IJMSIT

International Journal of Multidisciplinary Studies and Innovative Technologies

Volume : 1
Number: 1
Year: 2017
Pages: 24 - 28

Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi†

Fulya ASLAY[1*]

[1]*Bilgisayar Mühendisliği/Mühendislik Fakültesi, Erzincan Üniversitesi, Türkiye*
[*]*(faslay@erzincan.edu.tr)*

Özet **–**Bilişim teknolojilerinin hızlı gelişimi sayesinde artan bilgisayar ve Internet kullanımı hayatın vazgeçilmez bir unsuru haline gelmiştir. Bilişim ve internetin dünyada bir anda yaygınlaşması kullanıcılara bir yandan kolaylık ve özgürlük tanırken, öte yandan oluşan güvenlik açıkları sebebiyle sistemlerin kötüye kullanılmasına sebep olmaktadır. Sistemlerden kaynaklanan bu güvenlik açıkları kişileri etkilerken kimi zaman da kişisel ölçekte alınmayan tedbirlerden dolayı sistemler de tehdit altında kalmaktadır. Nesnelerin Internet'i (Internet of Things, IoT) kavramı ile internete bağlanan cihaz sayısının da çok daha artması ve bu cihazların insanların hayatına dâhil olmasıyla güvenlik ihlallerine maruz kalma riskinin de aynı doğrultuda artacağı düşünülmektedir. Birbiriyle bağlantılı donanım, yazılım, sistem ve insanların iletişim ve/veya etkileşimde bulundukları soyut veya somut alanı tarif eden siber uzay içerisinde alınan güvenlik tedbirlerinden özellikle son kullanıcının da haberinin olması ve bu konuda farkındalığının sağlanması giderek önem kazanmaktadır. Günümüzde çok çeşitli siber saldırı yöntemleri bulunmakta olup çalışmada bu siber saldırıları yöntemleri incelenerek, Türkiye'de siber güvenlik durum analizi yapılmaktadır.

Anahtar Kelimeler – Siber Güvenlik, Siber Saldırı Yöntemleri, Siber Uzay, Bilişim Sistemleri, Güvenlik

Siber Attack Methods and Current Situation Analysis of Turkey's Ciber Safety

Abstract **–**Computer and internet use that has increased by means of the rapid development of information technologies has become an essential component of life. Sudden spreading of information and internet across the world provides convenience and freedom to users on one hand, but leads to the misuse of systems due to security flaws on the other. These security flaws that are caused by systems not only affect individuals, but also threaten systems due to the failure of taking precautions on an individual scale from time to time. It is thought that as a result of the increase of the number of devices connected to internet thanks to the concept of Internet of Things (IoT) and involvement of these devices in people's lives; the risk of being exposed to security violations will increase in the same direction. The fact that security precautions taken within the cyber space that describes intangible or tangible areas where interconnected hardwares, softwares, systems and individuals communicate and/or interact are also known especially by end-users and an awareness is provided on this issue becomes more and more important. Today, there are various methods of cyber attacks and in this study these methods of cyber attacks are examined and situation analysis of cyber security in Turkey is carried out.

Keywords – Cyber Security, Cyber Attack Methods, Cyber Space, Cyber Force, Information Systems, Security

