SİBER SALDIRILAR, SİBER GÜVENLİK DENETİMLERİ VE BÜTÜNCÜL BİR DENETİM MODELİ ÖNERİSİ*

Dr. Öğr. Üyesi Mahmut Sami ÖZTÜRK[a]

Teorik İnceleme
(Theoretical Research)

Muhasebe ve Vergi Uygulamaları Dergisi
Nisan 2018; Özel Sayı:208-232

ÖZ

Artan rekabet koşullarına uyum sağlayabilmek ve global dünyadaki gelişmelere ayak uydurabilmek için işletmeler, bilgi teknolojilerini yoğun bir şekilde kullanmakta, elektronik ortamda işlemlerini gerçekleştirmekte ve raporlama yapmaktadırlar. Bilgi teknolojileri sağladığı faydalar ile birlikte, bazı önemli tehdit ve riskleri de beraberinde getirmektedir. Bu tehditlerin en önemlilerinden olan siber saldırılar işletmeler için son derece önem teşkil etmektedir. İşletmeler, gerek işletme içinden gerekse işletme dışından kaynaklanan siber saldırılara maruz kalabilmektedir. İşletme içerisinde gerçekleştirilen siber suçlar hile sınıflandırmaları içerisinde yeni bir madde olarak ayrıca yerini almaktadır. Dolayısıyla siber suç hileleri işletmelerin odaklanması gereken önemli noktalardan bir tanesi olacaktır. Meydana gelen siber saldırılar sonucunda işletmeler yüksek maliyetlerle karşılaşmaktadırlar. Aynı zamanda dünya genelinde siber suçların çok ciddi zararlara ve maliyetlere sebep olduğu görülmektedir. Siber saldırıları önlemek için işletmeler hazırlıklı olmalı, gerekli altyapı sistemlerini oluşturmalı, risk ve kontrol değerlendirmeleri ile siber güvenlik denetimlerini çok iyi bir şekilde uygulayabilmelidir. Literatürde yeni yerini almaya başlayan siber güvenlik denetimleri gün geçtikçe daha fazla önem kazanmaktadır. Bu çalışmanın amacı, siber güvenlik denetimindeki tüm sürecin bütüncül bir biçimde ele alınması suretiyle bir model dâhilinde gösterilmesidir. Geliştirilen model önerisinde siber güvenlik denetimi bir süreç olarak incelenmektedir. Bu kapsamda siber güvenliğe ve denetime etki eden iç ve dış faktörler ile denetimin planlamasından itibaren denetim raporu ve güvenceye kadar geçen tüm süreç akış şeması aracılığıyla oluşturulan bir model ile açıklanmaktadır.

Anahtar Sözcükler: Siber Saldırılar, Siber Güvenlik Denetimleri, Denetim Süreci, Bilgi Teknolojileri, Akış Şeması.

JEL Kodları: M42, O33, O39.

* Bu makale, 13-17 Aralık 2017 tarihinde Erzurum'da düzenlenen 4.Uluslararası Muhasebe ve Finans Araştırmaları Kongresinde sunulmuş olan özet bildirinin genişletilmiş tam metnidir.

[a] Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi İşletme Bölümü, samiozturk@sdu.edu.tr, Orcid Number: 0000-0002-7657-3150

CYBER ATTACKS, CYBER SECURITY AUDITS AND AN INTEGRATED AUDIT MODEL PROPOSAL

ABSTRACT

In order to adapt to the increasing competition conditions and keep up with the developments in the global world, the enterprises use information technology intensively and they perform transactions and make reports in electronic environment. Information technologies provide many benefits but also they bring some important threats and risks. One of the most important of these threats is cyber attacks, which are extremely important for businesses. Companies can be exposed to cyber attacks from inside and outside. Cybercrime committed within the company also takes place as a new substance within the fraud categories. Therefore, cyber attack frauds will be one of the important points that companies should focus on. As a result of the cyber attacks, enterprises face high costs. At the same time, it is seen that cybercrime causes very serious damages and costs throughout the world. Companies must be ready to prevent cyber attacks. Also they should establish the necessary infrastructure systems, implement risk and control assessments and cyber security audits very well. Cyber security audits, which are starting to take a new place in the literature, are getting more and more important. The aim of this study is to show the whole process of cyber security audit in a model by handling it in an integrated way. In the proposed model, cyber security audit is examined as a process. In this context, the internal and external factors that are affecting the cyber security and audit, and the entire process from the planning of the audit to the audit report and the assurance are explained by a model created through flow chart.

Keywords: Cyber Attacks, Cyber Security Audits, Audit Process, Information Technologies, Flow Chart.

JEL Codes: M42, O33, O39.

1. GİRİŞ

Bilgisayar ve internet, bütün dünyayı siber uzay denilen global bir köy haline dönüştürmüştür. Siber uzay, insanoğlunun ortak bir mirasıdır ancak ne yazık ki bazı kişilerin bu ortak mirası kötü olarak kullandıkları için siber uzay artık farklı bir suç çeşidi haline gelmiştir. İnternet, çeşitli alanlarda bireylere, işletmelere ve ülkelere büyük fırsatlar sunarken diğer taraftan yeni bir suç türü olan siber suçların doğmasına neden olmuştur. Siber suçlar dünya çapında trilyonlarca dolar finansal kayba sebebiyet vermektedir. Ancak birçok kişi veya kurum bu suçun büyüklüğünden ve etkilerden haberdar değildirler (Verma ve Bajaj, 2008: s.147).

Bilgi sistemleri teknolojilerindeki son gelişmeler, işletmelerdeki farklı alanlardaki birçok uygulamada otomasyona geçilmesine sebebiyet vermiştir. İşletmelerde verilerin çok önemli bir kaynak haline dönüşmesinden dolayı, verilere erişim, verilerin paylaşımı, verilerden bilgilerin oluşturulması ve bilgilerin kullanılması önemli bir ihtiyaç niteliğini taşımaktadır. Verilere ve bilgi yönetimine yönelik talebin artmasının yanında, veri tabanlarının, uygulamaların ve bilgi sistemlerinin güvenliğinin tesis edilmesi çok kritiktir.

En az yolsuzluklar kadar yetkisiz erişimlere karşı da verilerin ve bilgilerin korunması gerekmektedir. İnternetin hızla yayılması neticesinde, bu bilgi ve verilere birçok kişinin erişim imkânı bulunmaktadır. Dolayısıyla verilerin ve uygulamaların korunması için etkili mekanizmalara gereksinim duyulmaktadır (Kumar vd. 2005: s.3-4).

Siber saldırıların engellenebilmesi ve araştırılması için siber güvenlik denetimlerine ihtiyaç duyulmaktadır. Yakın dönemde konu ile ilgili araştırmalar ve raporlar yayınlanmaya başlanmıştır. Literatürde yeni yeni yer almaya başlayan siber güvenlik denetimleri hakkında gelecekte daha çok inceleme ve araştırma yapılacağı düşünülmektedir.

Siber güvenlik denetimleri ile ilgili literatür araştırması sonucunda yurtiçinde çalışmalara rastlanmamış olup son zamanlarda yurtdışında yapılmaya başlanan çalışmalar dikkat çekmektedir. Greitzer ve Frincke (2012) tarafından yapılan çalışmada, geleneksel siber güvenlik denetim verilerinin psikolojik veriler ile birleştirilmesi üzerine araştırma yapılmıştır. Peterson (2012) tarafından yapılan çalışmada, siber güvenlik denetimlerinde kullanılan saldırı tespit araçları hakkında araştırma yapılmıştır. Gandhimathi ve Prashanth (2013)'ın yaptıkları çalışmada, şifreleme ve şifre çözme işlemlerinin kullanılmasını içeren T-Pro şifreleme sistemi ile siber güvenlik denetimlerinin nasıl yapılacağı hakkında bir araştırma yapılmıştır. Mukhopadhyay ve diğerlerinin (2013) yaptıkları çalışmada siber risklere karşı alınacak önlemler araştırılmış, işletmelerin siber zararla karşılaşmalarının ardında hangi aşamaların olduğu incelenmiştir. Poonia'nın (2014)'deki çalışmasında siber güvenlik denetimlerinde planlama, teknik denetim ve dokümantasyon araçları üzerine bir araştırma yapılmıştır. City of Vancouver'ın (2016) yılında yayınladığı iç denetim özet raporunda siber güvenlik denetimi örnek olaylar ile açıklanmaya çalışılmıştır. Ojeka ve diğerlerinin (2017) gerçekleştirdikleri çalışmada, Nijerya bankacılık sektöründe siber güvenlik üzerinde denetim komitesinin etkinliği üzerine bir araştırma yapılmıştır. ISACA tarafından yayınlanan siber güvenlik denetimine ilişkin raporda, siber güvenlik denetimlerinin konu ve kapsamı, yürütücüleri ve anahtar noktaları hakkında bilgilendirme yapılmaktadır.

