2nd International Vocational Science Symposium., IVSS 2018
2. Uluslararası Mesleki Bilimler Sempozyumu, IVSS 2018

http://www.meslekisempozyum.com

IVSS 2018

© Mesleki Bilimler Dergisi (MBD) & Ankara Üniversitesi

Received date; reviewed; accepted date

Bilişim Sistemlerine Yönelik Siber Saldırılar ve Siber Güvenliğin Sağlanması

Ebru YENİMAN YILDIRIM[1]

[1]Uludağ Üniversitesi, TBMYO, Bilgisayar Teknolojileri Bölümü,
yeniman@uludag.edu.tr

Özet: Dünyada bilgi ve iletişim teknolojilerinin hızla yaygınlaşması, internet kullanımının artması, bilgi depolanması ve iletilmesinin çoğalması sonucunda Siber Güvenlik ve Siber Saldırı kavramı hem ulusal güvenliğin hem de kurumların rekabet gücünün sağlanmasında önemli rol oynamaktadır.
Siber Güvenlik kavramıyla birlikte bilgisayar korsanlarının sürdürdüğü saldırılar kimi zaman kullanıcıları, kimi zaman da şirketleri ve devlet kurumlarını hedef alarak büyük zarara uğratmaktadır. Bu saldırılar genellikle fidye yazılımları, olta saldırıları, DDOS saldırıları, mobil tehditler vb. olarak karşımıza çıkmaktadır.
Son yıllarda Siber Saldırılar dolayısı ile ortaya çıkan zararlar kurumları ciddi olarak tehdit etmektedir. Siber Güvenlikle bilişim sistemlerinin Siber Saldırılardan korunması, işlenen bilgilerin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınması, Siber Saldırıların önceden tespit edilmesi ve bu tespitlere karşı önlemlerin alınması kurumlar için artık bir zorunluluktur.
Bu çalışma kapsamında, dünyadaki bazı ülkelerde farklı kurumlar tarafından hazırlanan Siber Güvenlik Raporları ve yapılan Siber Güvenlik anketleri incelenmiştir. Bu inceleme sonucunda siber tehditler ve bu konuda neler yapıldığı, güvenlik riskleri, güvenlik zafiyetleri analiz edilmiş, alınması gereken önlemler ve farkındalık konusunda önerilere makalede yer verilmiştir.

Anahtar Kelimeler: *Siber Güvenlik, Siber Saldırı, Siber Risk Yönetimi, Kapsamlı Güvenlik Stratejileri*

Cyber Attacks Directed Information Systems (IS) and Maintenance of Cyber Security

Abstract: The concept of cyber security and cyber attacks have been playing a critical role in the achievement of both national security and corporate competitiveness as a result of the increase of worldwide rapid spread in the field of information and communication technologies, data storage and data communication.
Hacker attacks have severely damaged sometimes computer users, sometimes companies and government institutions. These attacks have confronted us in the forms of ransomwares, phishings, DDOS attacks, mobile threats and etc.
Economic losses resulting from cyber attacks in recent years have been threating corporations severely. It is mandatory for corporations any longer to protect information systems through cyber security, secure the data confidentiality, integrity and accessibility, detect cyber attacks in advance and take counter measures against these attacks.
Within the scope of this study, Cyber Security Reports and Surveys prepared by various institutions in some countries are examined. As a result of this examination, cyber threats and practices, security risks and weaknesses are analyzed, the recommendations regarding compulsory measure and the security awareness are given in the article.

Keywords: *Cyber Security, Cyber Attack, Cyber Risk Management, Comprehensive Security Strategies*

DOI:

1. Giriş

Bilgi teknolojileri ilerledikçe bilgiye erişim imkanları artmakta ve dolayısıyla da bilginin güvenliğinin sağlanması zorlaşmaktadır. Günümüzde bilişim sistemlerinin hayatın her alanında kullanılmaya başlanması ile birlikte Siber Güvenlik tehditleri de artmıştır.
Türkiye İstatistik Kurumunun 19.09.2017 tarihinde yayınladığı Hanelerde Bilişim Teknolojileri Kullanımı Araştırması raporuna göre 16-74 yaş arası 2017 yılı toplam internet kullanımı oranı %66,8'dir. Hanelerde internet erişimi oranı ise %80,7'dir (TÜİK, 2017). Son 5 yıllık sürece baktığımızda (2013-2017) 2013 yılında toplam internet kullanımı oranı %48,9 ve internet erişimi oranı ise %49,1'dir (TÜİK, 2013). Bu sonuçlara göre bireysel internet kullanımı oranı son 5 yılda %17,9 ve toplam internet kullanımı oranı ise %31,6 artış göstermiştir. Bireysel olarak internete erişimin ve internet kullanımının artması Siber Güvenlik tehditlerini de beraberinde getirmiştir. Aynı şekilde kurumlarda bilişim teknolojileri kullanımı anketi oranlarına göre 2017 yılında kurumlarda bilgisayar kullanımı oranı %97,2 ve internet erişimi oranı ise %95,9'dur(TÜİK, 2017). Son 5 yıllık sürece baktığımızda 2013 yılında ~~bu oranlara göre~~ kurumlarda bilgisayar kullanımı oranı %92 ve internet erişimi oranı ise %90,8'dir (TÜİK, 2013). Bu sonuçlara göre son 5 yılda kurumlarda bilgisayar kullanımı oranı %5,2 ve internet erişimi oranı ise %5,1 artış göstermiştir. Kurumsal olarak, kurumların bilgisayar kullanımının ve internet erişiminin artması Siber Güvenlik tehditleri de arttırmıştır.
Ayrıca bilişim teknolojilerindeki son gelişmeler, gelişen global iletişim ağları, tüm nesnelerin ağlarla birbirine bağlanmasını hedefleyen nesnelerin interneti, bulut teknolojileri, mobil internetin yaygınlaşması ve cihazların yenilenmesi ile birlikte siber riskleri ve belirsizlikleri de beraberinde getirmiştir. Siber Güvenlik tehditleri bireyleri, kurumların bilgi ve iletişim sistemlerinde güvenlik zafiyetlerini her geçen gün arttırmaktadır. Bu durum sistemlerin çalışmamasına, ekonomik zarara ve siber güvenliğin tehlikeye girmesine neden olmaktadır. Kurumlar ve bireyler siber riskleri ancak gelişmiş risk yönetimi ve kapsamlı güvenlik stratejileri sayesinde önleyebilirler (Yıldırım, 2016). Çalışma kapsamında farklı kurumlar tarafından uygulanmış Siber Güvenlik Raporları ve anketleri incelenmiş ve Siber Güvenliğin sağlanması ve siber farkındalık konusunda önerilere yer verilmiştir.