I. GİRİŞ

Günümüzde kişisel ve kurumsal anlamada vazgeçilmez bir unsur haline gelen bilgisayarların ilk önce haberleşme, şifreleme ve şifre çözme amaçlı olarak geliştirildiği daha sonra ise kullanımının giderek arttığı bilinmektedir. Internet ise 1960lı yıllarda ABD savunma bakanlığı tarafından olası bir savaş durumunda askeri iletişimin zarar görmeden kullanılmaya devam etmesi için bilgisayarlardaki verilerin başka bilgisayarlara aktarabilmesi amacıyla kurulan ARPANET ile ortaya çıkmıştır. Internet milyarlarca cihaz ile milyonlarca ağın birbirine bağlandığı ağların ağı olarak nitelendirilmektedir ve belirli protokoller çerçevesinde bilgi alışverişi yapılmasına imkân sağlamaktadır [20]. Internetin haberleşmeyi, bilgi alışverişini ve ayrıca bilgisayar kullanıcıları arasında bağlantıyı sağlaması nedeniyle tüm dünyada kullanımı hızla yaygınlaşmıştır [3]. Bilişim teknolojilerinin hızlı gelişimi sayesinde artan Internet kullanımı; kamuda, özel sektörde ve hatta kişisel ölçekte hayatın vazgeçilmez bir unsuru haline gelmiştir [17]. Bilişim ve internetin dünyada bir anda yaygınlaşması kullanıcılara bir yandan sınırsız özgürlük tanırken, öbür yandan da oluşan güvenlik açıkları sebebiyle bilişim sistemlerinin kötüye kullanılmasına ve bu anlamda bir suç işleme mekanizması haline gelmesine sebep olmaktadır [3].

Dijital pazarlama ajansı We Are Social ve Hootsuite işbirliği ile hazırlanan "Digital in 2017 Global Overview" raporuna göre dünya genelinde 3.77 milyarı bulan global internet kullanıcı sayısı %50'lik bir penetrasyona eşittir. Türkiye'de ise yaklaşık 80 Milyon nüfusun 48 milyonu internet kullanmaktadır [4]. Türkiye'nin 2008 yılında 6 milyon internet kullanıcısının olduğu bilinmekte olup bu sayının yaklaşık 10 yılda 8 kat arttığı görülmektedir. Yakın gelecekte bu sayının

† This is an extended version of a conference paper (ISMSIT2017).

daha da artacağı tahmin edilmektedir. Nesnelerin Internet'i (Internet of Things, IoT) kavramı ile internete bağlanan cihaz sayısının da çok daha artması ve bu cihazların insanların hayatına dâhil olmasıyla güvenlik ihlallerine maruz kalma riskinin de aynı doğrultuda artacağı düşünülmektedir [1]. Bu sebeple güvenlik önlemlerinin alınması ve bu alana daha fazla yatırım yapılması gerekmektedir.

II. SİBER GÜVENLİK

Siber, bilgisayar ve ağlarını içeren kavram ya da varlıkları tanımlamak için kullanılır. Siber alan (cyber space) kelimesi de birbiriyle bağlantılı system, yazılım, donanım ve insanların iletişim ve/veya etkileşimde bulundukları soyut veya somut alanı tarif etmek için kullanılmaktadır [15]. Siber Saldırı ise "hedef seçilen şahıs, şirket, kurum, örgüt ve devlet gibi yapıların bilgi ve iletim sistemlerine ve kritik altyapılarına yapılan planlı ve koordineli saldırılar" şeklinde tanımlanmıştır [11].

İlk olarak 1990'lı yıllarda bilgisayar mühendisleri tarafından, ağa bağlı bilgisayarlarla ilgili güvenlik sorunlarını ifade etmek için siber güvenlik terimi kullanılmıştır [10] ve daha çok bilişim sistemlerinin temel malzemesi olan bilgi üzerinden bu tanım yapılmaktadır. Buna göre siber âlemin güvenli olabilmesi için bilgi güvenliği yönetim sistemi standardında olduğu gibi bilginin gizliliğinin (confidentiality), bütünlüğünün (intergrity) ve erişilebilirliğinin (availability) sağlanması gerekmektedir. Bilginin sadece erişim yetkisi verilen kişiler tarafından kullanılması onun gizliliğidir. Bu erişim yazılı bir bilginin okunması yada bilişim sistemlerinde saklanan bilginin sadece yetkili kişilerce görüntülenebilmesi gibi erişimlerdir. Hassas bilgilerin varlığından bile sadece yetkililer haberdar olmalıdır. Bilginin bütünlüğü ise o bilginin değiştirilmemiş, kısmen yada tamamının silinmemiş olmasıdır. Erişilebilirlik, saklanan bilginin gerektiğinde yetkisi olan kişiler tarafından erişilebilir olmasıdır [12].

