit-15-Trillion-This- Year-Driven-by-Growth-Emerging-Markets/1010575.

Enigmasoftware, (2014). http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/ Erişim Tarihi: 14.08.2015.

Freier A., Karlton P., KocherP. (2011). The Secure Sockets Layer (SSL) Protocol Version 3.0, Internet Engineering Task Force (IETF), https://tools.ietf.org/html/rfc6101.

Golchha, P., Deshmukh, R., Lunia, P. (2015). A Review on Network Security Threats and Solutions. International Journal of Scientific Engineering and Research, 3(4): 21-24.

Gücüyener, A. (2015). Kritik Enerji Altyapılarına Yapılan Saldırılara İlişkin Bir Değerlendirme. Uluslararası Kritik Enerji Altyapı Güvenliği: Yeni Tehditler ve Fırsatlar, Hazar Strateji Enstitüsü.

Kara, M. (2013). Siber Saldırılar-Siber Savaşlar ve Etkileri. İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Programı

Karabacak, S. (2008). Güçlü Marka Konumlandırmasında Bilişim Sistemlerinin Rolü ve Bir E-İşletmecilik Örneği. Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı, Sayısal Yöntemler ve Yönetim Bilimi Programı, Yüksek Lisans Tezi, İzmir.

Kaspersky, (2014). http://www.kaspersky.com/tr/about/news/virus/2014/Kaspersky_Lab_Avrupa_daki_Siber_Guvenlik_Trendlerini_ve_Tehdit_Ortamini_Acikladi, Erişim Tarihi: 09.12.2014.

Kovacich, G. (1998). Electronic-Internet Business and Security, Computers & Security, 17(2): 129-135.

Lin, S.C., Tseng, S.S. (2004). Constructing Detection Knowledge for DDoS Intrusion Tolerance, Expert Systems with Applications, 27(3): 379–390.

McAfee, (2014). Net Losses: Estimating the Global Cost of Cybercrime, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf. (Erişim Tarihi:12.06.2015)

McAfee, (2014). Threats Report, November.

NetDiligence, (2014). Cyber Claims Study, http://www.netdiligence.com/files/NetDiligence_2014%20Cyber%20Claims%20Study.pdf

OECD (1997). Erişim Tarihi: 14.05.2004.

http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=OCDE/GD(97)185&docLanguage=En,.

O'Brien, J., Marakas, G. (2008). Management Information Systems. 8th ed. Boston: Mc.Graw-Hill Irwin, USA.

Özmen, Ş. (2013). Ağ Ekonomisinde Yeni Ticaret Yolu: E-Ticaret, İstanbul Bilgi Üniversitesi Yayınları, İstanbul.

Paypal, (2014). https://www.paypal.com.au/lead_gen/SpiceRoutes.

Pwc, (2014). Managing Cyber Risks in an Interconnected World, The Global State of Information Security Survey 2015.

Siberbülten, (2015), Siber Güvenlik Harcamaları 170 milyar $ Olacak, En Hızlı G. Amerika Büyüyecek!, Erişim Tarihi: 18.07.2015. http://siberbulten.com/sektorel,

Sevim, A., Gül, M. (2012). Elektronik İşletmelerde (E-İşletmelerde) Satın Alma İşlemleri ve İç Kontrol İlişkisi, Afyon Kocatepe Üniversitesi, İİBF Dergisi 14(2): 91-118.

Sınav, A., (2014), Siber Suçlar ve Kurum Güvenliği, Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Denizcilik Uzmanlık Tezi.

Symantec (2013). Internet Security Threat Report, Symantec Corporation, February 28, 2013.

Symantec (2014). İnternet Güvenlik Tehdidi Raporu.

Symantec (2015). 2015 Internet Security Thereat Report Volume 20. https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf

The Wall Street Journal (2014). Global Security Spending to Grow 7.9% in 2014, Gartner Says, August 22.

Trend Micro (2015), Magnified Losses, Amplified Need for Cyber-Attack Preparedness, TrendLabs 2014 Annual Security Roundop.

Turktrust (2014). http://www.turktrust.com.tr/tr/urunler/e-imza/.

UITSEC, (2015). 2014 Güvenlik Tehditleri ve 2015 Tahminleri. https://www.uitsec.com/tr/kaynaklar%C4%B1m%C4%B1z/ makaleler-hizmetlerimiz/2014-guvenlik-tehditleri-ve-2015-tahminleri.