2. Siber Güvenlik

Siber Güvenlik (SG), siber uzayı oluşturan bilgi teknolojileri sistemlerinin tehditlerden korunmasını, buradaki bilginin gizlilik, bütünlük ve erişilebilirliğinin güvenli bir şekilde sağlanmasını, saldırı ve siber durumların belirlenmesini, bu belirlemelere yönelik önlemlerin alınmasını ve sonrasında ~~ise~~ sistemlerde karşılaşılan sorunların Siber Güvenlik saldırısı öncesine geri getirilmesini anlatır (2016-2019 Ulusal Siber Güvenlik Stratejisi, 2018).
Büyük Siber Güvenlik ihlallerinin sıradan ve düzenli hale gelmiş olması tüm dünyada firmaların ve liderlerin dikkatini çekmektedir. Son yıllarda dünya çapındaki birçok kuruluş bu tür olaylara dikkat çekmekte, giderek karmaşıklaşan bir dijital toplumda ortaya çıkan siber riskleri anlamaya ve yönetmeye çalışmaktadır. Firmaların verilere ve verilerin birbirine bağlılıklarına olan ihtiyaç arttıkça, siber şoklara dayanmak için dayanıklılık geliştirmek çok önemli bir hale gelmektedir. Son yıllarda artan fidye saldırıları ve veri hırsızlığı, şirketlerin hem itibar hem de para kaybı yaşamasına sebep olmaktadır.
2013-2014 Ulusal Siber Güvenlik Stratejisi Eylem Planı 11. Maddede Siber Güvenlik riskleri konusunda SG ile ilgili kurumsal ve kişisel olarak yeterli bilinç seviyesine erişilmediği vurgulanmıştır. Ulusal siber güvenliğin sağlanması konusunda ise ilkeler 4. madde de SG sağlanmasında kişi, kurum, toplum ve devletin hukuki ve sosyal yükümlülüklerini yerine getirmesi gerektiği ifade edilmiştir (Yeniman Yıldırım ve Adalı, 2017).

2016-2019 Ulusal Siber Güvenlik Stratejisi Eylem Planındaki en önemli riskler ise: a) Sosyal ağlara bağımlılık, b) Kurumların siber uzaydaki pozisyonları, c) Siber casusluk faaliyetleri ve amaçlı saldırılar, ç) Personel, bilgi, beceri ve tecrübe konusunda yetersizlik, d) Kurumlar arası eşgüdüm noksanlığı, e) Siber uzayda farklı büyüklüklerde aktivite gösteren sektörlere ait ekonomik endişeler olarak sıralanmıştır (2016-2019 Ulusal Siber Güvenlik Stratejisi, 2018).

3. Siber Saldırılar

Bilgisayar ve internet konusunda profesyonel hacker veya hacker gruplarının kazanç sağlamak ve zarar vermek amacı ile kurumsal veya bireysel düzeyde web sitelerine, ağlara veya bilgisayarlara yaptıkları

saldırılara "Siber Saldırı" denir (Milliyet Gazetesi, 2017). Amerika Birleşik Devletleri Ulusal Araştırma Konseyinde 2009 yılında yapılan bir çalışmada Siber Saldırılar; "Ağlar, bilgisayar sistemleri veya bilgiyi ve bunlarda yerleşik olan ya da bunları taşıyan programları bozmak, aldatmak, küçük düşürmek veya yok etmek için yapılan kasıtlı hareketler" olarak tanımlanmıştır (Singer ve Friedman, 2015).
Günümüzde Siber Saldırılar siber guvenlik adına tehdit oluştururken bu tehditleri kurumsal ve bireysel daha kapsamlı anlamak ve farkında olmak büyük bir önem arz etmektedir. Kurumların ve bireylerin gelecek gerçek tehditleri fark etmeleri, hedefli saldırıların yöntem ve tekniklerinin daha geniş alanda nasıl olduğunu görmeleri tehditlere karşı koruyucu olacaktır (Miller, 2016).

DDOS (Distributed Denial of Service, Dağıtık Hizmet Engelleme) Saldırıları: Bu saldırılar bir bilgisayar aracılığıyla hedef olarak belirlenen bilgisayarın kullanılabilirliğini ortadan kaldırmaya yönelik gerçekleştirilir. Saldırı esnasında PC ve PC'nin kullandığı ağların olabildiğince yavaşlatılması ve kullanılamaz hale gelmesi amaçlanır. Aynı andan birden fazla PC ve bağlantı desteğiyle gerçekleştirildiği için kapsamı daha büyük zararlara neden olabilir. Engellemek için kurum içi güvenlik duvarlarından veya içerik filtrelerinden yararlanılmalıdır (Altundal, 2013). Bu saldırılarla;

- Site trafiğine yönelik yapılarak sitenin erişilebilirliği engellenir.
- Bant genişliğine yapılarak bağlantıda ciddi sorunlar yaratılabilir.
- Uygulamalar üzerinden kaynak bilgisayarın çalışması sonlandırılabilir.

Fidye Yazılımları: Şifreleyiciler ve kilitleyiciler olarak iki türdedir

- Bu tehlikeli yazılımlar ile bilgisayardaki bilgileri kilitlemekte ve dökümanların tekrar kurulumu için kişilerden her defasında para istemektedir. Fidye yazılımları genel olarak Windows ve Android cihazları hedef almaktadır.
- Günümüzde en yaygın ve en tehlikeli Siber Saldırı fidye yazılımı «WannaCRY» birçok büyük kurumun sistemine yayılmıştır. Bu yazılım, 'solucan' ismiyle anılan virüs aracılığıyla bilgisayarlara sızmaktadır. Bu zararlı yazılım, çoğunlukla menşei belli olmayan programlar, form siteleri, eposta, sahte oyunlar, disk vasıtasıyla bulaşmaktadır. "WannaCry" kurumların sistemlerine sızdığı an, zayıf makineleri belirlemekte ve kendi kendine bulaşmaktadır.
- Kurumlar kendilerini korumak için gerekli tedbirleri almalıdırlar.

Güvenlik duvarı oluşumu, antivirüs programları, dosya süzme uygulamaları, yetkisiz erişimleri belirleme yazılımları ve yazılımların devamlı güncellenmesi Siber Saldırıları önleyebilmektedir.

Phishing (Olta) Saldırıları:

- Olta Saldırıları, banka ve finans kuruluşları tarafından gönderilmiş görünen, çok önemli içeriğe sahipmiş gibi sanılan sahte elektronik postalardır.
- Gelen sahte elektronik postalardaki linklerle, kart şifreleri ve bilgileri, internet parolası ve kişisel veriler kişilere zarar vermek için kullanılabilir.