Siber tehditler artık sadece bilgisayar sistemlerine verdikleri zararlar (sistemlere sızma, sistemlerden bilgi çalma ve sistemlere asılsız bilgi koyma) ile sınırlı kalmamaktadır. Bir ülkenin kritik olarak kabul edilebilecek haberleşme sistemlerine, bilgisayar sistemlerine, enerji ve ulaşım ağlarına, askeri komuta ve kontrol sistemlerine zarar verecek ölçüde, asimetrik bir harp çeşidi olarak ortaya çıkmaktadır. Siber tehditlerin önümüzdeki yıllarda da önemli tehditlerden biri olacağı düşüncesi; tüm dünya tarafından kabul edilmeye başlanmıştır [1]. Bu sebeple daha etkin savunma sistemlerinin inşa edilmesi, acil durum hazırlıklarının oluşturulması çok önemlidir. Saldırıların, gerçekleştiği anda hemen tespit edilmesi, sanal ya da fiziksel bariyer inşa edilmesi, bölgesel ve ulusal anlamda siber güvenlik politikalarının geliştirilmesi zorunlu hale gelmiştir [22]. Ayrıca siber güvenlik ile ilgili farkındalık oluşturmak çok önemlidir. Son zamanlarda yeni ortaya çıkmaya başlayan "Siber Güvenlik Durumsal Farkındalık" ile ilgili çalışmalar bu ihtiyaca hitap etmekte ve çalışmalarda artış olması beklenmektedir [24].

Ülkeler, güvenli bir siber ortam sağlayabilme yolunda, siber ortamın parçası olan bileşenleri siber saldırılara karşı korumak, yapılan saldırılara müdahale etmek, saldıranları cezalandırmak, gerekli yasal mevzuatı oluşturmak ve bütün faaliyetleri yerine getirecek yapıları tesis etmek üzere siber ortama yönelik politika ve stratejiler geliştirmiş ve geliştirmeye devam etmektedir [7].

NATO Liderleri 2016 yılında yaptıkları Varşova Zirvesi'nde siber savunmaya kaynak sağlamaya öncelik verdiklerini vurgulayarak 2015 yılında aylık yaklaşık 500 saldırı olayı ile karşılaşırken bu sayının 2016 yılında %60 oranında arttığına dikkat çekip, durumun ciddiyetini ortaya koymuşlardır [16]. NATO üyesi ülkelerden birisinin kritik altyapılarına karşı gerçekleştirilecek bir siber saldırının diğer ülkeleri de ilgilendiren sonuçları olabileceği, bu nedenle üye ülkelerin siber savunma imkân ve kabiliyetlerinin artırılmasının önemi de vurgulanmaktadır [25]. Günümüzde teknoloji çok gelişmiş olmasına ragmen bir saldırının ne zaman yapılabileceğini tahmin etmek mümkün değildir. II. Dünya Savaşı yıllarında bir füzenin fırlatılması için 20 dakika gibi bir süre kullanılırken günümüzde siber saldırılar ışık hızında gerçekleşmektedir. Bu nedenle siber saldırılara anında karşılık vermek gerekmektedir [9]. Siber güvenlik tatbikatları sistemlerin açıklıklarının ortaya çıkarıp gereken tedbirlerin alınmasını sağlamak açısından oldukça önemlidir. Türkiye'de yapılan tatbikatların diğer ülkelerde yapılanlardan farkı ise gerçek saldırı ve savunma tekniklerinin kullanılmasıdır. Böylece siber güvenlik konusunu teoriden pratiğe taşıma ve gerçek durumu ortaya koymak daha mümkün olmaktadır [14].