Literatürdeki çalışmalar incelendiğinde, siber güvenlik denetimi süreçlerinin kısımlar halinde parça parça ele alındığı görülmektedir. Bu çalışmada, önceki yapılan çalışmalar birleştirilerek siber güvenlik denetim süreci, bütüncül bir biçimde ele alınmaktadır. Bu kapsamda siber güvenlik denetimlerinin başlangıcından bitişine yani raporlanmasına kadar geçen bütün süreç, bir model dâhilinde açıklanmaktadır. Model önerisinde, siber güvenliğe ve denetimlere etki eden faktörler, denetim planlaması, kanıtların toplanması, denetim faaliyetlerinin yürütülmesi ve icra edilmesi, denetimin raporlanması ve denetim güvencesi bir akış şeması şeklinde

gösterilmektedir. Gerçekleştirilen modelde siber güvenlik denetim modeli süreçleri bütüncül bir şekilde açıklandığından dolayı, siber güvenlik denetimlerinin daha iyi bir biçimde anlaşılması amaçlanmaktadır.

2. SİBER SALDIRILAR

Güvenlik ihlallerinin işletme üzerinde yıkıcı etkilere sahip olabileceğinden ötürü, siber güvenlik günümüz organizasyonlarındaki en büyük risklerden birisi olarak belirlenmektedir. Siber suçluların daha sofistike bir yapıya bürünmesinden ve siber saldırıların çok daha fazla yaygınlaşmasından dolayı bir siber saldırının önemli boyuttaki finansal, operasyonel ve itibarsal zararı; yönetilmesi gereken çok kritik bir risktir (City of Vancouver, 2016: s.1).

Gerek işletme içinden gerekse işletme dışından gelebilecek siber tehdit ve siber saldırı çeşitlerinin çok iyi analiz edilerek işletmeler tarafından gerekli güvenlik önlemlerinin alınması hayati önem taşımaktadır.

2.1. Siber Tehditler ve Çeşitleri

Hızla gelişmekte olan teknolojiler ve evrim geçiren operasyonel uygulamalar ve gereksinimler, hem özel hem de kamu sektöründeki işletmeleri, birbirine son derece bağlı ve teknolojik açıdan yakınsayan bilgi ağlarına yönlendirmektedir. Patentli bilgi işleme çözümleri ve ayrı ayrı veri depolayan veri tabanları, birleştirilmiş entegre sistemlerin kullanımına sebebiyet vermekte ve böylece iyi planlanan tek bir ağ ihlali, veri hırsızlığı veya hizmet engelleme saldırısının potansiyel etkisini önemli ölçüde artırmaktadır. Bu nedenle, ticari işletmelerin ve kamu kurumlarının, yeni saldırı stratejilerine ve taktiklere hızla cevap verebilen veya bunlara yönelik öngörülerde bulunabilen ağ savunma sistemlerini geliştirmeleri son derece önem taşımaktadır (Colbaugh ve Glass 2011: s.125).

Veri yönetim sistemleri, işletim sistemleri, ağlar ve ara yazılımlar gibi bilgi sistemlerine yönelik gerçekleştirilen genel siber tehditler şu şekildedir (Kumar vd., 2005: s.5-6):

Kimlik Doğrulama İhlalleri (Authentication Violations): Şifrelerin çalınmaları neticesinde kimlik doğrulama ihlalleri meydana gelmektedir. Çözüm için birden fazla şifreye ve ek verilere sahip olmak gerekmektedir.

İnkar Edememe (Nonrepudiation): Mesaj gönderen kişi, çok iyi bir biçimde mesaj gönderdiğini inkar edebilir. İnkâr edememe teknikleri ile göndericinin mesajları takip edilerek, inkâr edilmesi engellenebilmektedir. Ancak web sayfasına giren bir kişinin takip edilmesi çok kolay değildir.

Trojan Atları ve Virüsleri (Trojan Horses and Viruses): Trojen atları ve virüsler, bütün saldırılara sebebiyet veren kötü niyetli programlardır. Virüsler makineden makineye yayılarak bir çok bilgisayarda verilerin silinmesine sebebiyet vermektedir. Trojen atları yüksek seviyeden düşük seviyeye bilgilerin sızdırılmasına neden olmaktadır.

Sabotaj (Sabotage): Bilgisayar korsanları, sistemleri kırarak uygun olmayan mesajlar yükleyebilmektedir.

Hile (Fraud): Birçok işletme internet üzerinden faaliyet göstermekte ve satış yapmaktadır. İnternet hileleri ile işletmeler milyonlarca dolar zarar etmektedirler. Suçlular kullanıcıların kimliklerini ele geçirmekte ve gerçek kimliklerini gizleyerek banka hesaplarını boşaltmaktadırlar.

Altyapıların ve Hizmetlerin Engellemelerine Yönelik Saldırılar (Denial of Service and Infrastructure Attacks): Altyapılar, korsanlar tarafından kırılarak zarar görmektedirler. Telekomünikasyon, güç ve ısıtma sistemleri, altyapılara örnek olarak verilebilir. Bu sistemler, internet ortamında bilgisayarlar tarafından kontrol edilmektedirler. Bu saldırılar, hizmetlerin engellenmesine yol açmaktadır.

Doğal Afetler (Natural Disasters): Siber terörizme ek olarak kasırga, deprem, yangın ve benzeri felaketler gibi doğal afetler, bilgisayarların ve ağların zarar görmesine neden olabilmektedir. Veriler korunmalı ve veritabanları doğal afetlere karşı korunaklı hale getirilmelidir.

2.2. Siber Saldırı Çeşitleri

Siber saldırılar sonucu oluşan siber suçlar, çeşitli şekilde sınıflandırılabilmektedir. Literatürde yer alan bazı sınıflandırma çeşitleri aşağıda belirtilmektedir.

"Suçun hedefine göre sınıflandırma şu şekildedir (Milhorn, 2007: s.1-3):

- Kişilere yönelik siber saldırılar,
- Mülkiyete yönelik siber saldırılar,
- Kurumlara yönelik siber saldırılardır."

"Suçların meydana gelme şekline göre sınıflandırma şu şekildedir (Milhorn, 2007: s.1-3):

- Tek bir olay şeklinde meydana gelen saldırılar,
- Olaylar zinciri şeklinde meydana gelen saldırılardır."

AICPA tarafından 2013 yılında yayınlanan rapora göre dünya genelinde daha önce meydana gelen siber suçlar içinde en büyük 5 siber suç çeşidi aşağıdaki gibi bir araya getirilmiştir. Bunlar (AICPA 2013):

- **Vergi Dolandırıcılığı:** Meydana gelen tek bir siber suç vakasında, siber dolandırıcılar daha önce vergi mükellefi olan ölmüş kişilerin sosyal güvenlik numaralarını kullanarak beş binden fazla yanlış vergi iadesi doldurarak mağdurları yaklaşık 14 milyon dolar zarara uğratmışlardır. ABD Hazine Müfettişliği Genel Müdürlüğü Vergi Dairesi raporuna göre, 2011 yılında kimlik hırsızlığından ötürü yaklaşık 1,5 milyon adet yanlış vergi beyannamesinin fark edilemediği ve toplam 5,2 milyar doları aşan zarar meydana geldiği belirtilmektedir. Yine aynı vergi sezonunda yaklaşık 1 milyon hileli vergi iadesi sonucu 6,5 milyar dolar yanlış para iadesi yapıldığı tespit edilmiştir.
- **Kurumsal Hesapların Devri:** Son zamanlarda maliyetli, hızlı ve gizli yeni bir siber saldırı çeşidi keşfedilmiştir. Siber suçlular işletmenin banka hesaplarından para çalmak için bir yazılım kullanmak suretiyle gizlice işletmenin finansal bankacılık kimlik bilgilerini elde etmekte ve bilgisayarlarından bazılarına uzaktan erişim sağlayarak işletmeye binlerce dolar zarar vermektedirler. Elde edilen verilere göre 2009'un üçüncü çeyreğinde elektronik para transferi dolandırıcılığı nedeniyle küçük ve orta büyüklükteki işletmeler (KOBİ'ler) ve finansal kuruluşlar yaklaşık 120 milyon dolar zarara uğramışlardır. Bu rakam, iki yıl önce 85 milyon dolar civarındadır. FBI'a göre, Kasım 2009'da ise tek başına kayıplar, yaklaşık 100 milyon dolar seviyesindedir.
- **Kimlik Hırsızlığı:** Kimlik hırsızlığı, genellikle bir siber hırsızın bir kişinin kimliğine ait bilgileri çaldığı durumda ortaya çıkmaktadır. Maddi bir karşılığı olmadığı sürece kimlik hırsızlığı bir getiri sağlamamaktadır. Dolayısıyla kimlik hırsızlığı; vergi iadesi dolandırıcılığı, kredi kartı sahtekârlığı, kredi dolandırıcılığı ve benzeri diğer suçlara bir kapı oluşturmaktadır. Hileli olarak bir kredi hesabı açılması, mal veya hizmet satın alınması, bir ev veya dairenin kiralanması veya satın alınması, tıbbi bakım alınması, istihdam sağlanması, trafik ihlallerinin veya suçların işlenmesi, açık artırma dolandırıcılığı ve ücretlerle ilgili dolandırıcılıklar kimlik hırsızlığına ait bazı örneklerdir.
- **Hassas Verilerin Çalınması:** Bir işletme tarafından depolanan şifrelenmemiş kredi kartı bilgileri, kişisel olarak tanımlanabilir bilgiler, ticari sırlar, kaynak kodları, müşteri bilgileri ve çalışan kayıtları gibi hassas veriler, siber suçluların ilgisini çekmektedir. Bu siber suç çeşidi, kimlik hırsızlığı ve güvenlik ihlallerine benzemektedir. Hırsızlar bu verileri çalarak mağdurların yüksek maliyetlere katlanmasına sebep olmaktadırlar. Ayrıca işletmelerin

imajları zarar görmekte, iş kayıpları meydana gelmekte, finansal zararlar oluşmakta ve güvenlik önlemlerine daha fazla kaynak ayrılması ile parasal harcamalarda artış meydana gelmektedir.

- **Fikri Mülkiyet Hırsızlığı:** Müzik, film ve kitaplar da dahil olmak üzere ticari, telif hakkıyla korunan materyallerin fikri mülkiyetinin çalınması riski altındadır. Son on yılda müzik sahipleri, siber suç mağduru listesinde yer almaktadır. Ancak telif veya patent hakkı bulunduran işletmeler fikri mülkiyet hırsızlığına karşı korunmaya çalışmalıdırlar.

Siber ortamda birçok siber saldırı meydana gelmektedir. Tüm bu saldırılara örnek olarak; açık artırma dolandırıcılıkları, işletmedeki fırsatlara ve işlere yönelik dolandırıcılıklar, bağış dolandırıcılığı, çocuk istismarı, telif hakkı ihlalleri, sıkıştırmalar, kredi kartı hileleri, kredi dolandırıcılığı, sanal zorbalıklar, siber tacizler, siber soygunlar, siber medikal dolandırıcılıklar, siber terörizm, evlenme, boşanma ile ilgili dolandırıcılıklar, eğitim dolandırıcılıkları, kumar dolandırıcılığı, hacking, kimlik hırsızlığı, göç dolandırıcılığı, yatırım hileleri, laptop hırsızlığı, borç ve bağış dolandırıcılığı, organize suçlar, e-mail dolandırıcılığı, satış hileleri, istek dışı e-postalar (spam), seyahat dolandırıcılığı, virüsler, solucanlar (warms), truva atları (trojans), casus yazılımlar (spyware) verilebilmektedir (Milhorn 2007).

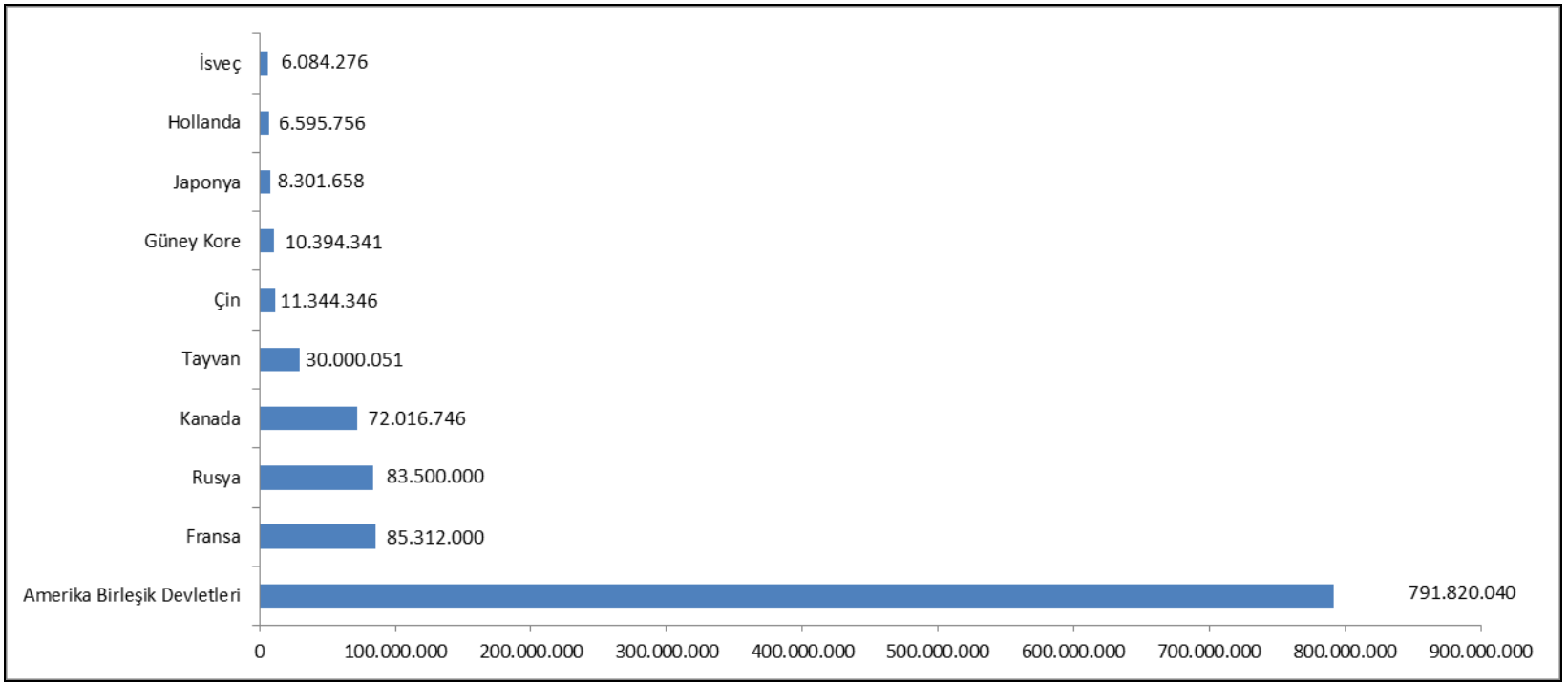
İşletmelere yönelik yapılan bir araştırmada, işletmelerin bilgi teknolojileri üzerinde aşağıdaki güvenlik ihlalleri meydana gelmektedir (Statista, 2015):

- Bilgi teknolojilerinin veya iletişim araçlarının çalınması,
- Çalışanları etkileyen sosyal mühendislik vakaları,
- Hassas dijital belgelerin çalınması,
- Bilgi teknolojileri sistemleri veya süreçlere yönelik sabotajlar,
- Hassas fiziksel belgelerin veya parçaların çalınması,
- Elektronik iletişime yönelik gerçekleştirilen casusluklar,
- Toplantıların veya telefon konuşmalarının gizlice dinlenmesidir.

2.3. Siber Saldırılara İlişkin İstatistiksel Veriler

Siber saldırılar konusunda birçok veri ve istatistik yayınlanmaktadır. Çalışmada bu istatistiklerinden bazılarına yer verilmektedir.

En çok meydana gelen siber saldırı çeşitlerinden birisi de kimlik hırsızlığıdır. 2016 yılında tüm dünyada meydana gelen kimlik hırsızlığı vakalarına ait istatistiksel verileri içeren grafik aşağıda gösterilmektedir.



Grafik-1: Ülkelere Göre 2016 Yılında Kimlik Hırsızlığı Sayıları

Kaynak: Symantec, 2017: 50'den uyarlanmıştır.

Yapılan çalışmalarda görüldüğü üzere, dünya genelinde en çok, Amerika Birleşik Devletlerindeki kişilerin kimlikleri çalınmaktadır. Symantec'in yayınladığı güvenlik raporuna göre 2016 yılında A.B.D.'de yaklaşık 791 milyon kimlik hırsızlığı vakası meydana gelmiştir. Sıralamada, Amerika'yı Fransa ve Rusya takip etmektedir.

Steve Morgan tarafından Forbes'da yayınlanan bir makalede 2016 yılında siber güvenlik konusunda yayınlanan bütün raporlar incelenmiştir. 2016 yılı için elde edilen istatistikler şu şekildedir (Morgan, 2016):

- AT&T Siber Güvenlik Raporu'na göre, bilgisayar korsanlarının saldırıları sonucu, Nesnelerin İnterneti bağlantılarındaki güvenlik açığı sayısında %458 oranında artış meydana gelmiştir.
- Cisco Yıllık Güvenlik Raporu'na göre, internet sitelerinin güvenlik ihlallerinde %221 oranında artış meydana gelmiştir.
- Dell Yıllık Güvenlik Raporu'na göre, kötü amaçlı yazılım sayısı yaklaşık iki katına çıkarak yaklaşık 8 milyara ulaşmıştır.
- Google Android Güvenlik Raporu'na göre, günlük 6 milyardan fazla uygulama ve 400 milyondan fazla cihaz tehditlere karşı kontrol edilmektedir.
- IBM X-Force Siber Güvenlik Endeksi Raporu'na göre, sağlık endüstrisi dünyada en hızlı siber saldırıya uğrayan sektördür. Bunu finansal hizmetler ve üretim sektörü takip etmektedir.
- McAfee Labs Tehdit Tahminleri Raporu'na göre, 2016 yılında otomobil sistemlerine yapılan siber saldırıların hızla artacağı öngörülmektedir.
- Symantec İnternet Güvenlik Tehdit Raporu'na göre çalışanları hedef alan kimlik hırsızlığı girişimleri geçen yıla göre %55 oranında artış göstermiştir.
- Verizon Veri İhlal Araştırma Raporu'na göre, bütün siber saldırıların %89'u finansal çıkar ve casusluk için yapılmaktadır.

3. SİBER GÜVENLİK DENETİMLERİ

Siber güvenlik denetimlerinin kapsamı ve hangi güvenlik ve kontrol noktalarından oluştuğu, Bilgi Sistemleri Denetimi ve Kontrol Kurumu (ISACA) tarafından yayınlanan raporda şu şekilde belirlenmektedir (ISACA: 1):

Siber güvenlik denetimleri için birincil güvenlik ve kontrol konuları (ISACA: 1):

- Hassas verilerin ve fikri mülkiyet haklarının korunması,
- Çoklu bilgi kaynağının bağlı olduğu ağların korunması,
- Cihazların ve bu cihazların içerdiği bilgilerin sorumluluğu ve hesap verebilirliğidir.

Siber güvenlik denetiminin kapsamı ise (ISACA: 1):

- Şebeke, veritabanı ve uygulamalara ilişkin veri güvenliği politikaları,
- Veri kaybı önleme tedbirleri,
- Uygulanan etkili ağ erişim denetimleri,
- Dağıtılan algılama / önleme sistemleri,
- Güvenlik kontrolleri (fiziksel ve mantıksal),
- Olaylara müdahale programlarıdır.

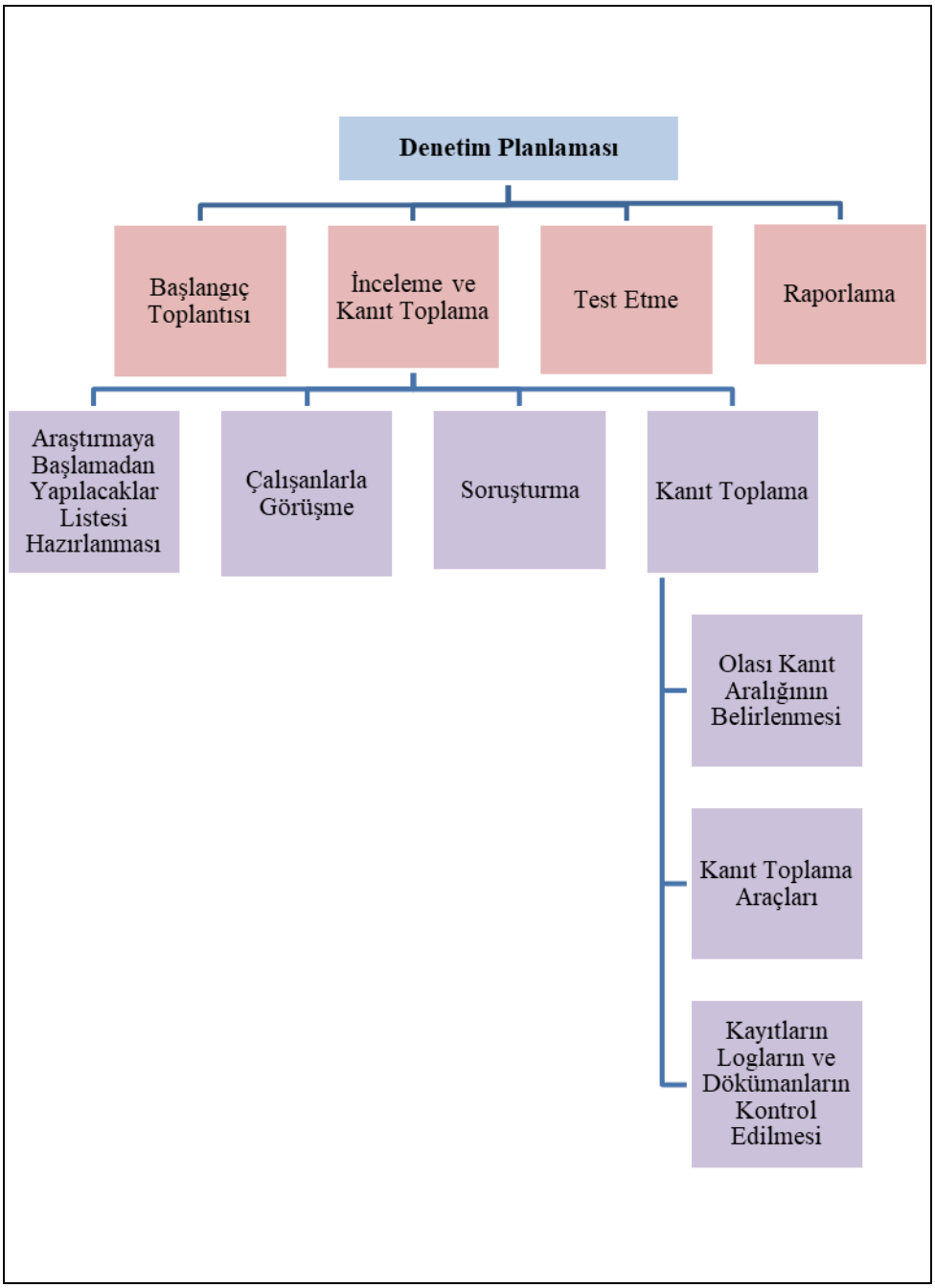
Siber güvenliğin amacı bilgi ve bilgi sistemlerinin korunmasıdır. Siber güvenlik kontrolleri aşağıdaki konuları bünyesinde barındırmaktadır (City of Vancouver, 2016: s.1).

- Çalışanların güvenliği,
- Fiziksel ve çevresel güvenlik,
- Hesapların ve şifrelerin yönetimi,
- Hassas verilerin gizliliği,
- İşletme sürekliliği yönetimi,
- Güvenlik konusunda bilinçlilik ve eğitim,
- Vaka yönetimi,
- Erişim kontrolleri,
- Varlık yönetimi,
- Değişim yönetimi,
- Uygunluk,
- Gizlilik ilkeleri,
- Sistemler ve verilerin korunması,
- Sigorta işlemleridir.

Siber güvenlik denetimlerinde gerçekleştirilecek öncelikli aşama denetim planlamasının yapılmasıdır. Denetim planlaması, yapılacak denetimin etkililiğini ve verimliliğini önemli ölçüde etkilemekte ve denetim sonuçlarına olumlu yönde katkı sağlamaktadır.

Siber suçların soruşturmasında, denetim planlaması, suçun oluştuğu yere gelinmeden önce gerekli tüm hazırlıkların yapıldığı ortamda, tasarlanan bir yöntem veya araçla gerçekleştirilmektedir. Yapılan hazırlıklarda, denetim ekibi, suçla ilişkili olarak sistemin geçmişi ve suçun kendisi hakkında en iyi bilgiyi elde etmek için kuruluşa ya da kişiye sorulması gereken her türlü soruları toplamaktadır. Soruşturma ekibi, siber suçun gerçekleşmesinin asıl sebebine ulaşmak için hazırlık aşamasında atılması gereken adımları planlamakta ve denetim ekibi denetim için kullanılacak tüm araçları hazırlamaktadır. Planlama faaliyetleri araştırmacıların kontrolü altında olmayan düzenlemeler, mevzuat ve diğer dış kaynaklardan etkilenmektedir. Planlama faaliyetleri ayrıca geri izlemeye ve daha fazla yetkilendirme ihtiyacına da neden olabilmektedir (Poonia 2014: s.16-17).

Siber güvenliğe ilişkin olarak yapılacak denetim planlamasının aşamaları ve gerçekleştirilecek faaliyetler, aşağıdaki şekil yardımıyla gösterilmektedir. Şekilde görüldüğü üzere, denetim planlamasına başlarken bir toplantı gerçekleştirilmekte, daha sonra ise yapılacak incelemeler için kanıtlar toplanmakta, ardından uygulanacak testler neticesinde raporlama yapılmaktadır. Denetim planlamasında incelemeler ve kanıt toplanması önemli bir yer tutmaktadır. Dolayısıyla denetim ekibi gerekli alt yapının tesis edilmesini sağlayarak planlamanın ve denetimin en iyi şekilde gerçekleştirilmesini sağlamalıdır.



Şekil-1: Siber Saldırılar ve Denetim Planlaması

Kaynak: Poonia, 2014: 17'den uyarlanmıştır.

Siber güvenlik denetiminin planlamasının ardından, denetimin nasıl gerçekleştirileceği ile ilgili önemli noktaların ve konuların belirlenmesi gerekmektedir. Denetimlerde kontrollerin nasıl uygulanacağı, kontroller ve

denetimler için bilgi sistemlerine yönelik tehdit unsuru taşıyan iç ve dış etkenler ile denetimlerin hangi ortamlarda gerçekleştirileceği aşağıda yer alan tabloda detaylı bir biçimde açıklanmaktadır.

Tablo-1: Siber Güvenlik Denetimlerinin Anahtar Noktaları

KONTROLLER
Denetimin bir parçası, işletmelerin kontrolleri uyguladığından emin olunmasıdır. Siber saldırıları önleyici araçlar ve kontroller, ➠ **Güvenlik duvarları, anti virüs programları,** ➠ **Çalışanların şifreler hakkında eğitilmesi,** ➠ **Yedeklerin düzenli olarak alınması,** ➠ **Güvenlik programlarının düzenli olarak güncelleştirilmesi,** ➠ **Düzenli siber güvenlik denetimleridir.** İşletme, bu süreçleri iyi bir şekilde tasarladığından, doğru ve mümkün olduğunca güncel olarak yürüttüğünden emin olmalıdır. Siber güvenlik denetimleri her yıl işletme ihtiyaçlarına göre yapılmalıdır. Net beklentiler ve etkili iletişim perspektifinde belirli başlangıç ve bitiş tarihlerine sahip planlı faaliyetleri içermelidir.
TEHDİTLER
Kontroller mevcut değilse, iç ve dış tehditler; gizlilik, bütünlük ve kullanılabilirliği etkileme potansiyeline sahiptir. Yeni yasalar ve düzenlemeler veya verilerdeki artış işletmeler için tehdit oluşturabilmektedir. İnsani tehditler, dikkatsizlikten casusluğa kadar her şeyi barındırabilmektedir. Kötü amaçlı kodlar ve yazılımlar, yetkisiz erişim ile donanım ve yazılım hataları da dahil ancak bunlarla sınırlı olmamak üzere bir dizi teknik tehdit bulunmaktadır.
VERİLERİN ORTAMI
İşletmenin bulut, mobil, Nesnelerin İnterneti (IoT), büyük veri veya güvenlik analitikleri üzerinde çalışıp çalışmadığına bağlı olarak tehditlerin miktarı veya önemi değişebilmektedir. Bilgiler yer değiştirdiğinde (örneğin, mobil ortamdan Nesnelerin İnternetine veya buluta geçerken), bilginin yeni konumuna hitap edebilmek için yeni kontrol ortamlarına ihtiyaç duyulacak ve bu yeni kontrol ortamları da hem güncellenmelere hem de denetimlere ihtiyaç duyacaktır.

Kaynak: ISACA: 1-2'den uyarlanmıştır.

Kontrollerin ve güvenlik sistemlerinin yeterli olmadığı durumlarda tehditler, parasal bir kazanç amaçlayan çevrelerden değil, politik çıkar sağlamayı

amaçlayan yada korsanlık yeteneklerini sergilemek isteyen kişilerden de gelebilmektedir. Aynı zamanda tehditler, çalışanlar veya sistemlere ulaşım sağlama hakkı olan diğer taraflar gibi işletme içerisindeki kaynaklardan da gelebilmektedir. Saldırılar, güvenlik duvarları ve diğer saldırı tespit sistemleri gibi işletmenin çevresel savunma sistemleri ile sınırlı değildir. Artık siber suçlular, işletmenin bilgisayar ağlarının birçok katmanındaki zaafları tespit edip bertaraf etme kabiliyetine sahip durumdadır (City of Vancouver, 2016: s.1).

Siber güvenlik denetimleri ve değerlendirme süreçleri, siber güvenliğin başarısına katkı sağlamaktadır. İç denetçiler ve risk yönetim uzmanları, işletme yönetimi ile birlikte denetimin yürütücüleri konumundadırlar (ISACA). Siber güvenlik denetimlerinin kimler tarafından idare edilip yürütüldüğüne ilişkin olarak detaylı bilgiler aşağıdaki tabloda gösterilmektedir:

Tablo-2: Siber Güvenlik Denetimlerinde Yürütücüler

Yönetim
Yönetim, işletme hakkında alınan risk kararlarının en son sahibidir. Bu nedenle, siber güvenlik kontrollerinin var olması ve etkin bir biçimde işletilmesi konusunda teşvik edici bir rol üstlenir. Risk yönetimi süreçlerinden edinilen klavuzlara dayanılarak kararlar, doğru bir şekilde alınabilmektedir.
Risk Yönetimi
Risk değerlendirmeleri genellikle işletmede bir güvenlik sorumlusunun rehberliğinde gerçekleştirilir ve işletme yönetimi risk yönetim süreçlerini işleterek kararlar vermektedir. Herhangi bir risk değerlendirmesinde iki temel amaç vardır. Risk düzeyinin netleşmesi ve kolay bir biçimde anlaşılabilmesi için, öncelikli olarak riskin durumu hakkında toplantı yaparak fikir birliğinin sağlanması çok önemlidir. En az ilki kadar önemli olmak üzere ikinci olarak, riskleri bertaraf etmenin yolları da belirlenmelidir. Bu, hem problemi hem de çözümü sağlar ve risklerin işletmeye olumsuz etki etmesini engeller. Siber güvenlik konusunda riskli alanlar sürekli değişmektedir. Tanımlanmış süreçlere, eğitilmiş ve yetenekli siber güvenlik kaynaklarına ve bir yönetim çerçevesine sahip olmak, işletmenin liderliği, etkili bir biçimde yönetilmesi ve ortaya çıkan tehditlerle mücadele edilebilmesi açısından son derece önemlidir.
İç Denetim
Bugünün küresel dijital ekonomisinde işletmeyi korumak kritk önem taşımaktadır. İç denetim departmanı birçok işletmede siber güvenlik

denetimleri konusunda çok önemli rol oynamaktadır. Aynı zamanda denetim kuruluna işletmenin yönetim kurulu seviyesinde bağımsız bir görüş bildirilmesi için çapraz raporlama ilişkisine sahiptir. Çapraz raporlamada yönetim kuruluna bilgilendirme yapılarak denetim kuruluna rapor verilmektedir. Denetim, kontrolleri objektif olarak değerlendirerek ve onları iyileştirmek için tavsiyelerde bulunarak ve üst yönetim ile yönetim kurulunun siber riskleri anlamasına ve bunlara tepki vermesine yardımcı olarak, siber tehditleri yönetme konusunda işletmeye katkı sağlamaktadır.

Kaynak: ISACA: 2'den uyarlanmıştır.

Siber güvenlik denetimlerinin yukarıdaki şekilde belirtilen yürütücüler tarafından uygulanabilmesi ve gerçekleştirilebilmesi için çeşitli araçlar ile teknik donanımsal ve yazılımsal ekipmanlara ihtiyaç duyulmaktadır.

Siber suçlara karşı uygulanan teknik denetim ve dokümantasyon araçları aşağıdaki gibidir (Poonia, 2014: s.17-20).

Siber Suçlara Karşı Uygulanan Teknik Denetim Araçları

- Veri Kurtarma Programları: Bilgisayarın hard diskinin zarar görmesi ya da silinmesi durumunda kullanılan yazılımlardır.
- Bal Küpleri: Bilgi sistemlerine karşı gerçekleştirilebilecek olan siber saldırıların tespit edilebilmesi için oluşturulmuş çok büyük bir ağın parçası olan tuzak sunuculardır.
- IP Adres Takip Sistemleri: Siber suçluların log kayıtlarının takip edilerek IP adreslerinin izlenmesidir.
- Sohbet Odalarının İzlenmesi: İnternet ortamında görüşme gerçekleştiren suçluların takip edilmesi için kullanılan bir araçtır (Poonia, 2014: 17-20).

Siber Suç Vakalarında Kullanılan Dokümantasyon Araçları

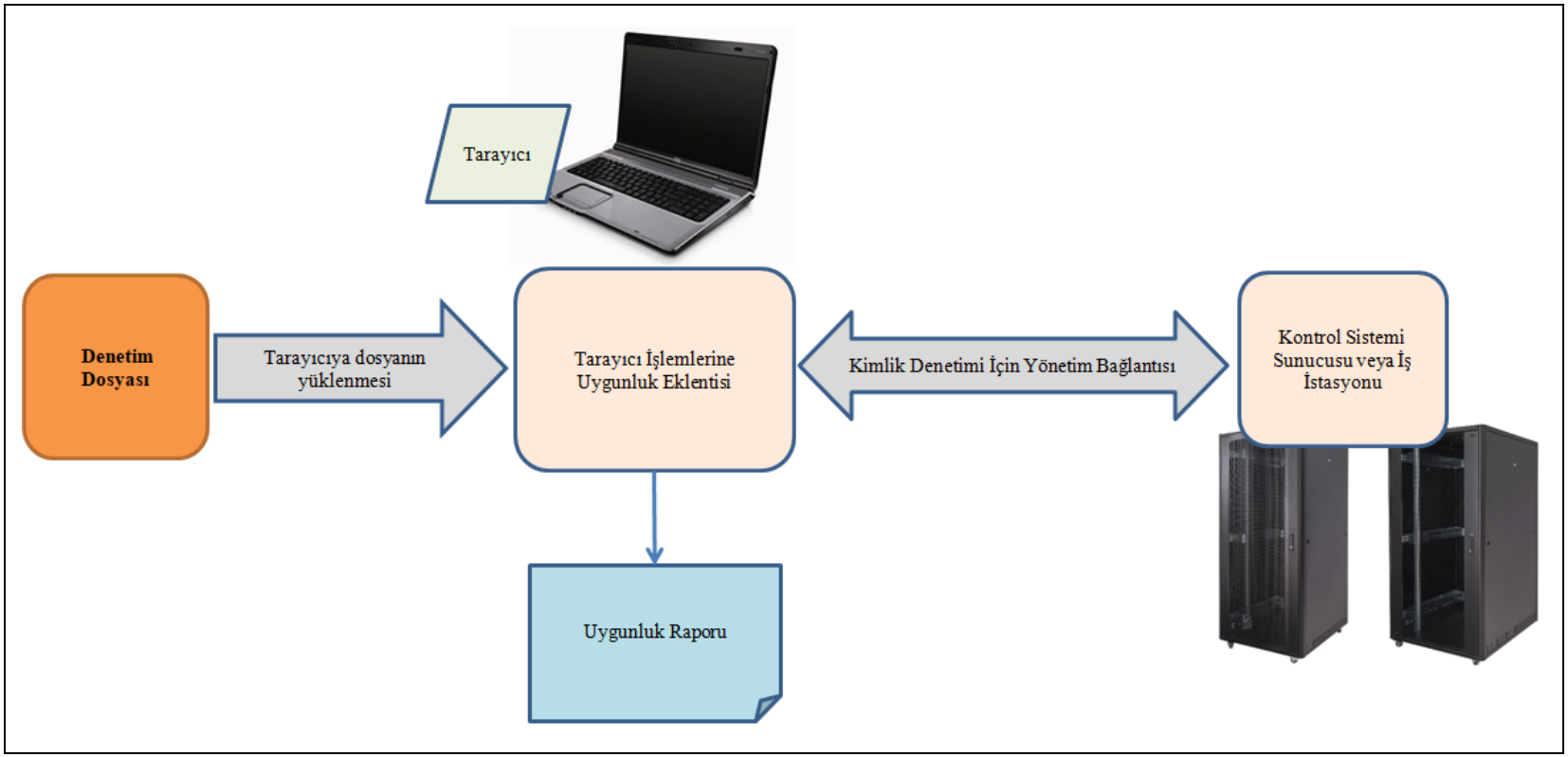
- Veri Akış Diyagramları: Bilgi sistemlerindeki veri işlemlerine ait süreçlerin diyagram olarak gösterimidir.
- Varlık İlişki Diyagramları: Örgütsel sistem unsurlarının birbirleriyle olan ilişkilerinin diyagram olarak ifade edilmesidir.
- Karar Ağaçları: Kararların ve olası sonuçlarının (olay çıktıları, kaynak maliyetleri ve yararlarının) ağaç şeklinde bir model veya grafik şeklinde ifade edilmesidir.

- Akış Şemaları: Bir algoritmayı veya işlemi temsil eden adımların akışlarının oklar ile ifade eden ve problemlerin adım adım çözümü için oluşturulan şemalardır.
- Veri Sözlükleri: Hangi verilerin hangi sistemlerde kullanıldığını ve bunların daha önce başka sistemlerde kullanılıp kullanılmadığını gösteren veri kalemleri toplamıdır (Poonia, 2014: 17-20).

ABD Enerji Bakanlığının gerçekleştirdiği bir çalışmadaki siber güvenlik denetimlerinde siber saldırıların tespitine yönelik olarak yapılan işlemlerde aşağıdaki araçlar kullanılmaktadır (U.S. Department of Energy Office of Electricity Delivery and Energy Reliability):

- **Güvenlik Zafiyeti Tarayıcısı:** Kontrol sistemi uygulaması seçimi, sistem verilerinin toplanması, denetim dosyalarının oluşturulması, sistemde dosyaların test edilmesi, dosyaların ve belgelerin güncellenmesi, benzer şekilde aynı formatta diğer dosyaların oluşturulması, bir denetim şablonun geliştirilmesi.
- **Laboratuar ve Saha Testleri:** Güvenlik verilerinin toplanması, verilerden güvenlik vakalarının tanımlanması ve siber saldırıları tespit edecek meta olayların geliştirilmesi, vaka tespit modülleri üzerine bu vakaların yazılması, modüllerin test edilmesi, diğer benzer olaylara kaynak oluşturması için kılavuzlar oluşturulması.
- **Güvenlik Vakaları Yönetimi:** Vaka tespit modülleri ve denetim dosyalarının Güvenlik Vakaları Yönetimine (Security Event Managers-SEM) entegre edilmesi, kontroller ve işletme bilgilerinden işletmenin Güvenlik Vakaları Yönetimi meta vakalarının tanımlanması, Güvenlik Vakaları Yönetimi ile testlerin gerçekleştirilmesidir.

Denetim araçları ile uygulanan denetime ait akış şeması ve raporlama süreci Peterson tarafından aşağıdaki şekilde ifade edilmektedir.



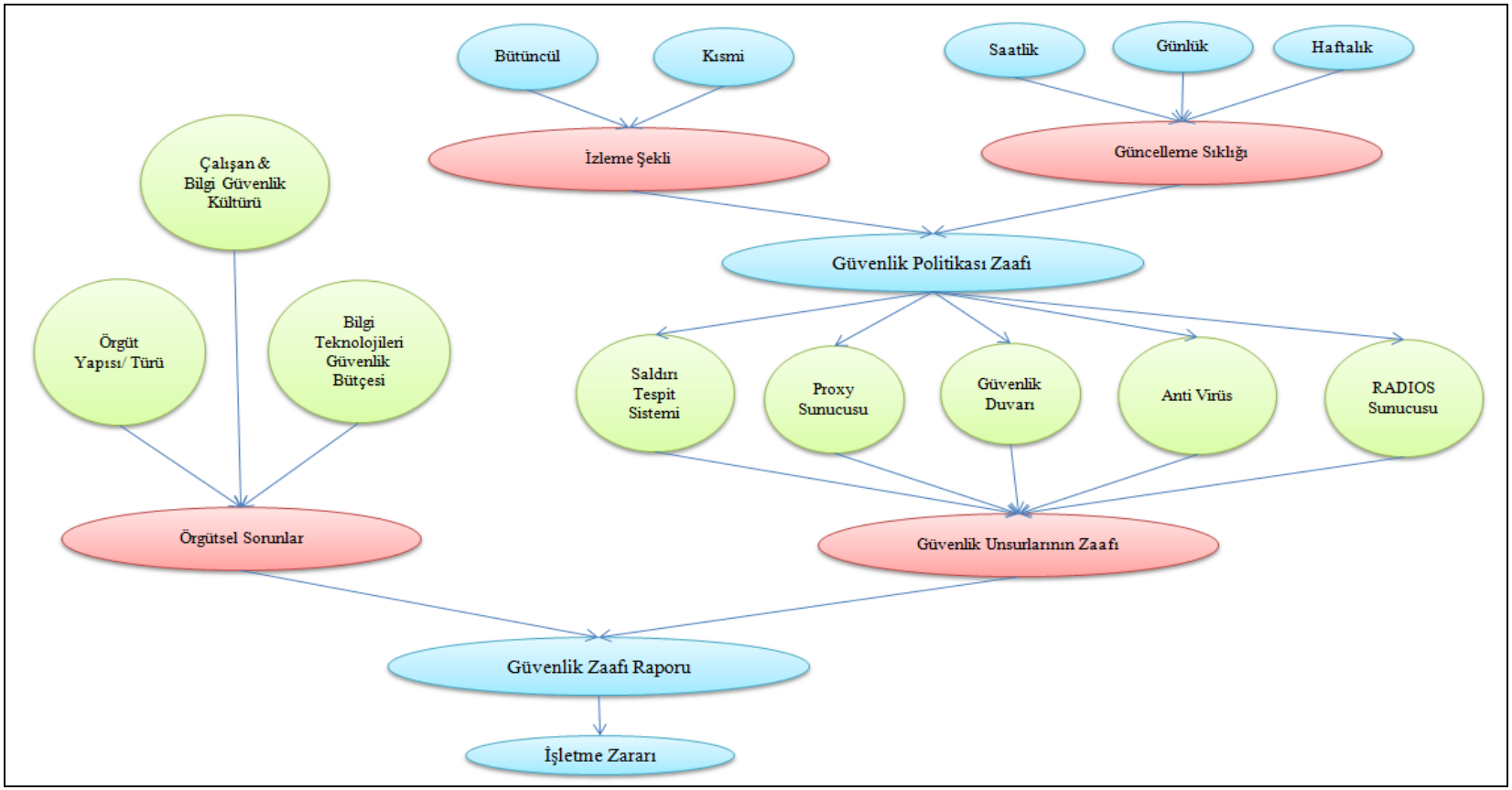
Şekil-2: Siber Güvenlik Denetim Araçları

Kaynak: Peterson, 2012: 6'dan uyarlanmıştır.

Yukarıdaki şekilde görüldüğü üzere, denetim dosyaları bir tarayıcı tarafından denetlenmektedir. Tarayıcının denetimi gerçekleştirilebilmesi için bir uygunluk eklentisinin tarayıcıya entegre edilmesi gerekmektedir. Uygunluk eklentisi, denetimlerin hangi kriterlere ve doğrulama kodlarına göre yapılacağını gösteren bir uygulamadır. Tarayıcının, kimlik denetimleri için iş istasyonu veya sunuculara bağlanması gerekmektedir. Denetlenecek dosya ve programların tarayıcı tarafından denetlenmesinin ardından bir uygunluk raporu oluşturularak denetim sonucu ilgili paydaşlara sunulmaktadır.

İşletmelerde siber saldırılara karşı yeterli güvenlik önlemi alınmaması veya kontrollerin ya da denetimlerin etkili bir biçimde yapılamaması sonucu çeşitli güvenlik zafiyetleri meydana gelebilmektedir. Güvenlik zaafı sonucunda ise işletmeler zararlara uğrayarak, kayıplar yaşayabilmektedirler. Mukhopadhyay ve diğerlerinin gerçekleştirdikleri bir çalışmada güvenlik problemlerinin nasıl ve ne şekilde oluştuğu ve işletme zararlarının hangi aşamalar sonucu meydana geldiği, aşağıdaki şekilde ifade edilmektedir.

Aşağıdaki şekilde yer aldığı üzere güvenlik zaafları, örgütsel sorunlar, izlemelerdeki aksaklıklar, güncellemelerde yaşanan problemler ile güvenlik unsurlarındaki eksiklikler neticesinde meydana gelmektedir. Güvenlik zafiyetinin oluşması durumunda güvenlik zaafı raporu oluşturulmakta ve süreç işletme zararı ile sonuçlanmaktadır. İşletmelerin zarar etmemesi ve güvenlik zaaflarının meydana gelmemesi için işletmede etkin bir güvenlik kültürü oluşturulmalı, izlemeler sistemin tamamını kapsayacak şekilde etkili bir biçimde yapılmalı, güncellemeler sürekli olarak gerçekleştirilmeli, denetim ekipmanları ve kontrol unsurları düzenli olarak takip edilerek meydana gelebilecek aksaklıklara engel olunmalıdır.



Şekil-3: Siber Güvenlik Zaafları ve Sonuçları

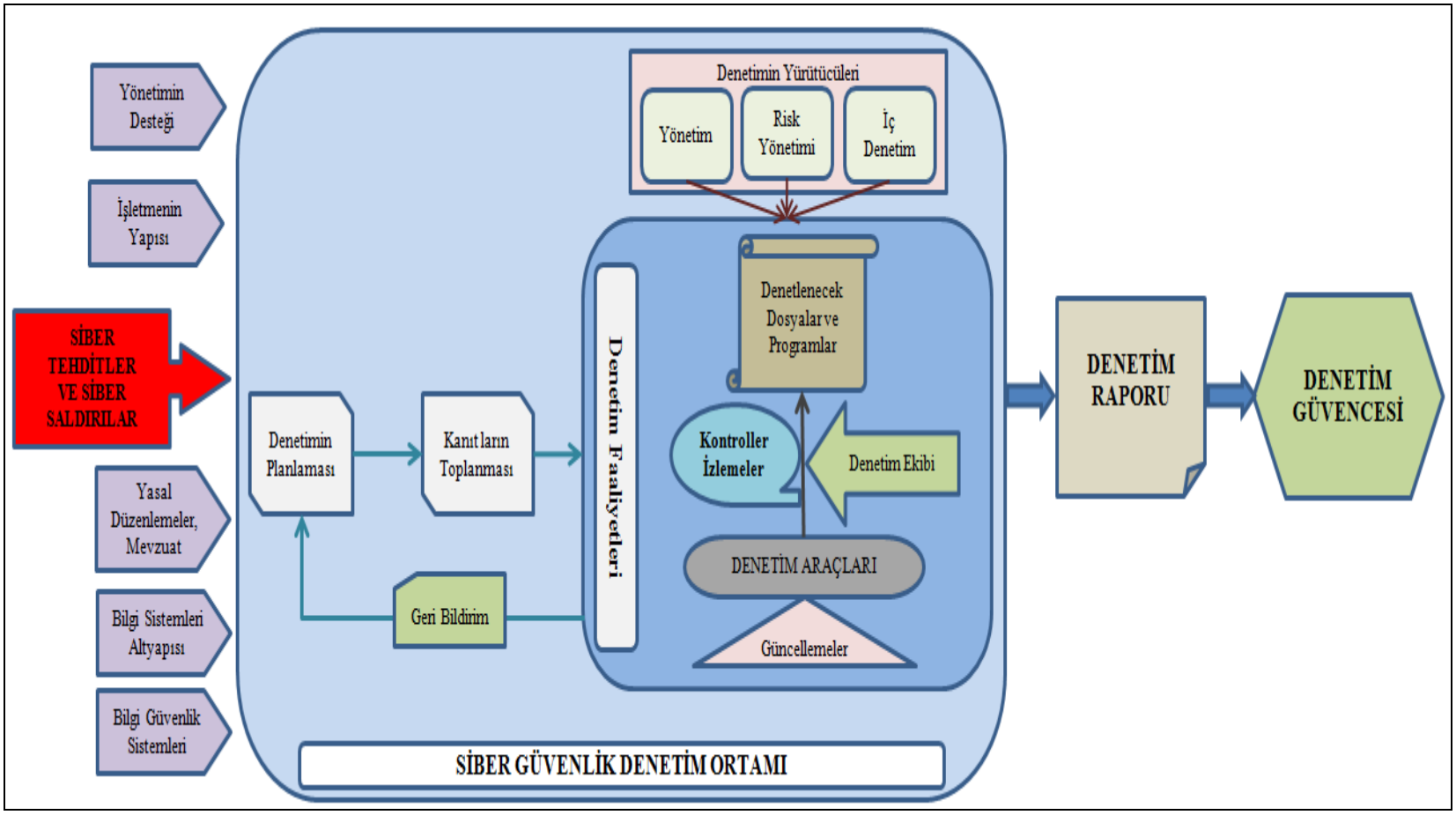
Kaynak: Mukhopadhyay vd., 2013: 15'den uyarlanmıştır.

4. SİBER GÜVENLİK DENETİM MODELİ ÖNERİSİ

Siber güvenlik denetimleri ile ilgili yapılan çalışmalar araştırıldığında, başlangıcından sonucuna kadar denetimi bütüncül şekilde ele alan bir çalışmanın gerçekleştirilmediği görülmektedir. Dolayısıyla bu çalışmada, literatürde yer alan konu ile ilgili olarak yapılan çalışmalardan yararlanılarak bütüncül bir model önerisi ortaya konulmaktadır. Modelde, siber güvenlik denetimlerine ait süreçlerin tamamını ele alan bütüncül bir yaklaşım kullanılarak, denetimin başlangıcından raporlanmasına kadar denetimde hangi işlemlerin gerçekleştirildiği özetlenmektedir.

Aşağıdaki şekilde yer alan modelde görüldüğü üzere, işletmelerin siber güvenliğine ve denetimlere birçok faktör etki etmektedir. En önemli etken siber tehditler ve siber saldırılardır. Ancak denetimleri etkileyen etmenler bunlarla sınırlı kalmamaktadır. Yönetimin desteği olmadan siber güvenlik denetimlerinin başarılı olması mümkün değildir. İşletme yönetimi, hem destek olma anlamında hem de denetimler için gerekli finansal bütçenin ayrılması anlamında, siber güvenlik denetimlerinde öncü olmalıdır. İşletmenin faaliyet alanı, yapısı, örgüt kültürü de siber güvenlik denetimlerinde etkili olmaktadır. Otomasyona, dijitalleşmeye ve bilgi teknolojilerine daha fazla önem gösteren işletmeler için siber güvenlik denetimleri, daha fazla önem arz etmektedir. Yasal düzenlemeler, işletme içinden ve işletme dışından kaynaklanan mevzuatlar, siber güvenliğe ve denetimlere önemli ölçüde etki edebilmektedir. Bilgi sistemlerinin altyapısı ve bilgi güvenlik sistemleri güçlü olan işletmeler siber güvenlikte daha fazla başarılı olmaktadır. Yapılacak denetimlerde kullanılan bilgi sistemlerinin ve araçların etkili, güncel, eksiksiz ve yeni olması son derece önemlidir.

Siber güvenlik denetimlerinde öncelikle planlamanın çok iyi bit şekilde yapılması gerekmektedir. Denetim planlamasında işletmenin durumu çok iyi analiz edilmeli ve karşı karşıya kalabileceği riskler iyi biçimde tespit edilmelidir. Planlamalar güncel olmalı ve sürekli olarak alınan geri bildirimler sayesinde bütün gelişmelere ayak uydurulabilmelidir. Planlamanın ardından siber saldırılara ilişkin kanıtlar toplanmalıdır. Kanıtların eksiksiz bir biçimde tam olarak toplanabilmesi denetimin başarısını etkilemektedir.



Şekil-4: Bütüncül Siber Güvenlik Denetim Modeli

Modelde belirtildiği üzere, siber güvenlik denetimlerindeki en önemli yürütücüler, işletme yönetimi, risk yönetim birimi ve iç denetim komitesidir. İşletme yönetimi denetimleri en üst düzeyde idare eden ve yöneten birim konumundadır. Risk yönetim birimi, işletmenin karşılaşabileceği siber risklerin ve denetim risklerinin analiz edilip yönetilmesinde önemli roller icra etmektedir. İç denetim birimi ise siber saldırılara karşı iç denetim mekanizmasının oluşturulmasında, güvenlik önlemlerinin alınmasında, siber güvenlik denetimlerinin icra edilmesinde ve yönetimle bağlantı kurulmasında anahtar rol üstlenmektedir.

Siber güvenlik denetim faaliyetleri denetim ekibinin kontrolünde sürekli güncellenen denetim araçları ile gerçekleştirilmektedir. Siber saldırıları tespit edebilen teknolojik sistemler, güvenlik duvarları, anti virüs programları, Proxyler, tarayıcılar, IP adres takip sistemleri, bal küpleri, kriptolama algoritmaları, şifreleme sistemleri ile kod çözme ve şifre çözme sistemleri gibi sistem, program ve yazılımlar, denetim araçlarına örnek teşkil etmektedir. Denetim ekibinde, bilgi teknolojileri ve siber güvenlik konusunda uzman olan kişiler görev yapmalıdır. Denetimlerin bilgi teknolojileri departmanı ile birlikte icra edilmesi daha çok başarı sağlayacaktır. Denetlenecek dosya yada programlar düzenli olarak izlenmeli ve kontroller sürekli olarak yapılmalıdır.

Siber güvenlik denetimleri neticesinde ulaşılan sonuçlar bir denetim raporu ile ilgililerle paylaşılmalıdır. Denetim raporu, denetlenecek bilgi, belge, dosya ve programların işletme tarafından belirlenen kriterler, standartlar, kurallar, ilkeler ve mevzuata uygunluğunun araştırılması sonucunda oluşturulmaktadır. Uygunluk konusunda sistemsel düzensizlikler ve zaafların meydana gelmesi durumunda güvenlik zafiyeti oluşmaktadır. Bu durum işletmenin çeşitli zararlara uğramasına neden olmaktadır. Yapılan siber güvenlik neticesinde belirlenen bir güven aralığında güvence verilmektedir. Siber güvenlik denetim güvencesi işletmenin siber güvenliği konusunda çok önemli veriler sunmaktadır. Denetim güvencesi ne kadar iyi olursa, işletmenin siber güvenlik politikalarının da o ölçüde etkili olduğu söylenebilir.

5. SONUÇ

Bilgi teknolojilerinin giderek yaygınlaşması sonucu işletmeler günümüzde birçok faaliyetlerini siber ortamda gerçekleştirmektedirler. Teknolojinin kullanımının artması avantajlar kadar bazı dezavantajları da beraberinde getirmektedir. Bu dezavantajlara en önemli örnekler ise siber tehditler ve siber saldırılardır.

Gerek kişilere gerekse işletmelere yönelik gerçekleştirilen siber saldırılar her yıl katlanarak artış göstermektedir. Siber saldırılara karşı uygulanacak en iyi yöntemler, siber güvenlik uygulamaları ve siber güvenlik denetimleridir. Siber güvenlik denetimleri yakın zamanda gündeme gelmeye başlamıştır. Akademik çalışmalarda ve yayınlanan raporlarda son zamanlarda ele alınan siber güvenlik denetimleri giderek önem kazanmaktadır. Yapılan çalışmalar siber güvenlik denetimlerinin belirli bölümleri üzerinde kısmi olarak gerçekleştirilmektedir. Dolayısıyla literatürde, siber güvenlik denetimlerinin tamamının bir süreç şeklinde incelenmesine yönelik bir eksiklik bulunmaktadır. Bu eksiklikten yola çıkılarak çalışmada, siber güvenliğin bir süreç olarak araştırılması amaçlanmıştır.

Çalışmada siber güvenlik denetimleri bütüncül bir biçimde ele alınarak bir model dâhilinde açıklanmaya çalışılmıştır. Önerilen modelde, öncelikle işletmelerin siber güvenliğine ve denetim ortamına etki eden iç ve dış faktörler, siber saldırılar ve tehditler açıklanmaktadır. Ardından, denetimin gerçekleştirilebilmesi için denetim planlamasının yapılması gerekliliği ortaya konulmaktadır. Planlama yapılırken siber güvenlik konusunda çok iyi bir risk analizinin yapılması son derece önemlidir. Denetim planlamasının sonrasında, denetimlerin objektif ve güvenilir bir biçimde yapılarak sağlıklı ve doğru sonuçlar verebilmesi için kanıt toplanması gerekmektedir. Gerçekleştirilecek denetim faaliyetleri işletme üst yönetimi, iç denetim ve risk yönetim birimi bünyesinde yürütülmektedir. Siber güvenlik denetimleri bilgi teknolojileri ve denetim konusunda uzman personel tarafından sürekli güncellenen denetim araçları ile yapılmaktadır. Programlar, antivirüs yazılımları, güvenlik duvarları, saldırı tespit sistemleri, Proxyler, tarayıcılar, yazılımsal ve donanımsal sistemler gibi denetim araçları denetimlerde kullanılırken, aynı zamanda meydana gelebilecek tehditlere ve risklere karşı işletmeyi koruma görevi üstlenmektedir. Yapılan denetimlerde izleme ve kontrol faaliyetleri de gerçekleştirilmektedir. Siber güvenlik denetimleri neticesinde bir denetim raporu oluşturulmaktadır. Bu raporda işletmenin siber güvenlik zaafları veya etkinliği yer almaktadır. Model önerisinin sonucunda ise siber güvenlik denetimlerinin en önemli kısımlarından birisi olan denetim güvencesi yer almaktadır. Yapılan denetim sonucu oluşan siber güvenlik denetim güvencesi, işletmenin siber güvenlik konusunda başarısını ortaya koyarken aynı zamanda dış paydaşlara karşı işletmenin güvenilirliği, imajı ve şeffaflığı ile denetimin doğruluğu, kalitesi ve objektifliği hakkında bilgi sunmaktadır.

Yapılan çalışma ile siber güvenlik denetimleri bir bütün olarak ele alındığı için denetim faaliyetleri daha iyi açıklanmakta ve anlaşılmakta ve literatüre katkı sağlanmaktadır. Yurtiçinde konu ile ilgili çok sayıda çalışma

olmamasından dolayı, gelecekte yapılacak çalışmalarda siber güvenlik denetimleri üzerinde daha fazla araştırma yapılabileceği öngörülmektedir.

KAYNAKÇA

AICPA. (2013). The top 5 cybercrimes, https://www.aicpa.org/content/dam/aicpa/interestareas/forensicandvaluation/resources/electronicdataanalysis/downloadabledocuments/top-5-cybercrimes.pdf.

City of Vancouver. (2016). Internal audit summary report. http://vancouver.ca/files/cov/internal-audit-cyber-security.pdf

Colbaugh, R. ve Glass, K. (2011). Proactive defense for evolving cyber threats. *IEEE International Conference on Intelligence and Security Informatics*, 10-12 Temmuz 2011, Beijing, China.

Gandhimathi, D. ve Prashanth, R. (2013). Cyber security and audit with password t-pro using encryption and decryption. *Proceedings of National Conference on New Horizons in IT - NCNHIT 2013*.

Greitzer, F.L., ve Frincke D.A. (2010). Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat mitigation. *Springer*, 85-113.

ISACA - Information Systems Audit and Control Association. Cyber security audit.

Kumar, V., Srivastava, J., ve Lazarevic, A. (2005). Managing cyber threats: issues, approaches, and challanges. *Springer*.

Milhorn, H.T. (2007). Cybercrime how to avoid becoming a victim. *Universal Publishers, Boca Raton, Florida*.

Morgan, S. (2016). Top 2016 Cybersecurity reports out from at&t, cisco, dell, google, ibm, mcafee, symantec and verizon. https://www.forbes.com/sites/stevemorgan/2016/05/09/top-2016-cybersecurity-reports-out-from-att-cisco-dell-google-ibm-mcafee-symantec-and-verizon/#3202dbbc1caf.

Mukhopadhyay A., Chatterjee S., Saha D., Mahanti A., ve Sadhukhan S.K. (2013). Cyber-risk decision models: to insure IT or not?. *Decision Support Systems*, 56, 11-26.

Ojeka, S.A., Ben-Caleb, E., Ekpe, Edara-Obong I. (2017). Cyber security in the nigerian banking sector: an appraisal of audit committee effectiveness. *International Review of Management and Marketing*. 7(2), 340-346.

Peterson, D. 2012. Cyber security audit and attack detection toolkit. *Digital Bond Inc.,* https://www.osti.gov/scitech/servlets/purl/1097617.

Poonia, A.S. (2014). Audit tools for cyber crime investigation. *International Journal of Enhanced Research in Science Technology & Engineering*, 3(12), 16-20.

Statista. (2015). Types of cyber crime in companies in germany 2015. https://www.statista.com/statistics/429635/cyber-crime-in-companies-germany/

Symantec. (2017). Internet security threat report. https://www.symantec.com/security-center/threat-report.

U.S. Department of Energy Office of Electricity Delivery and Energy Reliability. Cyber security audit and attack detection toolkit. https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/1-Attack_Detection_Toolkit.pdf.

Verma, A., ve Bajaj, S.K. (2008). Cyber fraud: a digital crime. *IADIS International Conference Information Systems*.