Korunmak için:

- Gelen elektronik posta'nın kimden geldiğinden ve gerçek olduğundan kesinlikle emin olmak gerekir.
- Bilmediğimiz kişi ya da kurumlardan gönderilen elektronik postaların içerisindeki linklerin tıklanmaması ve gelen dosyaların bilgisayara indirilmemesi gerekmektedir.
- Elektronik posta yoluyla veya farklı ortamlardada sunulan web sayfası linkleri kullanılmamalıdır.
- Erişmek istenilen web sayfalarının adreslerinin tarayıcının adres satırına yazılması gerekmektedir.

Son yıllarda Siber Saldırılar dolayısı ile ortaya çıkan zararlar kurumları ciddi olarak tehdit etmektedir. Siber Güvenlikle, bilişim sistemlerinin Siber Saldırılardan korunması, işlenen bilgilerin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınması, Siber Saldırıların önceden tespit edilmesi ve bu tespitlere karşı önlemlerin alınması kurumlar için artık bir zorunluluktur (Akyıldız, 2015).

4. Araştırma

4.1. Araştırmanın Amacı

Bu araştırmanın temel amacı, kurumların Siber Güvenlik konusundaki çalışmalarını tespit etmek, farkındalık düzeylerini ölçmek, Siber Saldırıların yol açtığı Siber Güvenlik risklerinin kurumlar üzerindeki etkisini değerlendirmek ve bu konuda neler yapılması gerektiği konusunda önerilerde bulunmaktır. Günümüzde bilgi ve iletişim teknolojilerinin hızlı bir şekilde gelişmesi ve internet'in yaygınlaşması ile birlikte güvenlik Siber Güvenlik riskleri de artmıştır. Bu nedenle kurumlarda siber güvenliğin sağlaması ve farkındalığın arttırılması ve gerekli önlemlerin alınmasının önemi vurgulanmıştır.

4.2. Araştırmanın Yöntemi

Bu çalışma kapsamında, dünyadaki bazı ülkelerde farklı güvenlik kurumları tarafından hazırlanan Siber Güvenlik anketleri incelenmiştir. Kurumlara Siber Güvenlik ve Siber Saldırılarla ilgili anket uygulaması yapılmıştır. Anket Siber Güvenlik ve Saldırılar konusunda alınması gereken önlemleri genel olarak ortaya koyacak niteliktedir. Anketlere ilişkin elde edilen veriler sayısal ve yüzdesel olarak değerlendirilip, yorumlanmıştır. Bu inceleme sonucunda siber tehditler ve bu konuda neler yapıldığı, güvenlik riskleri, güvenlik zafiyetleri analiz edilmiş, alınması gereken önlemler ve farkındalık konusunda önerilere yer verilmiştir.

4.3. Araştırmada Elde Edilen Bulgular

✓ Cyber Security Breaches Survey 2016'a göre, işletmelerin %69'unda siber güvenliğin kıdemli yöneticiler için yüksek öncelikli olduğunu, buna rağmen sadece %51'inin siber risklere karşı harekete geçtiğini, %29'unun resmi yazılı Siber Güvenlik politikalarına sahip olduğunu, %10'unun resmi siber kaza yönetim planının olduğunu söyleyebiliriz. 2015 yılında büyük firmaların %65'i Siber Güvenlik ihlal ve saldırılarılarına maruz kalmıştır. Bu firmaların %25'i ayda en az bir kez ihlal tecrübesi yaşamıştır. 2016 yılında firmaların en büyük Siber Güvenlik ihlal ve saldırılarının %68'i virüs, casus ve kötümcül yazılımlar, %32'si de başka kimliğe bürünmüş kurum içindeki kişilerden kaynaklanmaktadır. Firmaların %51'i hükümetin 10 adımda uygulamaya koyduğu Siber Güvenlik önlemlerinin 5 adımını uygulamaktadır. Firmaların %48'i hükümetin Siber Güvenlik temasına uygun teknik ölçüler kullanırken, %13'ünün tedarikçileri için kurdukları Siber Güvenlik standartları vardır. Firmaların %25'i orta ölçekte, %34'ü büyük firma niteliğindedir (Cyber Security Breaches Survey, 2016)

✓ PwC'nin "The Global State of Information Security Survey 2017" Global Bilgi Güvenliği Anketini geniş bir sektörel sektör yelpazesini kapsamakla birlikte, 10.000'i aşan bir katılım sağlanmıştır. Ankete katılan organizasyonların %48'inin geliri 500 milyon dolardır. Bu ankete göre firmaların önemsediği önemli bir konu, Mobil ve IoT'nin daha fazla kontrol gerektiren yeni düzenlemelere uyum sağlaması nedeniyle artan saldırı yüzeyinden kaynaklanan karmaşıklıktaki çarpıcı artıştır. Açıklığa kavuşan şeyler, güvenlik programlarının, çalışan eğitiminin, en yeni politikalar ve kontroller gibi temel konuların hazırlık ve esnekliğe yönelik kurumsal bir bağlılığa odaklanılması gerektiğidir (The Global State of Information Security Survey, 2017).

✓ EY'nin "EY Global Information Security Survey 2017-2018" göre ankete 1200 organizasyon katılmıştır. Ankete şirketlerin IT Uzmanları (CIO) ve Bilgi Güvenliği Baş Sorumluları (CISO)'ları katılmıştır. Bu kişilerin yanıtları analiz edilerek değerlendirilmiştir. Bu kuruluşların Siber Güvenlik konusunda güçlü ve zayıf yönleri tespit edilerek siber tehditlere yönelik neler yapılması gerektiği raporlanmıştır.

- Siber Güvenlik konusunda organizasyonların büyük çoğunluğu endişelidir. Organizasyonların çoğu 12 aydan daha fazla süredir risk altında olduklarını düşünmektedir. Siber saldırganlar sürekli organizasyonları tedirgin etmekte ve saldırılara devam etmektedir. Aynı zamanda organizasyonların yeni teknolojiler ile giderek daha fazla bağlantılı hale geliyor olması değer zincirinde fırsatlar yaratırken riskleri de beraberinde getirmiştir. Nesnelerin İnterneti (IoT) 'nin büyümesi ve birçok kuruluşun giderek daha büyük dijital ayak izi ile beslenen bu bağlantı patlaması, saldırganların istismar etmeleri için yeni güvenlik açıklarını getirmiştir. Bu nedenle işletmelerin kuruluşlarını bugün, yarın ve geleceğe dönük

büyütmelerine ve korumalarına yardımcı olmak için dijital açıdan değerlendirmeye ihtiyaçları vardır.