III. SIBER SALDIRI YÖNTEMLERI

Siber tehditlerin ortaya çıkmasına neden olan üç boyut bulunmaktadır [20]:

- Internet tasarımındaki zafiyetler (adresleme sistemi, yönetim eksikliği, internetin çalışmasını sağlayan sistemlerin çoğunun açık ve şifresiz olması, zararlı yazılımları dağıtma kabiliyeti ve internetin merkezî olmayan büyük bir ağ olması)
- Donanım ile yazılımlardaki hatalar
- Kritik sistemlere çevrim içi erişim imkânı

Siber saldırılar çok çeşitli yöntemlerle yapılmaktadır. Belli başlı siber saldırı yöntemleri ise şöyledir [21]:

- ✓ Bilgi ve veri aldatmacası (Data Diddling): Bilgisayara veri girilirken yanlış girilmesi, verileri saklarken özel yöntemlerle değiştirilmesi ya da bazı kayıtların silinmesi bu yöntemle yapılabilir [13].
- ✓ Salam tekniği (Salami Techniques): Genellikle bankacılık sektöründe kullanılır. Hesaplardaki virgülden sonraki küsuratların son rakam veya son iki rakam tutarı başka bir hesaba aktarılarak orada biriktirilmektedir [31].
- ✓ Süper darbe (Super Zapping): Bilgisayar sistemlerindeki arızalar ile sistemin kilitlenmesi durumunda güvenlik kontrollerinin aşılarak sistemin düzeltilmesi için geliştirilmiş programlardır. Bu durum kötüye kullanıldığında güvenlik devre dışı bırakılmaktadır [19].
- ✓ Truva atı (Casus Yazılımlar): Bilgisayar korsanları truva atları sayesinde sisteme arka kapıdan ulaşarak, bilgisayarın sistem yapısını değiştirebilir ayrıca kullanıcının şifrelerine ve diğer kişisel bilgilerine ulaşabilirler. Truva atı sisteme bulaştıktan sonra, sistemin açılmasıyla beraber kendisini hafızaya yükler ve sistem açıklarını kullanarak, programı yerleştiren bilgisayar korsanının istediklerini yapmasını sağlar [18].

- ✓ Zararlı yazılımlar (Kötücül Yazılımlar): Virüs gibi belli bir amaca yönelik olarak hazırlanmış kod parçalarıdır.
- ✓ Mantık bombaları (Logic Bombs): Bir programın içerisine istenen zararlı bir kod parçasının yerleştirilmesidir. Mantık bombası genellikle hedef alınan bilgisayar veya ağlardaki bilgileri tamamen yok etmek veya bird aha kullanılamaz hale getirmek için kullanılır [27].
- ✓ Oltalama (Phishing): Genellikle sahte web siteleri kullanılmaktadır. Örneğin bir banka yada alış veriş sitesinden kendisine e-posta geldiğini düşünen son kullanıcı; kredi kartı bilgilerini bu web sayfasına girerek yada sadece e-postayı yanıtlayarak bu tuzağa düşebilmektedir [2].
- ✓ Bukalemun (Chamelon): Normal bir program gibi çalışırır fakat arka planda bir takım hile ve aldatmalar ile çok kullanıcılı sistemlerde kullanıcı adları ve şifrelerini taklitm ederek gizli bir dosya içerisine kaydedip, sistemin bakımı için geçici bir süre kapatılacağına ilişkin bir (YerTutucu) uyarı verir. Bu sırada bukalemun programını kullanan kişi, bu gizli dosyaya ulaşarak kullanıcı adlarını ve şifrelerini ele geçirir [6].
- ✓ İstem dışı alınan elektronik postalar (Spam): Tartışma platformlarından dağıtılan listelerden ve web sayfalarından elde edilen elektronik adreslere alıcının haberi olmaksızın arasıra büyük hacimlerde gönderilen ve ticari amaç taşıyan e-postalar olarak tanımlamaktadır [29].
- ✓ Çöpe dalma (Scavenging): Sistem belleğinde bulunan ve artık ihtiyaç duyulmayan silinmiş bilgilerin gelişmiş yöntemlerle tekrar geri getirilmesidir [5].
- ✓ Yerine geçme (Masquerading): Sistemde yapılacak hileler ile erişim imkanı kısıtlı ya da yetkisi hiç olmayan kullanıcıların, erişime yetkisi olan başka kullanıcıların bilgi ve yetkilerini kullanarak sisteme erişim sağlamasıdır [18].
- ✓ Sistem güvenliğinin kırılıp içeri sızılması (Hacking): Hack kelimesi hacker topluluklarında kullanılan anlamıyla "teknolojinin orijinal, alışılmışın dışında ve özgün bir tarzda kullanılması" anlamına gelmektedir. Ayırt edici özelliği ise sadelik, ustalık ve yasa dışı oluşudur [28].
- ✓ Hukuka aykırı içerik sunulması: Özellikle web sitelerine reklam amaçlı ya da hukuka aykırı içeriklerin eklenmesidir.
- ✓ Web sayfası hırsızlığı ve yönlendirme: Web sitelerinin çalınarak kullanamaz hale gelmesi, web sitelerinde farklı içerikler sunulması, sayfa girişinde ya da içeriğinde başka sayfalara yönlendirilerek veri girişine zorlanılmasıdır.
- ✓ Sosyal mühendislik: Yalan söyleme ve karşı tarafı ikna etme üzerine kurulan bir bilgi toplama sanatıdır. Burada kişilerin güveni kazanılarak kendilerine güvenmelerinin sağlanması amaçlanmaktadır [8].

IV. TÜRKIYE'DE SIBER GÜVENLIK DURUM ANALIZI

Türkiye'de siber suçlarla mücadele 2012 yılına kadar Bilim, Sanayi ve Teknoloji Bakanlığının koordinatörlüğünde Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından sivil toplum kuruluşları ve kurumları ile beraber yürütülmüştür. Daha sonra ise "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" hazırlanarak yürürlüğe girmiştir. 20 Ekim 2012 tarih ve 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" 28447 sayılı Resmi Gazetede Yayımlanmıştır [26]. Türkiye'nin Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planında "Siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesi" şeklinde tanımlanmıştır [30].

9 Eylül 2016 tarihinde gerçekleştirilen bir toplantı ile tanıtılan Türkiye'nin 4 yıllık süreçte siber güvenlik konusunda izleyeceği yolu belirleyen 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı ise 5 ana eylem ve 41 alt eylemden oluşmaktadır. Eylemin amacı: siber güvenliğin, ulusal güvenliğin ayrılmaz bir parçası olduğu anlayışının tüm kesimlerde yerleştirilmesi, ulusal siber uzayda bulunan sistem ve paydaşların tamamının güvenliğini sağlamak üzere idari ve teknolojik önlemlerin alınmasını sağlayacak yetkinliğin eksiksiz bir şekilde kazanılmasıdır [25].

Ülkemizin, ulusal siber güvenlik stratejisinin ilgili eylem maddelerinde tüm kamu kurumları ile kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlara SOME (Siber Olaylara Müdahale Ekipleri) kurulması ile ilgili görevler verilmektedir. Sektörel ve Kurumsal SOME'lerin kurulması ile kamu-özel sektör arasındaki bilgi akışlarının hızlanması, gelişen siber tehditlere karşı etkin mücadele edilmesi mümkün olabilecektir.

Siber Güvenlik Eylem Planları, Ulusal Bilgi Güvenliği Programı, Ulusal Bilgi Güvenliği Kapısı, Yasal Çalışmalar, Siber Güvenlik Müdahale Ekipleri ve Birimleri, Siber Güvenlik Tatbikatları, Konferanslar ve Çalıştaylar ve de TSK bünyesinde icra edilen faaliyetler ve oluşumlar gibi Türkiye'de siber güvenlik bilincinin artması için son zamanlarda değişik çalışmalar yapılmaktadır [14].

Bilişim güvenliği açısından Türkiye'nin, dünyadaki diğer ülkelere göre konumu, farklı kıstaslara göre değerlendirildiğinde farklı sonuçlar ortaya çıkmaktadır. Örneğin; siber güvenlik firması olan FireEye tarafından hazırlanan en güncel istihbarat raporunda; 2016 yılında Türkiye'de bütün Avrupa'da meydana gelenden daha fazla "hedefli kötücül yazılım" olduğu vurgulanmaktadır. Fireye sözcüsüne göre bu kategorideki sızmalar; muhtemelen devlet destekli, gelişmiş ve bilinen hackerların aktiviteleri ile aynı karakteristiklere sahiptir [23]. Symantec'in Internet Güvenlik Tehdit Raporu'na göre ise Türkiye, 2016 yılında Avrupa, Ortadoğu ve Afrika'nın tüm zararlı yazılım tespitlerinin toplamının %3.4'ünü oluşturmaktadır [23]. Fortinet firması tarafından Ağustos 2016 ayında yayımlanan 2016 ikinci çeyrek siber tehdit analiz raporunda botnet, zararlı yazılım (malware) ve istismar kiti (exploit kit) tespit edilen ülke istatistiklerinde ülkemizin ilk 5 içerisinde yer aldığı görülmektedir [25]. Trend Micro tarafından yayımlanan 2016 yılının ilk yarısına ait bir diğer güvenlik raporundaki veriler, tüm dünyada fidye yazılım saldırılarının yüzde 172 oranında arttığını, ülkemizin Avrupa bölgesinde fidye yazılım

saldırılarını en fazla yaşayan ülke olduğunu, dünyada ise ABD ve Brezilya'dan sonra üçüncü sırada yer aldığı ifade edilmektedir [25]. Diğer yandan, yine Trend Micro'nun araştırması ülkemizde on-line bankacılığa yönelik tehditlerin de hız kesmeden devam ettiğini gözler önüne sermektedir. Tespitlere göre ülkemiz 11 bin 516 saldırı ile Avrupa bölgesinde en fazla on-line bankacılık saldırısı alan ülke olurken, ülkemizi 4 bin 880 saldırı ile Almanya ve 3 bin 529 saldırı ile Fransa izlemektedir [25].

Küresel pazar araştırma şirketi Vanson Bourne'nun yaptığı araştırmaya göre dünya genelinde şirketler veri sızıntısını engellemek için aylık ortalama 4129 Euro harcama yaparken, Türk şirketlerinin 3220 Euro harcadığı ifade edilmektedir. Cybersecurity Ventures firması tarafından en son yayımlanan 2016 üçüncü çeyrek siber güvenlik market raporuna göre siber suçların 2015 yılında 3 trilyon ABD Doları olan maliyetinin 2021 yılında 6 trilyon ABD Dolarına ulaşması beklenmektedir. Raporda dikkat çekici bir diğer husus da 2020 yılına kadar günümüzdekinin 50 katı daha fazla verinin siber tehditlerden korunmak zorunda olacağıdır. Siber suçlardaki bu artışlar doğal olarak siber saldırılarla mücadele için ayrılan bütçeleri gittikçe çok daha yukarılara çekmektedir. Kurumlar bu tarz durumların yaşanmaması adına bilgi güvenliği hizmetleri sunan şirketlerden ürün ve danışmanlık satın almaktadırlar. Bu kapsamda 2015 yılında 75 milyar ABD Dolarını bulan siber güvenlik harcamalarının, 5 yıl içerisinde toplamda 1 trilyon ABD Dolarına ulaşacağı öne sürülmektedir [25] NATO tarafından Denver Üniversitesi'ne yaptırılan bir araştırma sonucuna göre, 2030 yılında dünyada siber güvensizlikten dolayı meydana gelen hacmin 90 Trilyon Dolar'a ulaşması öngörülmektedir. Daha da endişe verici olanı; bu çalışma gelecekte siber güvensizliğin yaratacağı maliyetin siber uzayın getirdiği yararlardan daha ağır olabileceğinin altını çizmektedir. Bu nedenle, söz edilen harcama miktarının güvensizliğin getirebileceği toplam maliyet ile karşılaştırıldığında oldukça küçük kalabileceği belirtilmektedir [16].

V. SONUÇ

Siber güvenlik günümüzde artık ulusal güvenlik stratejilerinde de ele alınan bir kavram haline gelmiştir. Özellikle son birkaç yıldır, Türk şirketleri ve hükümet yetkililerinin de sürekli olarak siber suçların ve siber casusluğun hedefinde olmaları bu alandaki probleme dikkat çekmekte ve daha fazla yatırım yapılmasının gerektiğini gözler önüne sermektedir. Teknolojideki sürekli gelişme ile birlikte siber güvenlik konusunda da meydana gelen gelişmeler o kadar hızlı gerçekleşmektedir ki, alınan önlemler ve yapılan yasal duzenlemeler yetersiz kalabilmektedir. Olası tehditler ve ihtiyaçlar doğrultusunda alınan kararlar ileriye dönük olarak güvenliğin sağlanmasında yeterince etkili olamamaktadır. Çok çeşitli siber saldırı yöntemleri bulunmakta olup, özellikle kişisel ölçekte bunların çoğu bilinmemektedir. Bilişim sistemleri için güvenlik stratejileri ise konuyu bilen uzmanlar tarafından geliştirilirken çoğu zaman son kullanıcı bu güvenlik tedbirlerinden habersizdir. Bu bağlamda siber alanda oluşan tüm tehditlere karşı devlet, kurum ve bireylerin birlikte hareket ederek hatta devletler bazında işbirliği yaparak tüm dünyada bilinç seviyesinin artırılması gerekmektedir. Siber güvensizliğin getirebileceği maliyetin bu alanda yapılacak harcamalardan daha fazla olabileceği göz önüne alındığında siber savunmaya daha fazla yatırım yapılması gerektiği açıkça görülmektedir.

KAYNAKLAR

1. A. Aytekin. "Türkiye'nin Siber Güvenlik Stratejisi ve Eylem Planının Değerlendirilmesi", Yayımlanmamış Yüksek Lisans Tezi, Bilişim Sistemleri Anabilim Dalı, Gazi Üniversitesi, 2015.
2. A. Çubukçu, & Ş. Bayram (2013). Türkiye'de Dijital Vatandaşlık Algısı ve Bu Algıyı İnternetin Bilinçli, Güvenli ve Etkin Kullanımı ile Artırma Yöntemleri. Middle Eastern & African Journal of Educational Research, 5, 148-174
3. B. Alaca, (2008). "Ülkemizde Bilişim Suçları ve Internetin Suça Etkisi (Antropolojik ve Hukuki Boyutları İle)", Ankara Üniversitesi Sosyal Bilimler Enstitüsü Antropoloji Anabilim Dalı, Yayınlanmamış Yüksek Lisans Tezi. Ankara.
4. Dijitalajanslar 2017. Internet ve Sosyal Medya Kullanıcı İstatistikleri. Dijital Ajanslar. http://www.dijitalajanslar.com/internet-ve-sosyal-medya-kullanici-istatistikleri-2017/ (Access Date:12.08.2017).
5. E. Altınok, A.F. Vural. "Bilişim Suçları", 2011. http://dergipark.gov.tr/download/article-file/208853
6. E. Aydın (1992). Bilişim Suçları ve Hukukuna Giriş. Ankara: Doruk Yayınları.
7. H. Çifci., (2013). Her Yönüyle Siber Savaş, Tubitak, Ankara.
8. K. D. Mitnick,W.L. Simon, "Aldatma Sanatı", Nejat Eralp Tezcan, ODTÜ Yayıncılık, Ankara, 303, 2006.
9. K. VonKnop, "Institutionslisation of a Web-focused, Multinstional Counter-Terrorism Campaign - Building a Collective Open Source Intelligent System", Terrorism (Ed.), Responses to Cyber Terrorism NATO Science for Piece and Security, IOS Press (Cilt 34), Ankara, 2008, p. 9
10. L. Hansen, H. Nissenbaum, "Digital Disaster, Cyber Security and the Copenhagen School", International Studies Quarterly, Volume: 53, 1155-1175, 2009.
11. M. