CBÜ SOSYAL BİLİMLER DERGİSİ **Cilt:13, Sayı:2, Haziran 2015**

Geliş Tarihi: 28.01.2015 **Doi Number:** 10.18026/cbusos.40441 **Kabul Tarihi:** 01.06.2015

FİNANSAL HİZMET SEKTÖRÜNDE SİBER GÜVENLİK RİSKLERİ VE ÇÖZÜM YOLLARI: ÖDEME SİSTEMLERİ VE TEDARİK ZİNCİRİ BÜTÜNLÜĞÜ*

Hamdi YEŞİLYURT[1]

ÖZ

Türkiye kötücül yazılım kaynaklı siber güvenlik tehditlerine maruz kalma açısından dünya sıralamalarında en üst sıralarda olmaya devam etmektedir. Türkiye'de birçok akademik çalışmada siber güvenlikle ilgili siber suçların işleniş tarzı ya da hukuki boyutu incelenmiştir. Bununla beraber, bu hususların ötesinde siber güvenlik problemlerine neden olan risk faktörleri ve bu faktörlerin nedenleri yeterince incelenmelidir. İnternet bankacılığı, banka ve kredi kartları kullanımı ve e-ticaret finansal siber güvenlik sisteminin korunması gereken en önemli bileşenleridir. Yazılım tedarik sistemi ise finansal sistem güvenliğini oluşturan en önemli teknik altyapı unsurlarındandır. Artan siber riskler tüketici güveninin azalmasına, vatandaşların finans sistemini internet aracılığıyla daha az kullanmasına ve finans sistemlerinin beklenmeyen giderlerinin artmasına neden olacaktır. Bu nedenle siber güvenlik risklerinin ulusal bazda incelenmesi ve yorumlanması ülke ekonomisi ve siber kritik altyapı güvenliği açısından hayati öneme sahiptir. Bu çalışmada Türkiye'de çevrimiçi ödeme sistemleri ve bu sistemin siber güvenliğini destekleyen yazılım tedarik zincirlerinin barındırdıkları riskler incelenmiştir. Çalışmada, bahse konu potansiyel riskler siber güvenlik normları kapsamında tanımlanmakta ve siber güvenlik önlemleri yönetimsel açıdan tartışılmaktadır.

Anahtar Kelimeler: *Siber Güvenlik, Bankacılık, Finans, İnternet Bankacılığı, Yazılım Tedarik Zinciri, 3-D Secure, Güvenli Elektronik İşlem.*

CYBER SECURITY RISKS AND SOLUTIONS IN THE FINANCIAL SERVICES SECTOR: PAYMENT SYSTEMS AND SUPPLY CHAIN INTEGRITY

ABSTRACT

Turkey continues to be statistically in the forefront of the world rankings in terms of the exposure to cyber security threats. In Turkey, many academic studies related to cyber security or legal issues in regard to cyber-crime have been conducted to date. Further, the risk factors that lead to cyber security problems and the causes of these factors should be examined more

---

* Bu makale daha önce yayımlanmamıştır.

[1]Dr., Emniyet Genel Müdürlüğü/Ankara, hamdiyesilyurt@gmail.com.

rigorously. Internet banking, debit and credit card uses and e-commerce are the key components of the online payment system that suffer intrusions. Software supply system is also one of the most important technical infrastructure elements of the financial system security. Increasing cyber risks diminish consumer confidence regarding online payment systems, and such risks could cause extraordinary expenditures within financial system. Therefore, a nationwide analysis and interpretation of the cyber security risks is vital for national economy and cyber critical infrastructure security. In this study, online payment systems in Turkey and the appertaining cyber security systems that are supported by software supply chains are examined in terms of the associated risks. The study addresses the aforementioned potential cyber security risks in the context of cyber security norms and cyber security measures are discussed from an administrative perspective.

Keywords: *National Cyber Security, Banking, Finance, Internet Banking, Software, Supply Chain, 3-D Secure, Secure Electronic Transaction.*

I. Giriş

Bankalar, sigorta şirketleri, emeklilik fonları, hisse senedi, tahvil piyasaları ve benzeri kuruluşlar finans sektörünün başlıca unsurlarıdırlar. Bankacılık sektörü ise finansal aracılık hizmetlerini yerine getiren en önemli unsurdur(Coşkun ve diğerleri, 2012). Ülkemizde ve dünyada bankacılık sektörü mevduat ve kalkınma gibi birçok alanda kamu kurumlarına ve halka internet üzerinde interaktif bir biçimde 7/24 hizmet sunmaktadır. Bankacılık yalnızca kendisine ait ya da vatandaşlara ait değil, kamu kurum ve kuruluşlarına ait gizli içerikli ya da kişisel bilgileri(Müşteri ve kurum bilgileri gibi) ve işlem bilgilerini bilişim sistemleri aracılığıyla barındırmaktadır.

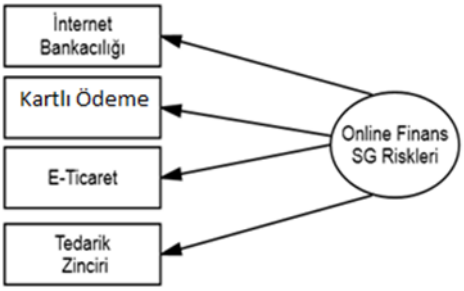
2013 yılı Ocak-Mart TÜİK (Türkiye İstatistik Kurumu) verilerine göre Türkiye'de 16-74 yaş arası bireylerin %39,5'i interneti düzenli olarak kullanmıştır. Şahısların internet aracılığı ile mal veya hizmet alım ya da satımı gerçekleştirme oranı ise %24,1'dir ve bir önceki yıla göre %3'e yakın bir artış gözlemlenmiştir(TÜİK, 2013). Ülkemizdeki internet kullanıcı sayısının giderek artması, ürün ve hizmetlerin pazarlama ve alımının internet üzerinden yapılmasında artışa neden olmuştur. İnternetin finans sektörünce kullanımının artmasında nedensel olarak, banka ve hizmet kuruluşları açısından maliyetlerin azaltılması ve hizmet kalitesinin artırımı yatmaktadır (Şıker, 2011). Özel sektör içerisinde en geniş bilişim ağlarına ve kişisel bilgilere sahip sektör internet bankacılığı ve e-ticaret odaklı organizasyonlardır. Bu şirketler yoğunluklu olarak dış kaynaklı yazılım ve donanımları kullanarak siber güvenlik altyapılarını korunaklı hale getirmektedirler. Günümüzde birçok ödeme işlemi(bankacılık ve ticaretle ilgili) elektronik ödemelerle(E-ödeme) gerçekleştirilmektedir.

E-ödeme elektronik olarak başlatılan, süreçlendirilen ve elektronik olarak alınan ödemelerdir. Elektronik ödeme elektronik ticaret işlemleri(Şirketlerden Müşteriye, B2C) ya da müşteriler arası(B2B) elektronik ödemeler olarak gerçekleşir(Raja ve Velmurgan, 2008). Çoğunlukla bankacılık ya da e-ticaret uygulamaları için gerçekleştirilen e-ödemeler, önceleri bilgisayarlar aracılığı ile başlatılmış, günümüzde ise cep telefonları ve diğer mobil araçlar aracılığı ile de yaygın şekilde yapılabilmektedir. Elektronik ödeme sistemlerinin siber güvenlik konsepti ile birlikte analiz edilmesi gereklidir. Zira, siber güvenlik açısından en önemli korunması gereken bileşenlerin arasında internet dünyasına oldukça açık bir şekilde hizmet veren elektronik finans sektörü gelmektedir. Dan ve Howard(2006) e-ödemelerde bilişim altyapısı güvenliğinin finans sektörü için dünya çapında önemli bir problem olduğunu belirtmiştir. Son yirmi yılda finansal değerler online bankacılık sistemi tarafından kontrol edilmeye başlanmıştır. Suçlular artık banka soygunu ile kendilerini riske atmak yerine, sandalyelerinde otururak banka soygunları gerçekleştirmektedir(Yesilyurt, 2011).

Bu çalışmada elektronik ödemeler BİT (Bilgi ve İletişim Teknolojileri) kapsamında değerlendirilmiştir. BİT'e dair sistemlerin bütünlüğü ve güvenilirliği gibi hususlar ülkelerin finansal refahı ve güvenliği için giderek daha önemli hale gelmektedir. Hükümetler dünya çapında BİT ürünleri için global tedarik zinciri yoluyla BİT sistemlerine karşı tehditlerin artmasından artan şekilde endişe duymaktadırlar. Bu endişelerin temel nedeni olarak bir ürünün geliştirilmesi, üretimi ya da dağıtımı esnasında ürüne yönelik bir siber saldırının gerçekleşmiş olması ihtimali yatmaktadır(Microsoft, 2014). Ülkemizdeki elektronik finans sistemlerinin yazılım ve donanımlarının çoğunlukla yabancı kaynaklı olduğu varsayılırsa, dağıtım aşamasına kadar hiçbir ulusal denetimden geçmeyen siber güvenlik ürünlerinin yazılım ve donanım tedarik zincirlerinin ödeme sistemleri riskleri ile birlikte değerlendirilmesi faydalı olacaktır.

Siber güvenlik sistemleri içerisindeki güvenlik zafiyetleri nedeniyle sanal ve fiziksel alanda finansal sistemler çok kereler zarara uğramakta, ulusal ve bireysel güvenlik zafiyete uğratılmaktadır(Yesilyurt, 2015). Bu araştırma finans sektörünün yaşayabileceği siber güvenlik risklerini analiz etmektedir. Siber güvenlik riskleri Çalışmada internet tabanlı birçok hizmeti yerine getiren finans sektörünün ve bu sektörün internet üzerinde sağlıklı olarak ayakta kalması sağlayan yazılım ve donanım içerikli tedarik zincirinin ülkemiz açısından mevcut durumu değerlendirilmiş ve bu değerlendirmeler çerçevesinde mevcut riskler ve çözüm yöntemleri temel bazda ortaya konulmuştur. Araştırma elektronik finans sistemi

olarak ödeme sistemlerini(kartlı ve kartsız online bankacılık ve e-ticaret) ve elektronik finans sisteminin güvenliğinin temel taşı olan tedarik zincirlerini ulusal siber güvenlik riskleri açısından incelemiştir. Mevcut araştırmada online(çevrimiçi) finans sistemi siber güvenlik risklerini etkileyen unsurlarla ilgili konseptler Şekil 1'de ifade edilmiştir.



Şekil 1. Elektronik Finans Sistemi Siber Güvenlik Riskleri

II. Elektronik Finans Sistemi Temel Bileşenleri

A. İnternet Bankacılığı

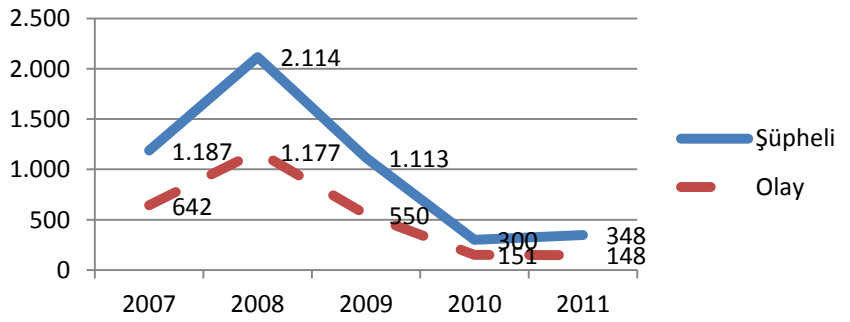
İletişim ve programlamaya bağlı ağ bilgi sistemi altyapısı insanlık tarihinin en büyük inşa projesidir. Bilgi ve iletişim teknolojileri(BİT) açısından bugün bulunduğumuz durum mihenk noktasıdır. BİT altyapısı daha modüler ve daha güçlü ağlarla tüm dünyayı sarmaktadır (Cowhey ve Aronson, 2009). BİT altyapısına dayalı internet bankacılığı sistemi banka işlemlerine kolay erişim sağlar. Kullanıcı ve banka arasındaki iletişim ATM'ler, telefon bankacılığı, internet bankacılığı ve mobil bankacılık sayesinde oldukça gelişmiştir. Bu bankacılık aktivitelerinden bazıları; hesap miktarı, kullanıcılar arasında para transferi veya hesap bakiyesi erişimi gibi hizmetlerdir(Claessens, Dem, De Cock, Preneel ve Vandewalle, 2002). İnternet Bankacılığı(İB) hızlıdır ve herhangi bir lokasyon ile sınırlı değildir. Bankalar, IB sayesinde oldukça düşük maliyetlerle bankacılık hizmetlerini verimli hale getirirler. Örneğin, tipik bir banka müşterisi banka şubesine gittiğinde kendisine harcanan masraf 1 dolar, telefonla 0.60 cent ve online olarak yalnızca 0,02 centtir(Nsouli ve Schaechter, 2002). BİT altyapısı sayesinde günlük hayatımızdaki birçok finansal aktivite sanal ağlar üzerinden uzaktan erişimle sağlanır ve sonuç olarak finans hizmetleri daha büyük çapta, aralıksız ve düşük maliyetlerle gerçekleştirilir.

Araştırmalar internet bankacılığı açısından algılanan yararlılık, müşteri güveni ve devlet desteğinin İB'ye pozitif olarak etki ettiğini savunmuşlardır (Ooi, Chong, Lin ve Tan, 2010). Web sitesi güvenliği, kişiye özellik, kullanılabilirlik gibi hususlar da müşterilerin

İB'ye olan güvenini pozitif olarak etkilemektedir (Casalo´, Flavia´n ve Guinalıu, 2007). Oysa yapılan araştırmalar bankaların yeterli güvenlik önlemlerini almadıklarını ve siber güvenlik gelişimleri açısından daha yeni fırsatların kullanılması gerekliliğini ortaya koymştur. Yeterli güvenlik önlemlerinin alınmadığı durumlarda, bankalar daha büyük maliyetler ve müşteri güveni kayıplarıyla karşı karşıya kalırlar (Dan ve Howard, 2006).

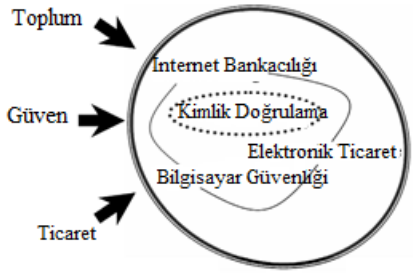
İnternet bankacılığı 1980'lerden itibaren dünyada kullanılmaya başlanılmıştır. Ancak, 2004 yılına kadar internet bankacılığı dolandırıcılıklarında ciddi bir artış görülmemiştir. Bu nedenle, bu tip saldırıların artışı son on yılda hissedilmiş denilebilir. İnternet bankacılık sisteminin gelişmiş olması ve dünya çapında giderek artan bir şekilde kullanılıyor olması bu sistemin suçlular için özel bir hedef olmasına neden olmuştur (Paganin, 2013). Yaygın internet kullanımı ve karmaşık internet bankacılığı platformları, bilgisayar korsanları açısından karlı ve geniş bir saldırı alanı meydana gelmesine sebep olmuştur. Artan hedef büyüklüğü ile birlikte siber güvenlik teknolojilerinin de geniş bir yelpazeye yayılması internet bankacılığı risklerini önemli ölçüde azaltamamıştır.

Şekil 2'de ülkemizdeki İnternet Banka Dolandırıcılığı Olay ve Şüpheli Sayıları yıllara göre görülebilir. 2008 yılındaki dikkate değer artışın ardından, 2010 yılında bu tür dolandırıcılık olayları önemli ölçüde düşmüştür. Kaçakçılık ve Organize Suçlarla Mücadele(2012) raporuna göre 2010 yılında meydana gelen düşüşlerin nedeni kamuoyu ve kullanıcıların yapılan çalışmalarla daha fazla bilinçlendirilmiş olmasıdır. 2010 yılında dolandırıcılık olaylarında meydana gelen düşüşün sebepleri daha derinlemesine araştırılmalıdır. Her ne kadar 2010 yılında ciddi bir düşüş yaşansa da önceki yıllar internet banka dolandırıcılığı açısından önemli bir potansiyelin de varlığını ortaya koymuştur.



Şekil 2. İnternet Banka Dolandırıcılığı Olay ve Şüpheli Sayıları (KOM Daire Başkanlığı)

Güven seviyesi ve internet bankacılığı'nın müşteriler tarafından benimsenmesi arasında ilişkisel bir bağlantı olduğu kabul edilmektedir (Kumar, Sareen ve Barquissau, 2012). Hutchinson ve Warren'e (2003) göre internet bankacılığı açısından önemli üç dış etkenden biri de güvendir(Şekil 3). Bankacılık sektöründe vatandaşın sektöre olan gerek finansal yapısı açısından güveni ve gerekse internet bankacılığı işlemleri açısından güveni bankacılık hizmetlerinin yürütülmesi ve devam edebilirliği açısından oldukça mühimdir. Toplumun neredeyse bütün mevduatının uzunca bir süre bankalarda saklandığı, yasal ve fiziksel güvence altına alındığı bilinmektedir. Ancak, internet bankacılığı parasal aktivitelerin sanal ortamlarda üçüncü kişiler tarafından takibi ve kişisel verilerin istenmeyen şahıslarca ele geçmesi ihtimalini güçlendirmektedir.



Şekil 3. İnternet Bankacılığı Güvenlik Elementleri (Hutchinson ve Warren, 2003).

Siber güvenlik prensiplerine göre yalnızca doğrulanan kullanıcılar gizli ve özel bilgilere ulaşabilirler. Doğrulama sistemlerine karşı ataklar iki ana parçaya ayrılırlar: a) kullanıcı bilgilerinin zararlı bir yazılım aracılığı ile ele geçirilmesi, b) "adam ortada" atakları gibi çevrimiçi kanal bağlantı kesimi atakları, sofistike saldırılara sahne olurlar. İkinci saldırı tipinde, kullanıcı bilgilerini elde etmek yerine, bilgisayar ve banka sunucusunun iletişimi fark ettirilmeden dinlenir. Saldırgan kendisini sunucuya istemciymiş gibi, istemciye ise sunucuymuş gibi gösterir (Hiltgen, Kramp ve Weigold, 2006).

E-ödeme sistemlerinin en önemli özelliklerinden biri karmaşıklıklarıdır. E-ödemeler tek bir işlem ya da metotla gerçekleşmezler. Dolaysıyla, bu sistemlere karşı yapılan saldırılar oldukça geniş çaplıdır. Siber güvenlik sistemleri ne kadar ileri düzeyde olursa olsun, yeni ve daha kompleks güvenlik önlemlerinin güvenlik açıklarının kapatılması amacıyla oluşturulması gerekir (Dzemydienė, Naujikienė, Kalinauskas ve Jasiūnas, 2010). İnternet bankacılığı bilgilerini elde etme ve yasadışı kazanç sağlama amaçlı birçok eylem şekli gelişmiştir ancak son yıllarda artan siber güvenlik tedbirlerine

karşın suçlular da daha karmaşık ve kendileri açısından güvenli yöntemler geliştirmektedirler. Bu yöntemler arasında Oltalama(Phishing), Yalak (Watering hole), Pharming ve Kredi Kartı Yeniden Yönlendirme (Credit Card Redirection), Kötücül Yazılım Tabanlı Ataklar ve Adam Web Tarayıcısında (Man In The Browser) ataklar sayılmaktadır (Kharouni, 2012) .

SpyEye ve ZeuS kötücül yazılımlarının varyasyonu olan WebInject dosyaları, kullanıcıların bankacılık bilgileri, web e-posta servisi ve diğer finansal servis bilgilerini(Örn: PayPal Hesapları) çalmakta kullanılırlar. Siber suçlular hedef kullanıcının bilgilerini elde etmek için WebInject dosyaları gibi pop-up pencereler kullanmak yerine, ATS'ler(Otomatik Transfer Sistemleri) gibi görünmez nesneler kullanmaya başlamışlardır. ATS'ler pop-up penceresi kullanmadan hesap bakiyesi kontrolü yaparlar ve sistem uyarısına neden olmadan para transferini çevrimiçi hesaplar üzerinden gerçekleştirirler. Gerçekleştirilen bu transfer bilgileri de kullanıcılardan saklanır. ATS'ler sistemde kaldıkları müddetçe, kullanıcılar hesaplarından yapılan illegal transferlerden haberdar olmazlar(Kharouni, 2012). ATS'lerin internet banka dolandırıcılığına etkisi, birçok banka ve müşterilerini zor durumda bırakacak düzeydedir. Olayın işleniş tarzı veya işlenişinin geç öğrenilmesi, siber suç soruşturmalarının verimini azaltıcı niteliktedir.

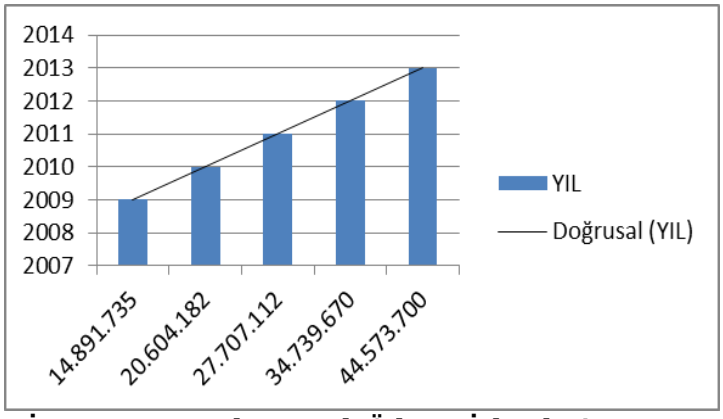
B. Banka ve Kredi Kartları(Kartlı Ödeme Sistemleri)

Kartlı ödeme sistemleri Türkiye'de ilk defa 1968 yılında faaliyete geçmiştir. Tablo 1'de de görüldüğü gibi, Bankalararası Kart Merkezi (BKM) verilerine göre 2014 Ocak ayı sonunda Türkiye'de 56,8 milyon adet kredi kartı ve 100,9 milyon adet banka kartı olmak üzere toplamda 157,7 milyon adet kart mevcuttur (BMK, 2014). Bankalararası Kart Merkezi (BKM) ve Avrupa Merkez Bankası (ECB) 2012 yılı verilerine göre Türkiye banka ve kredi kartı kullanımında İngiltere'den sonra 2. sırada yer almaktadır(Sabah, 2014). Dolaysıyla, banka ve kredi kartı kullanımının Türk toplumunda oldukça yaygın olduğu söylenebilir.

Tablo 1. Banka Kartı ve Kredi Kartı Sayıları Gelişimi (Milyon Adet)

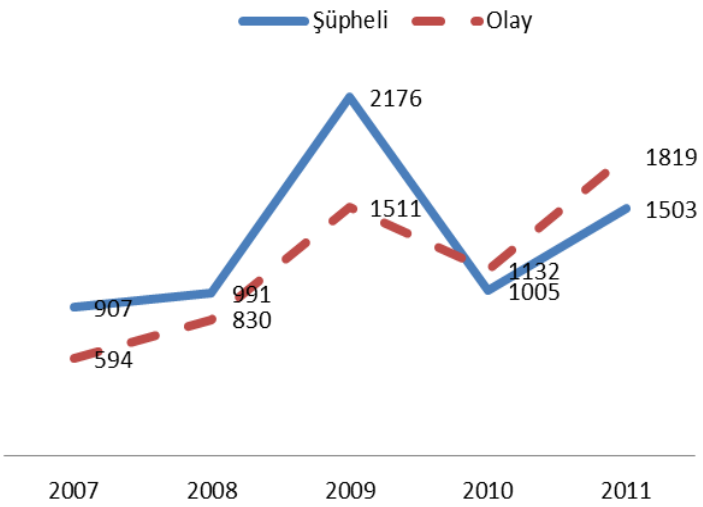
Kart Adetleri (Milyon Adet)	2013 Ocak	2014 Ocak	Değişim
Banka Kartı	91,9	100,9	10%
Kredi Kartı	54,7	56,8	4%
Toplam	146,6	157,7	8%

Şekil 4'e göre internette yapılan kartlı ödeme işlemleri kapsamında yerli ve yabancı kartların yurt içi kullanımının her yıl %38(2010) ile %28(2013) arasında artış gösterdiği görülmektedir. İnternette yapılan yurtiçi kartlı ödeme miktarı 2009 yılında 14,891,795 iken 2013 yılında aynı dönemde 44,573,700 olarak gerçekleşmiştir. Bu artış hızının internet bankacılığı dolandırıcılarının iştahını kabartacağı öngörülebilir. Artış hızları araştırılırken 3. dönem(yaz ayları) kart kullanımları esas alınmıştır. 3. dönem, internette yapılan kartlı ödeme işlemlerinin ülkemizde en yoğun olduğu dönemdir.



Şekil 4. İnternette Yapılan Kartlı Ödeme İşlemleri Kapsamında Yerli ve Yabancı Kartların 3. Dönem Yurt İçi Kullanımı
Kaynak: BKM (2014)

Kredi kartı dolandırıcıları; kredi kartları üzerinde depolanmış olan verileri ele geçirmek amacıyla, işyerleri ve ATM cihazlarına çeşitli aparatlar yerleştirmek suretiyle kartlar üzerindeki bilgileri elde etmekte ve yasadışı yollardan harcama yapmaktadırlar (KOM, 2012). Şekil 5'de 2007-2009 yılları arasında banka ve kredi kartı dolandırıcılığı sayısında oldukça yüksek bir artış olduğu gözlemlenmektedir. Özellikle 2008 ve 2009 yılları arasındaki önemli yükselişe bakıldığında 2009 yılında şüpheli ve olay sayısında sıra dışı bir artış olduğu gözlemlenmektedir. 2009 yılında ülkemizde(%-4,8) ve dünyadaki ekonomik büyümenin negatif yönde değişmesi ile banka ve kredi kartı dolandırıcılığındaki artış arasında nedensel bir bağlantı olabilme ihtimali mevcuttur. 2010 yılında ise artan olay ve şüpheli sayısının yerini önemli ölçüde düşüş takip etmektedir.



Şekil 5. Banka ve Kredi Kartı Dolandırıcılığı Olay ve Şüpheli Sayıları (KOM Daire Başkanlığı, 2012)

C. E-ticaret

E-ticaret, "mal ve hizmetlerin internet üzerinden alım-satımı" olarak tanımlanmaktadır. Ancak, e-ticaret daha başka birçok aktiviteyi de kapsamaktadır. Bunlardan başlıcaları şirketlerin birbirleriyle olan ticareti, firmaların satın alma, kiralama, satış işlemleri ve diğerleridir. Dünyada esasen 1990'larda elektronik ticaret iş hacmi açısından yeni bir yol olarak ortaya çıkmaya devam ediyordu. 90'larda Amazon.com ve eBay büyük kar elde eden müzayede siteleri olarak yerlerini almıştı. AltaVista, HotBot, Lycos ve Yahoo gibi arama motorları ise başka bir arama motoru tarafından önlerine geçilmesi zor yerleşik araçlar olarak kabul edilmekteydi. Sonraları Google'ın arama sonuçlarındaki tutarlılık ve başarısı e-ticaret açısından reklam gelirlerinin artmasına yol açtı(Schneider, 2010). E-ticaret Türkiye'de 90'lı yılların sonuna doğru ortaya çıkmış, bugünse birçok vatandaş tarafından benimsenmiştir. Hepsiburda.com, sahibinden.com, Teknosa, Markofoni, Migros(Sanal Market) ve benzeri birçok alışveriş sitesi farklı segmentlerde günlük hayatımızda önemli bir yer tutmaktadır.

Dünya İnternet İstatistiklerine göre Türkiye internet kullanımında 2012 yılı verilerine göre Avrupa'da beşinci sırada bulunmaktadır. Avrupa e-ticaret alışveriş verilerine göre en önde gelen ülke Norveç ve İngiltere olmakla beraber Türkiye ise listenin sonlarında yer almıştır (Internet World Statistics, 2012). Bu veri ülkemizin önemli bir ekonomik ve teknolojik imkândan yeterince yararlanamadığını ortaya koymaktadır. E-ticaret'in ülkemizde

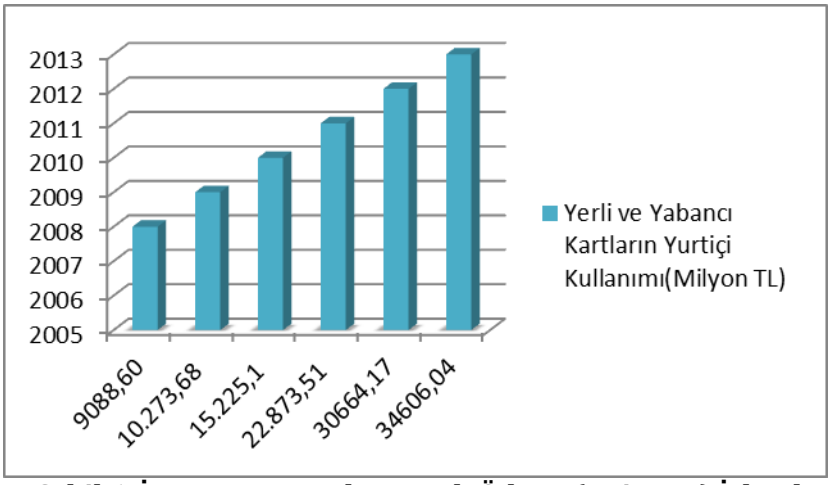
ekonomik açıdan yeterince ilerlememiş olmasının nedenleri siber güvenlik perspektifinde farklı açılardan incelenmelidir. E-ticarete olan ilginin nispi olarak düşüklüğü vatandaşın e-ticarete olan güveninin düşük olmasıyla ilgili olabilir. Zira, banka ve kredi kartı kullanımı hususunda herhangi bir negatiflik yaşanmazken, bu husus e-ticaret açısından tam tersidir.

Suh ve Han'a (2003) göre özellikle e-ticaret alanında müşterilerin özel veya gizli bilgilerini paylaşmaktan çekindikleri bilinen bir sorundur. Suh ve Han, güvenlik kontrolleri üzerindeki algısının e-ticaret benimsemesi üzerindeki etkisini 502 kişi üzerinde internet üzerinden bir anket düzenleyerek incelemiştir. İstatistiki analize göre müşterilerin inkâr edememe(nonrepudiation), gizli bilgilerin korunması(privacy protection) ve veri bütünlüğü(integrity) gibi siber güvenlik konseptleriyle ilgili algılarının e-ticarete olan güvene önemli derecede etki ettiği bulunmuştur. Çalışma neticesinde, güvenin e-ticaretin benimsenmesinde de oldukça önemli bir etkiye sahip olduğu ortaya çıkmıştır.

E-ticaretin başarılı şekilde uygulanması açısından bütün finansal sistemlerin üzerinde durması gereken en önemli hususlar para ve materyal akışının sağlanması ve e-ticaret süreci içerisinde bilgi akışının da sağlanmasıdır(Tsiakis ve Sthephanides, 2005). Güven teorilerinin çoğunluğu iş ortakları arasında değiş tokuşların var olduğu üzerine kuruludur. Ancak, e-ticaret paydaşlar arasındaki kırılgan yapıdan dolayı güven ilişkisinin oldukça zorlanıldığı bir alandır (Tsiakis ve Sthephanides, 2005). Pavlou'a (2003) göre e-ticaret üzerindeki belirsizlikler yüzünden güven ve risk bilimsel açıdan değerlendirilmelidir. Pavlou 103 öğrenci ve 155 çevrimiçi müşteri üzerinde yapmış olduğu anket çalışmasında güven ve risk algısının e-ticaret açısından önemli olduklarını ortaya koymuştur. Pavlou'ya göre müşterilerin yalnızca internet güvenliği ve teknolojilerine olan güveni yeterli değildir. E-ticaret aktörlerine olan siber güvenlik algısıda e-ticaretin benimsenmesi açısından yüksek öneme haizdir.

David Bollier (2004), ticaretin internet üzerindeki farklılıkları ve internete dayalı ticaretin kişiselleştirmesinin getirdiği özellikleri ikiye ayırmıştır. Bollier'e göre çekici ekonomi, müşteri taleplerinin tahmini ve kaynakların doğru yerde, doğru zamanda, doğru kişilere ulaştırılmasıdır. İtici ekonomi ise, internet ortamında çoğunlukla görülen, açık ve esnek üretim platformlarına dayalı bir ekonomik anlayıştır. Bu anlayış çerçevesinde geniş yelpazedeki kaynaklar bilişim ağları kullanılarak, kişiye özel nitelikteki ürünler kısa zamanda hazırlanarak müşterilere ulaştırılır. Dolaysıyla kişisel özellikli ihtiyaçlar toplu üretim mantalitesinin önüne geçmektedir. Günümüz

internet dünyasında Bollier'in savını en iyi destekleyecek ve değerlendirecek sistem ise e-ticaret yordamıdır. BKM (2014) verilerine göre e-ticaret işlemlerinde 2008 yılından itibaren düzenli bir artış olduğu aşikârdır(Şekil 6). Artan e-ticaret hacmi artan siber güvenlik riski olarak kaşımıza çıkabilecektir. Bu artışın nedensel olarak yükselen internet kullanımı ve teknoloji adaptasyonu ile bağlantılı olabileceği değerlendirilebilir.



Şekil 6. İnternette Yapılan Kartlı Ödeme(e-ticaret) İşlemleri
Kaynak: Bankalararası Kart Merkezi, 2014

D. Tedarik zinciri

A. Yazılım ve Donanım Üretimi

Her firma veriye sahiptir ve verilerin korunması gerekmektedir. Bu bilgiler, personel bilgileri, patent bilgisi ya da ağ'ın güvenli işletimi ile ilgili olabilir. Siber güvenlik her düzeydeki işletme için ihtiyaçtır (Reeves, 2013). Global bazda ticaret ile ağlardan oluşan bir dünya meydana gelmektedir. Ancak, ürünler yolculukları esnasında doğal, kazayla ya da kötü niyetli bir saldırı neticesinde meydana gelebilecek önemli sorunlarla karşılaşabilir (White House, 2013). Siber güvenlik firmaları gerek kamu gerekse özel sektörün güvenlik ihtiyaçlarını karşılamakta başrolü üstlenmektedir. Siber güvenlik girişimleri yalnızca geliştirdikleri güvenlik teknolojileri ile değil aynı zamanda ülke ekonomisine olan katkılarıyla da tanınmaktadır. Dünyada siber güvenlik yazılım ve teknolojileri üreten büyük çaplı şirketlerin çoğunluğunu ABD ve İsrail menşeli firmalar oluşturmaktadır.

Reeves'e (2013) göre dünya sıralamasındaki ilk beş siber güvenlik şirketi Tablo 2'de sunulmuştur.

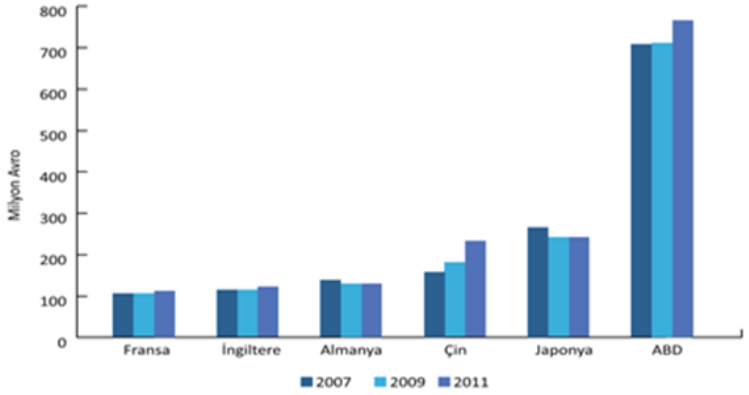
Tablo 1. Siber Güvenlik Şirketleri

Siber Güvenlik Şirketi	Siber Güvenlik Uzmanlık Alanı
Cisco (CSCO)	Ağ Cihazları ve Dijital Finans Sistemleri Koruma
Symantec (SYMC)	Antivirüs ve Ağ Güvenliği
FireEye (FEYE)	Ağ Güvenliği
Check Point (CHKP)	Ağ Güvenliği
Guidance Software (GUID)	Dijital Soruşturma

Kaynak: Reeves (2013)

Türkiye'de Bankacılık, E-ticaret ve diğer internet tabanlı finans sektörü siber güvenlik yazılım tedariklerini çoğunlukla dış ülkelerden elde ederek gerçekleştirmektedir. Burada önemli olan; araç, gıda, ilaç ve benzeri diğer ürünlerin ithalatındaki prosedürlerin aksine, siber güvenlik yazılımları herhangi bir kontrolden geçmeden, internetten indirilmek suretiyle yurt içi temininin gerçekleştirilmesidir. Diğer konulardaki hassasiyetin siber güvenlik yazılımı tedarik zincirinde hemen hiç bir yerde uygulanmayışı siber güvenlik açısından önemli riskleri beraberinde getirmektedir.

Dünyadaki, bilgi işlem teknolojileri açısından en büyük pazara sahip olan ülkeler, başlıca ABD, Japonya ve Çin'dir(Şekil 7). 2009 ekonomik krizî ardından bilgi teknolojileri pazarındaki artışa rağmen Tablo 3'deki ülkelerle kıyaslandığında, ülkemizdeki bilgi teknolojileri pazarının dünya BİT pazarındaki oranı çok düşük bir seviyede kalmaktadır (TÜİK, 2011).



Şekil 7. Bilgi İşlem Teknolojileri(Bit) Pazarı
Kaynak: EITO raporu Including Consumer Electronics, 2010
Not: 2011 yılı verileri tahmindir.

Ulusal Siber Güvenlik Strateji Belgesi 3.1. maddesinde "Siber güvenlik gereksinimlerinin karşılanmasında yerli ürün ve hizmet kullanımı teşvik edilir, bunların geliştirilmesi için araştırma ve geliştirme projeleri desteklenir, inovasyon(yenileşim) anlayışı kabul edilir" ve ayrıca strateji belgesinin 4.6. maddesinde "kurumların bilişim sistemlerinde yerli olarak geliştirilmiş ürünleri tercih etmeleri, yerli ürünlerin mevcut olmadığı durumlarda ise güvenlik değerlendirmesi yerli olarak gerçekleştirilmiş sertifikalı ürünleri tercih etmeleri teşvik edilecektir" ifadesi yer almaktadır. Ulusal güvenlik strateji belgesi resmi olarak siber güvenlik ile ilgili yazılım ve donanımların ülke güvenliği açısından stratejik ve kritik öneme haiz olduğunu göstermektedir.

Özel sektör girişimlerinin yabancı menşeli siber güvenlik yazılım ve donanımlarını yeterli tedarik zinciri kontrolü bulunmadan ülkemizin ulusal siber güvenlik kritik altyapılarına entegre etmeleri ulusal güvenlik açısından riskler taşımaktadır. Teknik olarak analiz edildiğine bu risklerden bazıları şunlardır:

1. İthal yazılımların kaynak kodları incelenememektedir. Dolaysıyla, temin edilen ürünlerin ihtiyaçlara uygun şekilde yerel kaynaklarca geliştirilme ve ilerletilme ihtimali bulunmamaktadır. Endüstriyel bazda yabancı ülkelere yüksek miktarlarda yazılım ve donanım ücreti ödenmekte ve her yıl güncellenen yazılım, maliyetleri daha da artırmaktadır. Yüksek yazılım ücretleri sebebiyle siber güvenlik yazılımlarına daha az pay ayrılmaktadır.

2. İthal güvenlik yazılımlarının içerisinde backdoor(arka kapı) tarzı güvenlik açığı bulunan yazılımları barındırma ihtimali söz konusudur.

3. Ulusal bazda siber güvenlik girişimlerinin zayıf kalması, siber güvenlik endüstrisi gibi kar getiren bir sektörde var olamamaya neden olur.

4. Siber güvenlik yazılım ve donanımı temin edilen ülkelerle ilişkilerin gerilmesi durumunda, teknik destek ve ürün takibinin durdurulması ihtimali söz konusudur.

5. İthalatta meydana gelebilecek sektörel riskler, yazılım ve donanım ithalatında da geçerlidir.

Organizasyonlar artan bir şekilde standart yazılımlar, açık kaynak kodlu yazılımlar ya da dış kaynak kullanımını (outsourcing) tercih etmekteler. Bu tip güncel yaklaşımlar karmaşık yazılım tedarik zincirlerinin risk yönetim mantalitesine uygun düşmemektedir. Genellikle, zamanında teslim alma ve uygun fiyatlar daha fazla dikkat çekmekte, fakat en önemli riskler göz ardı edilebilmektedir. Yazılımlardaki dizayn ve uygulama hataları sıra dışı hatalara neden

olabilmekte, sistem hatası ve güvenlik açıkları neticesinde saldırılar gerçekleşebilmektedir(CERT, t.y.).

B. Yazılım Tedarik Zinciri

Sofistike bilgi teknolojileri çözümleri mühendislik açısından birçok ortak noktaya sahiptir. Bütün bileşenler a) tedarikçileri tarafından ya da tedarikçiler adına taşeronlar tarafından geliştirilir b) bir başka satıcı tarafından tedarikçiye lisanslanır ya da açık kaynak kod ambarlarından elde edilir ya da c) tamamen ve doğrudan tedarikçiden temin edilir. Tedarik zinciri iş aktiviteleri çerçevesinde müşteri taleplerinin karşılanması açısından tedarikçinin tedarikçisinden müşterinin de müşterisine kadar olan süreci kapsar (Simpson, 2009).

Yazılım tedarik zincirleri olarak fiziksel bileşenler, ağ anahtarları ve yazılımı gibi entegre bileşen örneklerini içermektedir. Bir yazılım tipik olarak tek bir parça halinde tüm organizasyona dağıtılır ve tedarik zinciri prensiplerine tabi olur. Donanım ve entegre bileşenleri ise birden çok dağıtım paketlerini içerir ve dolaysıyla her dağıtım için tedarik zinciri bütünlüğü kontrol edilmelidir. Devletlerin askeri, sivil ve istihbarat kapasitelerini artırmak için kompleks yazılımlara artan ihtiyacı, tedarik zincirine dair güven konusundaki endişeleri artırmıştır(Ellison ve diğerleri, 2010). Tedarik Zinciri Risk Yönetimi(TZRY) ticari olarak elde edilen bilgi ve iletişim teknolojilerine dair tehdit ve güvenlik açıklarına hitap eden bir disiplindir. TZRY sayesinde sistem mühendisleri, güvenilmeyen, tanımlanamayan ya da ilave materyal ve parça sağlayan sisteme dair riskleri minimize ederler (MITRE, t.y.).

Sistematik risk değerlendirmesi, sonucu güçlü bir biçimde etkileyebilecek küçük faktörlere bağlıdır. Bu faktörler amaçların yerine getirilmesi noktasında meydana gelebilecek riskleri barındırır. Tüm bu faktörlerin cevabı evet ya da hayır olarak verilir. Evet minimal risk olarak kabul edilir ve hayır ise tedarik zincirine karşı yüksek risk anlamına gelir (Alberts ve Dorofee, 2009).

III. Güvenlik Önlemleri

A. Ödeme Sistemleri Güvenliği

Genel olarak kaliteli güvenlik sistemlerinin kullanıcılarının sisteme olan güvenini artırdığına inanılır ve netice olarak e-ticaretin artması beklenir (Kim, Tao, Shin, ve Kim, 2010). Ödeme sistemlerinde ve e-ticaret içerisinde güvenliği sağlayabilmek için Ödeme Kartları Endüstrisi Veri Güvenliği Standardı (PCI DSS) oluşturulmuştur. Bu standardın amacı, ödeme kartı sahiplerine ait kartların güvenliğinin sağlanması ve alınabilecek güvenlik tedbirlerinin global çapta yayılmasının teşvik edilmesidir. Bu standart, banka ve kredi kartlarının kullanımı esnasındaki güvenlik tedbirlerinin yanısıra, e-

ticaret sektöründeki tüm aktörlere uygulanabilecek niteliktedir. Bunlar arasında tüccarlar, hizmet sağlayıcılar ve mağazalar gibi birçok sektör bulunmaktadır. PCI Güvenlik Konsülü'ne (2013, s. 5) göre Ödeme Kartları Endüstrisi Veri Güvenliği Standardı özet olarak aşağıdaki hususları içerir:

1. Güvenli Ağ ve Sistemlerinin Oluşturulması ve Bakımı
2. Kart Sahibinin Verilerinin Korunması
3. Güvenlik Zaafiyeti Yönetimi Programı Takibi
4. Güçlü Erişim Kontrol Önlemlerinin uygulanması
5. Ağların Düzenli Olarak Takibi ve Testleri
6. Bilgi Güvenliği İlkelerinin Korunması

Yukarıdaki hususların birçoğu erişim haklarının korunması ve düzenlenmesi ile ilgilidir. İnternet bankacılık sistemleri kullanıcılarını spesifik sistemlere erişim hakkı sağlamadan önce kimlik doğrulamasını gerçekleştirmek zorundadır. Bankacılık sistemi kullanıcının gerçekten de o kişi olup olmadığını bir takım gizli sorular sorarak teyit eder(Hiltgen, Kramp ve Weigold, 2006). İnternette neredeyse tüm çevrimiçi alışverişler ve tarayıcı tabanlı işlemler uzunca bir süre SSL(Soket Düzeyi Güvenlik) tarafından güvenlik altına alınmıştır. SSL istemci ve sunucu arasında kriptolu ve doğrulamalı iletişim amacıyla kullanılan de fakto bir güvenlik standardıdır. SSL e-ticaretin dışında birçok alanda da aşağıda belirtilen amaçlar için kullanılır (Blue Coat, 2008, s. 1):

1. Finans merkezlerine ait hesap ve PİN numaralarını gizlemek,
2. Sigorta şirketlerine ait sigorta politikalarını gizlemek,
3. Organizasyonlar ve iş dünyası arasındaki işlemleri güvenli hale getirmek,
4. Özel organizasyonların çalışanları arasındaki iletişim gizliliğini korumak,
5. E-posta sunucularının ve web tabanlı postaların korunmasını sağlamak.

E-ticaret açısından güvenli ödeme yapmak oldukça kritik bir husustur. SSL online ödemelerde oldukça güvenli bir ödeme metodu olmasına rağmen, müşteri ve satıcıların birbirlerine güvenmesi gerekliliğine dayalıdır. SSL banka ve müşterisine ait iletişimi dinlemek suretiyle mesaj akışını kestirenlerin önüne geçilmesi amacıyla kullanılır ve bu sayede ödeme bilgileri gizli kalır. Ancak SSL bir takım riskleri de barındırır. Satıcılar reklamını yaptıkları ücretten daha fazla ücret ödenmesini sağlayabilir ya da ticari maksat kılığındaki bir web sitesi tarafından da taklit edilebilir(Li ve Yun, t.y.). SSL'de birçok güvenlik protokolü gibi kendisine göre daha üstün bir teknoloji ile geliştirilmiş olan bir başka protokol olan TLS'e yerini devretmiştir.

TLS (Transport Layer Security) SSL 3.0 versiyonu ile oldukça yakındır ve zaman zaman SSL 3.1 olarak da tanımlanır. Farklı uygulamalar arası iletişimi sağlayan uygulamalar SSL 3.0 ve TLS'i desteklemelidirler(Microsoft, t.y.)

Güvenli Elektronik İşlem (SET- Secure Electronic Transaction) ise, VISA ve MasterCard tarafından ortaklaşa geliştirilmiş olan açık ağlarda ödeme ve işlemleri güvenli hale getirmek için oluşturulmuş bir e-ticaret protokolüdür(Lu ve Smolka, 1999). SET protokolü kredi kartı bilgilerinin internet ortamında işlem yaparken çalınmayacağını taahhüt eder(Boping ve Shiyu, 2009). Bu protokol formal bir model oluşturarak spefisifik protokol amaçlarını belirlemek ve ispatlamak için vardır. Yapılan araştırmalar, protokolün amaçlarını gerçekleştirmede bir takım eksiklikleri olduğu belirlemiştir. Protokolün karmaşıklığı ve bilgi paylaşımındaki sıra dışı olgular temel risk unsurlarıdır (Bella, Massacci ve Paulson, 2005). SET protokolü DES kripto algoritmasını kullanmaktadır. Ancak, DES güvenli bir algoritma olarak kabul edilmemektedir. Ayrıca, protokol işlemleri sertifikanın imzalayanlar tarafından gerçekleştirildiğini ispatlayamamaktadır (Boping ve Shiyu, 2009).

SSL ve TSL'de yaşanan son kullanıcı güvenlik gereklilikleri açısından yetersizlikler(Jarupunphol ve Mitchell, 2003) ve SET protokolündeki mevcut hatalar, 3-D Secure protokolünün geliştirilmesi ve yaygınlaşmasına yol açmıştır. Ödeme sistemleri endüstrisinin SET'i bırakarak online ödemelerde dolandırıcılığı önleme odaklı 3-D Secure protokolüne geçiş yapması yaklaşık on yılı bulmuştur. 3-D Secure sistemi kullanıcılara yeni bir şifreleme sistemi sunarak büyük avantajlar sağlamıştır. Ancak, 3-D Secure sitemi, uygulamasına geçişteki süreye rağmen, sahip olma, kullanılabilirlik ve güvenlik açısından birçok sorunları barındırmaktadır(Bouch, 2011).

Bahsi geçen kriptografik protokollerin yanı sıra kriptografik süreçlerin güvenilirliği anahtarların ne kadar güçlü olduğu ile bağlantılı olduğundan kriptografik anahtarların güvenli yönetimide oldukça önemlidir. Kriptografik anahtarlar bir kasanın açılmasında kullanılan kombinasyona benzerler. Eğer saldırgan kombinasyonu öğrenirse kasa artık güvenli değildir. Kötü anahtar yönetimi güçlü bir kriptografik algoritmanın alt edilmesine neden olabilir(Radack, 2010).

Yukarıda bahsi geçen birçok teknoloji güncellenerek devam ettirilmekte ya da rafa kaldırılmaktadır. Ancak, bahse konu teknolojilerin zamanında adaptasyonu, verimli ve etkin yönetimi ve finansal sistemimize maliyetleri ayrıca değerlendirilmelidir. Diğer bir husus, kullanılmakta olan kriptografi protokollerinin tamamen Türkiye'den bağımsız olarak geliştirilmekte olan de fakto standartlar

olması, kriptografik protokol gelişimi açısından dışa bağımlı bir finansal siber güvenlik altyapının devamı anlamını taşımaktadır.

B. Tedarik Zinciri Güvenliği

Tedarik zinciri; süreçler, ürünler, ürün akışları, veri, veri akışları ve katılımcılardan oluşur. Günümüz organizasyonları yazılım gereksinimlerini güvenilir ya da çevrimiçi teknik destek üniteleri gibi güvenilir olmayan birçok farklı kaynaktan elde etmektedirler(Goertzel, 2010). Yazılım tedariği zinciri genel olarak fonksiyonelliğin yerine getirilmesi üzerine inşa edilmekte, yazılımda bulunabilecek riskler sıklıkla göz ardı edilmektedir(US-CERT, 2009). Global tedarik zincirlerine olan tehditlerden dolayı tedarikçi ve alıcılar arasındaki bağımlılıkların tanımlanması ve değerlendirilmesi gerekmektedir. Tedarik zinciri bütünlüğü ve risk azaltımı herhangi bir spesifik ülkeyi kapsamamaktadır. Amaç, tedarik zincirinin daha güvenli olmasını sağlamak olmalıdır. Siber güvenlikle ilgili diğer hususlarda da olduğu gibi, efektif Tedarik Zinciri Risk Yönetimi güçlü bir kamu-özel ortaklığı gerektirmektedir. Finansal güvenlik açısından güvenli tedarik zincirlerinin oluşturulabilmesi açısından teşvikler, iletişim, gönüllü risk analizleri ve bilgi paylaşımı anahtar rol üstlenebilecektir (Filsinger, 2012).

Microsoft, (2014, s.3) tedarik zinciri güvenliğini esas olarak aşağıdaki altı adım ile kontrol etmektedir:

1. Yazılımlara erişimin gelişim aşamasında kontrol edilmesi
2. Kötücül yazılımların taranması
3. Kullanıcıların teslim alacağı ikili dosyalara dijital imza atılması yoluyla gerçekten de dağıtılan ürünleri teslim aldıklarının teyit olunması
4. Güvenlik Geliştirme Hayat Döngüsünden yararlanarak istenmeyen güvenlik zaafiyetlerinin önüne geçilmesi
5. Kimlik tanımlama
6. Sahtecilik önleme

Microsoft'un belirttiği adımların birinci aşamasında ülkemizde önemli sıkıntılar mevcuttur. Zira, siber güvenlik yazılımı geliştirme açısından geride bulunan ülkemiz, tedarik edilen yazılımları geliştirme aşamasında inceleme şansını elde edememektedir. İkinci aşama ile ilgili ise birçok sorunla karşılaşıldığı bilinmektedir. Vatandaşların antivirüs programı satın almadaki isteksizlikleri zararlı yazılımların geniş çapta ülke internet ağındaki bilgisayarlara yayılmasına sebep olucu niteliktedir. Diğer adımlarla ilgili ülkemizde birçok önemli çalışma bulunmakla beraber, ilk iki adımda meydana gelebilecek siber güvenlik tehditlerinin önlenememesi, sonraki adımlarıda olumsuz etkileyebilecektir.

IV. Sonuç

Dünya üzerindeki birçok ülke siber saldırılara karşı radikal çözümler ortaya koymakta ve bu amaçla yatırımlar yapmaktadırlar(Grauman, 2012). ABD gibi bir takım ülkeler pazar tabanlı olarak siber güvenlik kritik altyapılarını korumakta iken, İsrail gibi ülkeler devlet odaklı siber güvenlik stratejileri geliştirmektedir (Assaf, 2008). Birçok siber güvenlik uzmanıysa, telekomünikasyon sektörü ve internet servis sağlayıcıları gibi özel sektör girişimleri kamu hizmetlerini ve aktivitelerini desteklediğinden, savunmacı ve karşılık verici bir güvenlik rejiminin özel sektör temsilcileriyle birlikte hareket etmeden efektif olarak gerçekleşemeyeceğini beyan etmektedir(INSA, 2009).

Halkın ve devletin büyük çoğunluğuna ait verilerin saklandığı yer olan elektronik finans sistemi ve bunların destekçisi olan tedarik zinciri ihmal edilmemesi gereken kritik siber güvenlik unsurlarıdır. Ulusal ve uluslararası ticaretin en önemli bileşenlerinden biri olan internet bankacılığı, e-ticaret ve onları destekleyen tedarik zincirlerinin güvenlik boyutunun göz ardı edilmesi düşünülemez. Zira, ülke ekonomileri giderek artan bir hızla rekabete dayalı ekonomilerini özel sektör desteğiyle internet üzerinden yürütmekteler ki elektronik finans sürdürülebilirliği bu yapıyı taşıyan internet altyapısının korunaklılığı ile ilişkilidir. Kalpazanlık, dolandırıcılık ve benzeri asayiş suçları ile mücadelede yürütülen önleyici hizmet mantalitesi, dijital sistemler üzerinde de en az aynı yorum ve donanım ile devam ettirilmelidir.

Ülkemizdeki elektronik finans sektörünün, kendi açısından yeterli standartlara sahip olması, ISO 31000 - Risk Yönetimi benzeri prensip ve rehberlere uygun bir risk yönetimi anlayışını tercih etmesi, yazılım ve donanım tedariğinde mümkün olduğu kadar ulusal kaynaklı, ancak uluslararası standartlarda güvenlik teknolojilerine sahip ürünleri tercih etmesi, ödeme sistemleri ve e-ticaret güvenliği açısından oldukça önemlidir.

Uluslararası bazda yapılan birçok yatırım ve alınan güvenlik önlemlerine rağmen finansal sistemin güvenliğinin internet ortamında yeterince sağlanabileceği söylenemez. Ticari açıdan birçok büyük bankanın internet kullanıcı bilgileri ya da ödeme kartlarına ait bilgilerin topluca ya da bireysel olarak çalındığı haberleri sıklıkla medyada yer almaktadır. Türkiye'nin özellikle e-ticaret noktasında zayıf olması, bu alanda yatırım teşviklerinin yeterince oluşturulmasının yansıra siber güvenlik politikalarının geliştirmesi için adımlar atılması gerekliliğini ortaya koymaktadır.

Bu çalışmada ortaya konulan siber güvenlik açıkları finansal sistem bilgi işlem ve güvenlik birimlerince göz önünde

bulundurulmalı ve aynı zamanda ulusal bazda finansal sistemimizin analizlerinde karşımıza çıkan problemler daha hızlı bir şekilde onarılmalı ve yerlerine güncel çözümler üretilmelidir. Finansal sistemin çoğunlukla yabancı kaynaklı yazılım ve donanım firmalarınca korunaklı hale getirilmesi Türkiye açısından yeterli değildir. Bankalar siber güvenlik altyapılarına daha fazla bütçe ayırmalı ve yerli çözümlere daha fazla yatırım yapmalıdır.

Kamu yöneticilerinin elektronik tabanlı ödeme sistemlerinin bütün teknik altyapısını irdeleyerek kavramasına ihtiyaç yoktur. Ancak, neden ve sonuçları hakkında temel bilgi sahibi olmadan da politika analistleri açısından gerçekçi finansal siber güvenlik politikaları üretilmesi mümkün değildir. Bu nedenle, yukarıda sunulan hususların kamusal problem olarak ele alınması ve gerekli araştırmaların süratle yapılması faydalı olacaktır.

KAYNAKLAR

ASSAF, Dan (2008), "Models of Critical İnformation İnfrastructure Protection", *International Journal of Critical Infrastructure Protection,* Sayı: 1, ss. 6-14. http://www.researchgate.net/profile/Dan_Assaf/ erişim tarihi: 19.05.2014.

ALBERTS, Christopher, J., & DOROFEE, Audrey, J, (2009, Nisan), A Framework for Categorizing Key Drivers of Risk (No. CMU/SEI-2009-TR-007 Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, http://repository.cmu.edu/cgi/viewcontent.cgi?article=1045&context=sei, erişim tarihi: 08.05.2014

ANDRIJCIC, Eva ve HOROWITZ, Barry (2006), "A Macro-Economic Framework for Evaluation of Cyber Security Risks Related to Protection of Intellectual Property", *Risk Analysis*, Sayı: *26*(4), ss. 907-923. erişim tarihi: 20.05.2014

BANKALARARASI KART MERKEZİ (BKM), 2014. *Dönemsel Bilgiler,* İstanbul, http://www.bkm.com.tr/donemsel-bilgiler.aspx erişim tarihi: 08.05.2014

BELLA, Giampaolo, MASSACCI, Fabio ve PAULSON, Lawrence, C. (2005), "An Overview of the Verification of SET", *International Journal of Information Security*, Sayı:4(1/2), 17-28. doi:10.1007/s10207-004-0047-7.

BOLLIER, David (2006), *When Push Comes to Pull Economy*, Washington, DC: The Aspen Institute. http://bollier.org/sites/default/files/aspen_reports/2005InfoTechText.pdf erişim tarihi: 08.05.2014

BOPING, Zhang ve SHIYU, Shang (2009, Ağustos), *An Improved SET Protocol*. In *Proceedings of the 2009 International Symposium on Information Processing (ISIP'09)*, ss. 267-272. erişim tarihi: 21.05.2014

BLUE COAT (2008), *Technology Primer: Secure Sockets Layer (SSL),* Sunnyvale, CA, https://www. bluecoat.com, erişim tarihi: 08.05.2014

BOUCH, Anthony (2011), *3-D Secure: A critical review of 3-D Secure and its effectiveness in preventing card not present fraud*, University of London, Londra,
erişim: http://www.58bits.com/thesis/3-D_Secure.pdf, erişim tarihi: 08.05.2014

CASALO, Luis. V., FLAVIÁN, Carlos ve GUINALÍU, Miguel (2007), "The Role of Security, Privacy, Usability and Reputation in the Development of Online Banking", *Online Information Review*, Sayı: 31(5), ss.583-603, erişim tarihi: 08.05.2014

CERT(t.y.), Supply chain assurance, CERT Software Engineering Institute Web sitesi: http://www.cert.org/cybersecurity-engineering/research/supply-chain-assurance.cfm, erişim tarihi: 08.05.2014

CLAESSENS, Joris, DEM, Valentin, DE COCK, Danny, PRENEEL, B., & VANDEWALLE, Joos (2002), "On the Security of Today's Online Electronic Banking Systems", *Computers & Security*, Sayı: 21(3), ss. 253-265, erişim tarihi: 08.05.2014

COŞKUN, M. Necat, ARDOR, Hakan. N. ve diğerleri (2012), *Türkiye'de Bankacılık Sektörü Piyasa Yapısı, Firma Davranışları ve Rekabet Analizi*, Türkiye Bankalar Birliği, İstanbul.
erişimhttp://www.tbb.org.tr/Content/Upload/Dokuman/796/rekabetKitap.pdf, erişim tarihi: 08.05.2014

CHONG, Alain Yee-Loong ve diğerleri (2010), "Online Banking Adoption: An Empirical Analysis", *International Journal of Bank Marketing*, Sayı**:** 28.4, ss.267-287.

COWHEY, Peter. F. ve ARONSON, Jonathan. D (2009), *Transforming global information and communication markets*, Cambridge, Massachusetts: The MIT Press.

DAN, Sarel ve HOWARD, Marmorstein (2006), "Addressing Consumers ' Concerns About Online Security: A Conceptual And Empirical Analysis of Banks ' Actions", *Journal of Financial Services Marketing,* Sayı:11.2, s s. 99-115.

DZEMYDIENĖ, D., NAUJIKIENĖ, R., KALINAUSKAS, M., & JASIUNAS, E. (2010). "Evaluation of Securıty Disturbance Risks in Electronic Financial Payment Systems", *Intellectual Economics*, Sayı:2(8), ss.21-29.

ELLISON, Robert. J., ALBERTS, Christopher, CREEL, Rita., DOROFEE, Audrey ve WOODY. Carrol (2010), *Software supply chain risk management: From products to systems of systems*, Software Engineering Institute, Pittsburgh. http://www.sei.cmu.edu/reports/10tn026.pdf, erişim tarihi: 02.05.2014.

FILSINGER, Jarrellann, FAST, Barbara, WOLF, Danial.G., PAYNE, James, F.X. (2012), *Supply chain risk management awareness* ,Armed Forces Communication and Electronics Association, Cyber Committee.
http://www.afcea.org/committees/cyber/documents/Supplychain.pdf, erişim tarihi: 08.05.2014

GOERTZEL, Karen Mercedes (2010) "Supply Chain Risk Management and the Software Supply Chain", *OWASP AppSec DC*, erişim https://www.owasp.org/images/7/77/BoozAllen-AppSecDC2010-sw_scrm.pdf, erişim tarihi:15.05.2015.

GRAUMAN, Brigid (2012), Cyber-security: The Vexed Question of Global Rules. Security and Defence Agenda, http://www.isssource.com/wp-content/uploads/2012/02/020212rp-sda-cyber-security.pdf, erişim tarihi: 23.05.2014

HILTGEN, Alain, KRAMP, Thorsten ve WEIGOLD, Thomas (2006), "Secure Internet Banking Authentication", *Security & Privacy*, *IEEE*, Sayı:4(2), ss.21-29, erişim tarihi: 08.05.2014

HUTCHINSON, Damien, & WARREN, Matthew (2003), "Security for internet banking: a framework", *Logistics Information Management*, 16(1), 64-73, erişim tarihi: 08.05.2014

Internet World Stats (2012). *Internet Usage Statistics,* http://www.internetworldstats.com/stats.htm. erişim tarihi: 08.05.2014.

INSA (2009), Addressing cyber security through public - private partnership - an analysis of existing models, Arlington, VA, http://www.insaonline.org/, erişim tarihi: 08.05.2014

JARUPUNPHOL, Pita ve MITCHELL, Chris (2003, June), Measuring 3-D Secure and 3D SET against e-commerce end-user requirements. İçinde 8th Collaborative Electronic Commerce Technology and Research Conference, CollECTeR, Europe, Galway, Ireland, ss. 51-64.

KHAROUNI, Loucif (2012), Automatic transfer system: The latest cybercrime toolkit feature. trend micro ıncorporated research paper. Trend Micro, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-

papers/wp_automating_online_banking_fraud.pdf, erişim tarihi: 08.05.2014

KIM, Changsu, TAO, Wang, SHIN, Namchul ve KIM, Ki-Soo (2010). "An Empirical Study of Consumers' Perceptions of Security and Trust in e-Payment Systems." *Journal of Electronic Commerce Research and Applications*, Cilt No: 9, Sayı: 1, ss. 84-95.

KOM Daire Başkanlığı (2012), *Kaçakçılık ve Organize Suçlarla Mücadele, 2011 raporu,* KOM Yayınları: Ankara, erişim www.kom.gov.tr, erişim tarihi: 21.08.2014

KUMAR, Muneesh, SAREEN, Mamta ve BARQUISSAU, Eric (2012), "Relationship between types of trust and level of adoption of Internet banking", *Problems and perspectives in management : PPM*.., Sayı:10 (1), ss. 82-92. http://businessperspectives.org/journals_free/ppm/2012/PPM_2012_01_Kumar.pdf, erişim tarihi: 08.05.2014

LI, Yang ve WANG, Yun (2001), *Secure Electronic Transaction (SET protocol)*, http://ccc.cs.lakeheadu.ca/set/set-lw.pdf, erişim tarihi 15.05.2014

LU, S., & SMOLKA, S. A. (1999), Model Checking the Secure Electronic Transaction (SET) Protocol. In Modeling, Analysis and Simulation of Computer and Telecommunication Systems, 1999. Proceedings. 7th International Symposium on, ss. 358-364, IEEE.

MITRE(t.y.), *Supply Chain Risk Management*. MITRE: http://www.mitre.org/publications/systems-engineering-guide/enterprise erişim tarihi: 08.05.2014

MICROSOFT (2014), *Toward a Trusted Supply Chain: A Risk Based Approach to Managing Software Integrity*, http://www.microsoft.com/en-us/download/details.aspx?id=26828, erişim tarihi: 08.05.2014

MICROSOFT (t.y.), *TLS vs. SSL*, http://msdn.microsoft.com/en-us/library/windows/desktop/aa380515(v=vs.85).aspx, erişim tarihi: 08.05.2014

NASHERI, Hedieh (2005), *Economic espionage and industrial spying*, New York: Cambridge University Press.

NSOULI, Saleh, M. ve SCHAECHTER, Andrea (2002), "Challenges of the E-Banking Revolution", *Finance and Development,* Cilt: 39 Sayı: 3 https://www.imf.org/external/pubs/ft/fandd/2002/09/nsouli.htm, erişim tarihi: 08.05.2014

OOI, Keng-Boon, LIN, Binshan, TAN, Boon-In, ve YEE-LOONG CHONG Alain (2011), "Online Banking Adoption: An Empirical

Analysis", *International Journal of Bank Marketing*, Sayı: *28*(4), ss.267-287.

PCI GÜVENLİK KONSÜLÜ (2013), Ödeme Kartları Endüstrisi Veri Güvenliği Standardı, https://www.pcisecuritystandards.org/security_standards/, erişim tarihi: 08.05.2014

PAGANIN, Pierluigi (2013), Modern Online Banking Cyber Crime, erişim http://resources.infosecinstitute.com/modern-online-banking-cyber-crime/, erişim tarihi: 08.05.2014

PAVLOU, Paul. A, (2003), "Consumer Acceptance of Electronic Commerce: Integrating Trust And Risk With The Technology Acceptance Model", *International journal of electronic commerce*, Sayı:*7*(3), ss.101-134.

RANDAZZO, Marisa R, KEENEY, M., KOWALSKI, E., CAPPELLI, D., & MOORE, A. (2005), *Insider Threat Study: Illicit Cyber Activity in The Banking And Finance Sector* , Carnegıe-Mellon Unıv, Pıttsburgh, Software Engıneerıng Inst.

REKABET KURUMU (2013), *Ticari Sırların Korunması,* http://www.rekabet.gov.tr/default.aspx?, erişim tarihi: 08.05.2014

RADACK, SHIRLEY (2010), *Secure Management of Keys in Cryptographic Applıcations: Guidance for Organizations,* http://csrc.nist.gov/publications/nistbul/february2010_key-management-part3.pdf, erişim tarihi: 08.05.2014

RAJA, J. ve VELMURGAN, Senthil, M. (2008), E-payments: Problems and Prospects, *Journal of Internet Banking & Commerce*, Sayı:*13*(1), ss.1-17, erişim tarihi: 08.05.2014

REEVES, Jeff (2013), Cybersecurity – 5 *security companies for uncertain times.* http://investorplace.com/2013/12/investing-cybersecurity-5-security-companies-uncertain-times/view-all/#.Ux7I5T9_tGQ, erişim tarihi: 09.05.2014

SABAH (2014), Türkiye Kartta Avrupa liderliğine Soyundu. http://www.sabah.com.tr/Ekonomi/2014/05/12/turkiye-kartta-avrupa-liderligine-soyundu, erişim tarihi: 08.05.2014

SCHNEIDER, Gary P. (2010), *Electronic Commerce 2010,* Boston, Massachusetts: Prentice Hall Press.

SHARMA, Surinder ve RAMANDEEP, Singh (2011), Factors Influencing Internet Banking: An Empirical Investigation. *IUP Journal Of Bank Management*, Sayı**:***10*(4), ss.71-80.

ŞIKER, Perihan (2011), Müşterilerin İnternet Bankacılığını Benimsemelerine Yönelik Keşifsel Bir Araştırma. *Uygulamaları ve Yönetimi*, Sayı: 35.

SIMPSON, Stacy (2009), *The software supply chain integrity framework.*

http://www.safecode.org/publications/SAFECode_Supply_Chain0709.pdf, erişim tarihi: 08.05.2014

SUH, Bomil ve HAN, Ingoo (2003), "The İmpact Of Customer Trust And Perception Of Security Control On The Acceptance Of Electronic Commerce", *International Journal of electronic commerce*, Sayı:*7*, ss.135-161.

TÜİK (2011), Bilgi Toplumu İstatistikleri*,* Ankara: TÜİK İstatistik Konseyi, www.tuik.gov.tr

TÜİK(2013), Hane Halkı BT Kullanım Araştırması, Ankara: TÜİK İstatistik Konseyi, http://www.tuik.gov.tr/PreHaberBultenleri.do?id=13569, erişim tarihi: 01.05.2014

TSIAKIS, Theodosios ve George STHEPHANIDES (2005), The Concept of Security and Trust İn Electronic Payments. *Computers & Security***,** Sayı:*24*(1), ss.10-15.

YESİLYURT, Hamdi, (2011), "The Response of American Police Agencies to Digital Evidence" *University of Central Florida* Doktora Tezi, Orlando, ABD.

YESİLYURT, H. (2015). *Siber Suçlar: Tehditler, Farkındalık ve Mücadele,* İçinde F. Tombul, M. Gunestas, O. Basibuyuk (Eds.), Global Press, ss. 169- 195.

White House (2013), *National Strategy for Global Supply Chain Security Implementation Update*. http://www.whitehouse.gov/sites/default/files/docs/national_strategy_for_global_supply_chain_security_implementation_update_public_version_final2-26-131.pdf erişim tarihi: 12.05.2014

US-CERT(2009). "Software Supply Chain Risk Management & Due-Diligence". Cilt:2 https://buildsecurityin.us-cert.gov/sites/default/files/DueDiligenceMWV12_01AM090909.pdf