- Siber Saldırılar kamu ve özel sektöre, küçük ve büyük işletmelere rastgele veya yüksek hedefli olabilir. Organizasyonlar bunu iyi kamufle ederek, ortaya çıkan ataklar için savunma geliştirebilmelidir. Fakat organizasyonlar bunu her zaman başarılı bir şekilde yönetememektedirler.
- Aynı zamanda kurumlar için dijital çevrede çalışmak ve etkileşim kurmak çok zor değildir. Fakat her kuruluşun teknoloji altyapısı kendi içerisinde karmaşıktır. Kurumlar dijitalleşmeyle birlikte şirket bilgilerini bulutta tutabilmektedir. Aynı zamanda şirket çalışanlarının, müşterilerin ve tedarikçilerin (dizüstü bilgisayarlar, tabletler, cep telefonları vb.) ait cihazların çoğalması nedeniyle de kurumların Siber Güvenlik önlemleri alması gerekmektedir.
- Bu ankete göre kurumlar Siber Güvenlik harcamalarının arttığını belirtmişlerdir. Anket katılımcılarının %75'i Siber Güvenlik harcamalarının yıllık toplam bütçenin %25'ini aşabileceğini beyan etmiştir. Katılımcıların% 59'u son 12 ay içinde Siber Güvenlik harcama bütçelerinin arttığını, %87'si bütçenin %50'sinden daha fazla ihtiyaç olacağını, %12'si bütçenin %25'inden daha fazla ihtiyaç olacağını belirtmişlerdir. Kurumların yalnızca %4'ü mevcut Siber Güvenlik stratejilerini gözönünde bulundurdukları, siber tehditleri ve güvenlik açıklarını izlediklerini ifade etmişlerdir.
- Kurumlara yapılan yaygın siber ataklar: Bir web sitesinde serbestçe kullanılabilir istismar kiti kullanılarak istismar edilen güvenlik açığı, bir kimlik avı kampanyası yoluyla sunulan genel kötü amaçlı yazılımlar ve DDoS saldırılarıdır. İleri siber ataklar: Özel kötü amaçlı yazılımları kullanarak mızrak avı saldırıları, özel tasarlanmış istismar kodu kullanılarak güvenlik açıklarının istismar edilmesi, çalışanların casusluk yapması ve satıcı/tedarikçilerin hedef organizasyona kötü niyetli yaklaşımıdır.
- Ortaya çıkan ataklar: Verilere veya kontrol sistemlerine erişmek için "akıllı" cihazlardaki güvenlik açıkları ve kişisel ve kurumsal cihazların tek bir ağda bir araya getirilmesiyle oluşturulan güvenlik boşluklarıdır.
- Ankete katılanların maruz kaldığı risklerin en fazla arttığını düşündüğü savunmasızlıklar: dikkatsiz veya güvenliğin farkında olmayan çalışanlar, güncel olmayan bilgi güvenliği denetimleri veya mimarisi ve yetkisiz erişimdir. Ankete katılanların maruz kaldığı risklerin en fazla arttığını düşündüğü tehditler ise kimlik avı, IP veya veri çalmak için Siber Saldırılar, finansal bilgileri ele geçirmek için yapılan Siber Saldırılar ve iç saldırılardır.
- Ankette kurumlara yapılan ortak saldırı yöntemlerine karşı savunma konusunda katılımcıların %75'i kurumlarında güvenlik açığı tanımlamasının yetersiz olduğunu, %35'i veri koruma politikalarını geçici veya mevcut olmadığını, %12'sinin ihlal tespit programına sahip olmadığını, % 38'inin kimlik ve erişim programlarının olmadığını ifade etmişlerdir. Gelişmiş Siber Saldırılara karşı katılımcıların% 48'inin bir Güvenlik Operasyon Merkezi (SOC) yoktur, %57'sinin tehdit istihbarat programına sahip değildir veya resmi olmayan şekilde sahiptir. %12'si komplike bir Siber Saldırı olabileceğini tahmin ediyor. Çıkan Siber Saldırılara karşı katılımcıların %63'ü IT departmanının içerisinde raporlama yapan Siber Güvenlik işlevine sahiptir. %89'u Siber Güvenlik işlevinin kuruluşlarının ihtiyaçlarını tam olarak karşılamadığını, kurumların sadece %50'si kurul'a düzenli olarak rapor verdiğini ifade etmiştir. Kurulların %36'sı, kurumun karşı karşıya olduğu riskleri ve organizasyonun aldığı önlemleri tam olarak değerlendirmek için yeterli bilgi güvenliği bilgisine sahiptir. Ankete katılanların %43'ü, önemli bir saldırı durumunda mutabık kalınmış bir iletişim stratejisine veya planına sahip değildir (EY Global Information Security Survey, 2017-2018).

✓ Dünya ekonomik formunda belirtildiği üzere şu anda dünyada en büyük ölçekli beş en ciddi risklerden birisi Siber Güvenlik ihlalidir (Global Risks Report, 2017). Tehditler gittikçe artmaktadır ve 2021 yılında global Siber Güvenlik harcamaları 6 trilyon dolar olacağı tahmin edilmektedir (Cybercrime Report, 2017). Sadece bu yıl İngiltere'de, WannaCry fidye saldırısı saldırısı Ulusal Sağlık Hizmetinin (NHS) önemli bir bölümünü etkilemiştir (Investigation: WannaCry cyber attack and the NHS Report, 2017). Fransa'da, Emmanuel'in Cumhurbaşkanlığı kampanyasının ihlali, siber tehditler dolayısıyla seçimleri kaosa sürüklemiştir (Financial Times, 2017). Amerika'da Yahoo 3 milyon kullanıcısının hesabını ihlal ettiğini ve riske attığını açıkladı (The New York Times, 2017).

✓ PwC'nin "The Global State of Information Security Survey 2018" GSISS Global Bilgi Güvenliği Anketi PwC, CIO ve CSO tarafından doldurulan dünya çapında bir anket çalışmasıdır. Ankete

şirketlerin IT Uzmanları (CIO) ve Bilgi Güvenliği Baş Sorumluları (CISO)'ları katılmıştır. CIO ve CSO okuyucuları ve dünya çapındaki PwC müşterileri ankete katılmak üzere e-posta yoluyla davet edilmiştir. Bu raporda ele alınan sonuçlar, 122'den fazla ülkeden, 9.500'ün üzerinde CEO'nun, CFO'nun, CIO'nun, CISO'ların, STK'ların, VP'lerin ve IT yöneticilerinin ve güvenlik uygulamalarının yanıtlarına dayanmaktadır. Ankete katılanların %37'si Kuzey Amerika, %29'u Avrupa, %18'i Asya Pasifik, %14'ü Güney Amerika ve % 1'i Orta Doğu ve Afrika'dır.

- Birçok kurumun dijital risklerini değerlendirmeye ve dijital risk ve bunları önlemeye yönelik çalışmalar yapmaya ihtiyacı vardır. Ancak bu farkındalığa rağmen, Siber Saldırı riski olan pek çok şirket Siber Saldırılara karşı hazırlıksız yakalanmaktadır. 2018 GSISS tarafından araştırılan 122 ülkedeki 9.500 yöneticinin %44'ü genel bir bilgi güvenliği stratejisine sahip olmadığını ifade etmiştir. %48'i de çalışanların güvenlik farkındalığı eğitimi programlarının olmadığını ve % 54'ünün bir kaza-cevap süreci olmadığını söylemiştir (The Global State of Information Security Survey, 2018).
- Dünya çapında birçok ülke özellikle Japonya, Amerika Birleşik Devletleri, Almanya, İngiltere ve Güney Kore diğer ülkelerden gelen Siber Saldırılardan endişe duymaktadır (Global Attitudes Survey 2017). Dünya çapında Siber Saldırıların yürütülmesi için araçlar artmaktadır. ABD Ulusal Güvenlik Ajansı (NSA) saldırı araçlarının sızdırması, kötü niyetli bilgisayar korsanlarına karşı son derece gelişmiş yetenekler geliştirmiştir. Siber Saldırıların meydana gelmesi durumunda, çoğu mağdur şirket, suçluları açıkça tanımlayamadıklarını söylemektedir. 2018 GSISS'imizde, ankete katılanların yalnızca % 39'u Siber Saldırıların öznitelik yetenekleri konusunda çok emin olduklarını ifade etmişlerdir (The Global State of Information Security Survey, 2018).
- Güvensiz İnternet aygıtlarının (IoT) cihazlarının artan üretimi, yaygın Siber Güvenlik açıkları yaratmaktadır (The Global State of Information Security Survey, 2017). Veri bütünlüğüne yönelik artan tehditler, güvenilen sistemleri zayıflatabilir ve kritik altyapıya zarar vererek fiziksel zarara neden olabilir. Birleşmiş Milletlerin (BM) 2017 Küresel Siber Güvenlik Endeksi'ne göre, hem bölgeler içinde hem de bölgeler arasında dünya çapında Siber Güvenlik hazırlığı konusunda büyük bir eşitsizlik vardır. (The report ranked Singapore, the United States, Malaysia, Oman, Estonia, Mauritius, Australia, France, Georgia, and Canada as the most committed member states). BM, üye devletlerin sadece % 38'inin yayınlanmış bir Siber Güvenlik stratejisine sahip olduğunu tespit etmiştir. %11'i bağımsız bir stratejiye sahiptir. Sadece % 12'sinde gelişme Siber Güvenlik stratejisi vardır. Üye devletlerin% 61'i ulusal sorumluluğa sahip bir acil müdahale ekibine sahip olsa da, devletlerin sadece % 21'i Siber Güvenlik kazaları için metrikler yayınlamaktadır.
- 2018 GSISS'de, genel bir Siber Güvenlik stratejisine sahip olan kuruluşların sıklığının özellikle Japonya'da (%72), Siber Saldırıların ulusal güvenlik tehdidi olarak görüldüğü (Global Attitudes Survey, 2017) ve Malezya'nın (%74) oldukça yüksek olduğu görülmektedir. BM Siber Güvenlik endeksine göre, Doğu Asya ve Pasifik, Dünya Ekonomik Forumu'nun Siber Saldırıların ilk beş işletme riski arasında olduğu bir bölgedir (Global Risks Report, 2017).
- Liderler siber esnekliği geliştirmek için daha fazla sorumluluk üstlenmelidirler. Özel sektörde, iş sonuçlarına yol açanlar, iş yapma ile ilgili risklerden sorumlu tutulmalıdırlar. Kurullar etkin gözetim ve proaktif risk yönetimi kullanmalıdırlar. İş sürekliliği, planlama, stratejik uyum ve veri analizi için stratejiler kilit öneme sahiptir. Bununla birlikte, 2018 GSISS, şirket yönetim kurullarının çoğunun kendi şirketlerinin güvenlik stratejilerini veya yatırım planlarını proaktif olarak şekillendirmediğini tespit etmiştir (The Global State of Information Security Survey, 2018).
- GSISS katılımcılarının sadece% 44'ü şirket kurullarının şirketlerinin genel güvenlik stratejisine aktif olarak katıldığını ifade etmiştir. "National Association of Corporate Directors' 2016-2017" anketlerine göre, az sayıdaki yönetim kurulu üyeleri şirketlerinin Siber Saldırılara karşı güvenli bir şekilde güvence altına alındığından emin olduklarını belirtmişlerdir. Çoğu zaman, kurulların güvenlik önlemlerine katılmamalarının bir sonucu olarak, bu tür bir şüphe sürpriz olmamalıdır. Katılımcıların yarısının riskin güvenlik harcamalarını etkilediğine katılıyor. GSISS katılımcılarının çoğu (%66), kuruluşlarının güvenlik harcamalarının her bir iş kolunun gelirleriyle uyumlu olduğunu belirtmektedir, ancak geri kalanı (%34) durumun böyle olmadığını veya emin olmadıklarını söylemektedirler. Baş güvenlik görevlisi (CISO) giderek daha önemli hale gelmektedir. 2018 GSISS'ye göre, bir şirketin CISO'su ya da baş güvenlik

görevlisinin doğrudan CEO ya da yönetim kuruluna daha fazla bilgi vermesi daha yaygındır. Siber Güvenlik yöneticileri, pek çok kuruluşta halen bulunmamaktadır. Katılımcıların sadece yaklaşık yarısı %52'si kurumlarının bir CISO kullandığını; %45'i bir baş güvenlik görevlisi kullanacaklarını ve %47'si iç iş operasyonlarını desteklemek için özel güvenlik personeli çalıştırdıklarını ifade etmiştir. Katılımcıların %34'ü kuruluşlarının iş ekosistemindeki IoT siber risklerini değerlendirmeyi planladıklarını ifade etmiştir. Birçok kurum siber riskleri daha proaktif olarak yönetebilmelidir. Katılımcıların yarısı kurumlarının Siber Güvenlikle ilgili arka plan kontrolleri yaptığını söylemiştir. Siber tehditlere karşı Penetrasyon testleri, bilgi güvenliğinin aktif olarak izlenmesi, istihbarat ve savunmasızlık değerlendirmeleri dahil olmak üzere iş sistemlerinde siber risklerin ortaya çıkarılması için önemli süreçlerdir. Ankete katılanların yarısından azı tarafından bu durum benimsenmiştir (The Global State of Information Security Survey, 2018).

✓ Kaspersky'nin Business Advantage danışmanlığında hazırladığı "The State of Industrial Cybersecurity 2017"anketi kurumların Siber Güvenlik tutumlarını anlamak ve kuruluşları etkileyen Siber Güvenlik konularını tespit etmek amacıyla kurumların güvenlik danışmanları ve uzmanlarına uygulanmıştır. Dünya genelinde 21 ülkede 359 kişiye ulaşılmıştır. Şirketlerin %56'sı üretici, % 19'u inşaat ve mühendislik, %11'i petrol ve gaz olmuştur. Geriye kalan % 14'ü kamu hizmetleri ve enerji, hükümet veya kamu sektörü, gayrimenkul, eğlence ve savunmadan oluşmaktadır (The State of Industrial Cybersecurity, 2017).

- Ankete göre kurumlarda endüstriyel siber risklerin ve Siber Güvenlik konularının sürekli olarak gerçekleştiği tespit edilmiştir. Şirketlerin yarısından fazlası son 12 ayda en az bir siber olay yaşamıştır. Rapor edilen mali ortalama yıllık kümulatif zararın 347.603$ olduğu görülmektedir. 500 + çalışanı olan büyük şirketler, yıllık 497,097 $ 'lık kümulatif zarar rapor etmektedir. Bu büyük şirketlerin çoğunluğu (% 71) son 12 ayda 2 ve 5 Siber Güvenlik olayları yaşadıklarını bildirmiştir.
- Genel olarak güvenlik uzmanları, sektörlerindeki Siber Güvenlik tehditlerinin farkındadırlar, ancak belirli tehlikeleri her zaman iyi bilmemektedirler ya da bu sorunlarla nasıl başa çıkılacağına dair net planları yoktur. Çalışma yapılan dört şirketten üçü Siber Güvenlik konusunda bir olay yaşanacağını beklemektedir. Ayrıca büyük şirketler daha fazla risk altındadır. Risk yapısı çeşitli endüstriler ve farklı derecelerde farklılıklar göstermektedir. Çoğu kuruluş %83'ü bu riskleri yönetmeye hazır olsa da, siber güvenliğine yönelik mevcut genel yaklaşım karmaşık olduğundan dolayı bazı şirketler, güvenlik çözümleri kurduklarını belirttikleri halde, çoğunun süreçleri işletme risklerini yönetmek için etkili olma olasılığı düşük görünmektedir. Ayrıca, Siber Güvenlik olaylarının çok az rapor edilmesi durumunu söz konusudur. Beş işletmeden sadece birinin güvenlik ihlallerini rapor ettiği görülmektedir. Kurumlarda endüstriyel Siber Güvenlik bilincini yükseltmek için çalışan işgücü önemlidir. Bu, Siber Güvenlik uzmanlarının eğitimini içerir. Endüstriyel iş gücünün tüm düzeylerinde genel endüstriyel Siber Güvenlik bilincini arttırmak gerekmektedir.
- Siber Güvenlik uzmanları sürekli olarak endüstriyel ortamların yeterince iyi korunmadığını ifade etmişlerdir. Güvenlik uzmanlarının tecrübeleri ve tarafsız görüşlerine dayanarak, şirketlerin genellikle siber risklerin etkisini hafife aldığını ancak bir ihlalden sonra gerçek güvenlik önlemlerine yatırım yaptığını söyleyebiliriz. Ayrıca kurumlar genellikle dışarıdan gelen güvenlik açıklarından kaynaklanan olayları beklemekte, altyapı ve ortak kuruluş ağlarından gelen potansiyel tehditler için yeterince önlem almamaktadır.
- Şirketlerin %54'ü son 12 ayda Siber Güvenlik saldırısı yaşamıştır. %17'si bir kez, %21'i iki kez, %12'si üç-beş kez, %3'ü 6-10 kez ve %1'i 11-25 kez saldırıya uğramıştır. Gerçekleşmiş Siber Güvenlik tehditleri: kötümcül yazılımlar, 3. parti tedarik zinciri partnerlerinden gelen tehditler, sabotaj yada kasıtlı diğer dışsal zararlar, fidye saldırıları, hedefli saldırılar, çalışan hataları ve kasıtlı olmayan hareketler, sabotaj ve diğer kasıtlı içsel zararlar, endüstriyel yazılım hataları ve donanım hatalarıdır. Gerçek kazaların çoğunluğu %53'ü geleneksel kötümcül yazılım ve virüs olaylarından kaynaklanmıştır. Anket katılımcılarının en büyük endişelerinden birisi de budur. Hedefli saldırılar aslında sistemlere yönelik en büyük ikinci tehditti ve şirketlerin üçte birinden fazlasında %36'sı siber olaylara neden oldu. Çalışan hatası, tüm olayların üçüncü en büyük nedeni %29 iken algılamalar arasındaki boşluğu belirten altıncı en büyük endişe olarak değerlendirilmiştir. Veriler, hedefe yönelik saldırıların sayısının yüksek olduğunu ve kuruluşların kendi işindeki güvenlik sorunları tehdidini hafife almaması gerektiğini, özellikle

de tehditlerin PC'ye bir USB çubuğu takılarak kontrol sistemlerini enfekte etmesiyle ortaya çıkabileceğini gösteriyor.

- Dört şirketten üçü (%74) bir Siber Güvenlik saldırısının gerçekleşmesini bekliyor. İşletmelerin çoğunluğu (%83), ortamlarında böyle bir olayla mücadele etmeye hazır olduklarını düşünmektedir: %86'sı onaylanmış ve belgelendirilmiş bir endüstriyel Siber Güvenlik politikasına veya programına sahip olduğunu iddia etmiştir. Buna rağmen, kurumların henüz tam olarak hazırlanmadığına dair bir gösterge vardır; personelin Siber Güvenlik ihlalleri konusunda farkında olmadıkları tespit edilmiştir. Kurumların siber güvenliğin potansiyel zayıflıklarını ve risklerini nasıl belirleyebileceklerini daha iyi anlamaları için prosedürlerini test etmeye ve değerlendirmeye ihtiyaçları vardır. Bu sorunları tasarlanmış düzenli testler yaparak gidermek ve güvenlik açıklarını tanımlamak gelecekteki olayların önlenmesine yardımcı olacaktır. Çoğu kurum, Siber Saldırılarla mücadele için gerekli olan potansiyel etkili önlemler hakkında iyi bir fikir sahibi olmasına rağmen geçen yıl kurumların %55'inin bir olayla karşılaştığı göz önüne alındığında, kabul edilen tedbirlerin yeterince güçlü olmadıkları ya da uygulamalarında bir sorun olduğu varsayılabilir (The State of Industrial Cybersecurity, 2017).
- Kurumlar, Siber Güvenlik ihlalleriyle mücadele etmek için "kötümcül amaçlı yazılım önleme" çözümlerini endüstriyel bir ortam için en etkili önlem olarak görmektedir. Ankete katılan kurumların üçte ikisinden fazlası bu önlemleri kullanmaktadır. Ayrıca kurumların %62'si personeli için özel güvenlik farkındalığı eğitimi aldırmış ve ağlarına uzaktan ve kablosuz erişim üzerinde kontrollerini arttırmıştır. Kurumların %55'inin "izinsiz giriş tespiti", %50'si "tek yönlü ağ geçiti", %48'inin "güvenlik açığı taraması ve yama yönetimi" kullandığı görülmektedir. Yama ve güncelleme sıklığına baktığımızda kurumların %32'si her hafta, %27'si iki haftada bir, %26'sı her ay, %13'ü her birkaç ayda bir, %2'si her altı ayda bir yapmaktadır.
- Ankete katılan kurumların %38'i bulut tabanlı kontrol çözümü SCADA'yı kullanmaktadır. Kurumların bunu uygulamaya geçirmesi ve yerleştirilmesi zaman alacağı düşünülmektedir. SCADA'nın kablosuz bağlantı üzerinden kullanımı, şirketlerin daha dikkatli olmaları gerektiğini de vurgulamaktadır.
- Ankete katılan kurumlar siber güvenliği yönetme zorlukları olduğunu ifade etmişlerdir. Bunlar, %50'si Siber Güvenlik çalışanlarını doğru becerilerle işe almak, %43'ü kurumsal IT ile ara bağlantıyı arttırmak, %39'unun varlık sahipleri ve operatörler arasında güvenlik farkındalığının olmaması, %35'i Siber Güvenlik ortamı / endüstriyel ağın karmaşıklığı, %48'i Siber Güvenlik çözümünü uygulayabilen güvenilir ortaklar, %32'si uygun ürün / hizmetlerin olmaması, %31'inin siber güvenliğin üst düzey yönetim için düşük öncelikli olması ve %22'sinin bütçe eksikliği önceliklidir. Siber Güvenlik ihlali raporlaması önemli olmasına rağmen kurumlar tarafından marka itibarını korumak için herhangi bir siber olayda raporlama tercih edilmemektedir. Ankete katılan kurumların %81'i raporlamanın gerekli olmadığını, %19'u ise gerekli olduğunu bildirmiştir (The State of Industrial Cybersecurity, 2017).
- Kurumların Siber Güvenlik ihlali için onaylanmış Siber Güvenlik politikaları olamalıdır. Siber Güvenlik kontrol/denetimini gerçekleştiren bir dizi güvenlik önlemi alınmalıdır. Kontrol ağları ve kontrol sistemleri ile diğer ağ çalıştırma güvenlik açığı taramaları arasında tek yönlü bir ağ geçidi kurularak her iki haftada bir tarama ve güncelleme işlemleri yapılmalıdır.

✓ Bursa şehrinde mevcut olan toplam kayıtlı 5000 işletmeden rassal yöntemle seçilen Bursa Ticaret ve Sanayi odasına kayıtlı 150 küçük ve orta büyüklükteki işletmelere Bilgi Güvenliği konusunda (IT Müdürlerine) anket uygulanmıştır. Anket sonuçlarına göre kurumlarda güvenlik politikaları standartlara uygun olmadan yönetilmektedir. Birçok kurum ve kuruluş tarafından da bilgi güvenliği yönetiminin yeterli olduğuna inanılmaktadır. Bu durumun açıklığa kavuşturulması ve dünya genelinde kabul görmüş ve uygulanabilirliği test edilmiş bilgi güvenliği standartları esas alınarak kuruluşların "bilgi güvenliği yönetimi" konusunda eksikliklerini gidererek Bilgi Güvenliği Yönetim Sistemi (BGYS) kurmaları, uygulamaları ve belgelendirilmeleri gerekmektedir (Yeniman Yıldırım vd., 2011).

- BGYS standartlarının kurum ve kuruluşlara adapte edilmesi, çalışanların ve yöneticilerin eğitilmesi için kurumların içerisinde güvenlik uzmanları çalıştırmaları veya danışmanlık hizmetleri almaları gerekmektedir.
- Üst yönetim ve çalışanlar tarafından Siber Güvenlik politikalarının benimsenmesi ve uygulanması,

- Küçük ve orta ölçekli işletmelerde yılda en az 2-3 kez penetrasyon testlerinin yapılarak siber güvenliğin üst düzeye çıkarılması,
- Türkiye'deki şirketlerin bilgi güvenliğine yeterince önem vermediği,
- Kurumlarda Bilgi Güvenliği konusunda çalışan farkındalığının yetersiz olduğu,
- Kurumlarda İletişim ve Operasyon Yönetimi, Güvenlik Politikaları, Organizasyonel Güvenlik, Personel Güvenliği, Fiziksel ve Çevresel güvenlik, Erişim Kontrolü ve Sistem Geliştirme ve Bakım geliştirilmelidir (Yeniman Yıldırım vd., 2011)
- Kurumlarda siber güvenliğin sağlanmasında aşağıdaki durumlar dikkate alınmalıdır:
- Kurumlarda siber güvenliği sağlamanın canlı bir süreç olduğu ve devamlılık gerektirdiği,
- Kurumlarda siber güvenliğin yalnızca teknoloji ile değil aynı zamanda insan, eğitim ve teknoloji üçgeninde bir yaklaşımla dikkate alınması gerektiği,
- Uluslararası standartlarla uyumlu olarak çalışılması ve uygulanması gerektiği,
- Bilgi güvenliği standartları üst düzeyde güvenliği garanti etse bile bazen güvenlik standartlarının yetersiz olabileceği,
- Kurumlarda Siber Güvenlik seviyesinin son durumunun belirlenmesi için zaman zaman kurumların bağımsız uzman kuruluşlar tarafından denetlenmesi gerektiği,
- Kurumlarda siber güvenliğin yönetiminin zaruri bir proses olduğu ve her durumda iyileştirmelere gerek duyulacağı, kurumlarda en güvensiz olunacağı varsayımıyla hareket edilerek gerekli önlemlerin alınması gerektiği bilinmeli ve uygulanmalıdır (Vural ve Sağıroğlu, 2008).

5. Sonuç ve Değerlendirme

Uygulanan anketlerin ortak sonuçlarına göre;

- Kurumların yaklaşık %50'sinin genel bir bilgi güvenliği stratejisine sahip olmadığını ve önemli bir saldırı durumunda hazırlanmış bir iletişim stratejisine veya planına sahip olmadıkları görülmektedir.
- Çoğu kurum, Siber Saldırılarla mücadele için gerekli olan potansiyel etkili önlemler hakkında iyi bir fikir sahibi olmasına rağmen kurumların yarısı bir olayla karşılaştığı göz önüne alındığında, kabul edilen tedbirlerin yeterince güçlü olmadıkları ya da uygulamalarında bir sorun olduğu varsayılabilir.
- Kurumlarda siber risklerin en fazla artan tehditleri Ddos saldırıları, fidye yazılımları, kimlik avı, IP veya veri çalmak için ve finansal bilgileri ele geçirmek için yapılan Siber Saldırılardır.
- Anket yapılan pek çok kuruluşta Siber Güvenlik yöneticisi bulunmamaktadır. Herhangi bir ihlal durumunda acil Siber Güvenlik yöneticisinin olması siber risklerin önlenmesi konusunda destekleyici nitelikte olacaktır.
- Çalışma yapılan dört şirketten üçü Siber Güvenlik konusunda bir olay yaşanacağını beklemektedir.
- Ayrıca büyük şirketler daha fazla risk altındadır. Risk yapısı çeşitli endüstriler ve farklı derecelerde farklılıklar göstermektedir.
- Siber Güvenlik ihlali raporlaması önemli olmasına rağmen kurumlar tarafından marka itibarını korumak için herhangi bir siber olayda raporlama tercih edilmemektedir.
- Anket yapılan tüm kurumlar Siber Güvenlik harcamalarının arttığını belirtmişlerdir. Anket katılımcılarının yaklaşık %80'i Siber Güvenlik harcamalarının yıllık toplam bütçenin %25'ini aşabileceğini beyan etmişlerdir. Katılımcıların % 60'ı son 12 ay içinde Siber Güvenlik harcama bütçelerinin arttığını vurgulamışlardır.
- Kurumlarda çalışanların yaklaşık %65'i Siber Güvenlik konusunda yeterli bilgiye sahip değildirler. Bu nedenle kurumlarda Siber Güvenlik konusunda farkındalık çalışmalarının yapılması ve çalışanların siber riskler konusunda bilinç düzeylerinin arttırılması gerekmektedir.

6. Kaynakça

Akyıldız, M. A., (2015), Uygulamalarla Siber Güvenliğe Giriş, Gazi Yayınevi, ss.585, ISBN:9786053442745, Turkey.

Altundal Ö.F., (2013), "DDoS nedir, ne değildir?", https://encokbilisimhukuku.wordpress.com/2013/04/16/ddos-saldirisi/ E.Tar:28.03.2018

Cyber Security Breaches Survey 2016, (2016), HM Government&Social Research Institute&University of Portsmouth,https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf, E.Tar: 02.04.2018

Cybercrime Report 2017, (2017), Cybersecurity Ventures, https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf, E.Tar: 05.04.2018

EY Global Information Security Survey Report 2017-2018, (2017-2018), Ernst & Young, https://www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2017-18, E.Tar: 03.04.2018

Financial Times, (2017), "Hackers hit Macron campaign with 'massive' attack,", https://www.ft.com/content/79341cc4-3233-11e7-bce4-9023f8c0fd2e, E.Tar: 05.04.2018

Global Risks Report 2017 (2017), World Economic Forum, http://www3.weforum.org/docs/GRR17_Report_web.pdf, E.Tar: 05.04.2018

Global Attitudes Survey 2017, (2017), Pew Research Center, http://www.pewresearch.org/methodology/international-survey-research/international-methodology/global-attitudes-survey/indonesia/2017/, E.Tar: 29.03.2018

Investigation: WannaCry cyber attack and the NHS Report 2017, (2017), National Audit Office, https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf, E.Tar: 05.04.2018

Miller, K. L., (2016) , About Reasonable Cybersecurity: A Proactive and Adaptive Approach, The Florida Bar Journal, 90:22, USA.

Milliyet Gazetesi, (2017), http://www.milliyet.com.tr/sibel-saldiri-nedir--teknoloji-haber-1991343/ E. Tarihi: 04.04.2018

New York Times, (2017), "All 3 billion Yahoo Accounts Were Affected by 2013 Attack", https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html, E.Tar: 06.04.2018

Singer, P.W., Friedman, A., (2015), Siber Güvenlik ve Savaş, Buzdağı Yayınları, Ankara, ss:182.

Ulusal Siber Guvenlik Stratejisi 2016 - 2019, (2018), http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf, E.Tar: 28.03.2018

The Global State of Information Security Survey 2017, (2017), PWC, https://www.pwc.com.tr/en/gsiss2017, E.Tar: 02.04.2018

The Global State of Information Security Survey 2018, (2018), PWC, https://www.pwc.com.tr/gsiss2018-en, E.Tar: 06.04.2018

The Global State of Information Security Survey 2017, Bold Steps to Manage Geopolitical Cyber Threats, (2017), PwC, https://www.pwc.com/gx/en/issues/assets/2017-gsisss-bold-steps-to-manage-geopolitical-threats-final.pdf, E.Tar: 29.03.2018

The Global State of Information Security Survey 2017, Uncovering the Potential of the Internet of Things, (2017), PwC, https://www.pwc.com/gx/en/issues/assets/pwc-GSISS-2017-uncovering-the-potential-of-iot.pdf, E.Tar: 26.03.2018

The State of Industrial Cybersecurity 2017, (2017), Kaspersky, https://go.kaspersky.com/rs/802-IJN-240/images/ICS%20WHITE%20PAPER.pdf, E.Tar: 25.03.2018

TUİK (2013), http://www.tuik.gov.tr/UstMenu.do?metod=temelist, E.Tar: 24.03.2018

TUİK (2017), http://www.tuik.gov.tr/PreIstatistikTablo.do?istab_id=41, E.Tar:24.03.2018

Ulusal Siber Güvenlik Stratejisi 2016-2019, (2016-2019), Ulaştırma ve Denizcilik Bakanlığı, http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf, E.Tar: 26.03.2018

Vural, Y., Sağıroğlu, Ş., (2008), Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme, Gazi Üniv. Müh. Mim. Fakültesi Dergisi, 23(2), 507-522.

Yeniman Yıldırım, E., Adalı, E., (2017), The Threats and Risks in Personal Data Security, 2017 International Conference on Computer Science and Engineering (UBMK), IEEE Xplor, Doi: 10.1109/UBMK.2017.8093478, 610-615, 5-8 Oct., Turkey.

Yeniman Yıldırım, E., Akalp, G., Aytaç, S., Bayram, N., (2011), Factors Influencing Information Security Management in Small and Medium-sized Enterprises: A Case Study from Turkey, International Journal of Information Management, 31(4):360-365, ISSN: 0268-4012, Doi: 10.1016/j.ijinfomgt.2010.10.006, USA.

Yildirim, E., (2016), Advances in Human Factors in Cybersecurity, The Importance of Information Security Awareness for the Success of Business Enterprises, 501:211-222, ISBN: 978-3-319-41931-2, Doi: 10.1007/978-3-319-41932-9_17, Springer, USA.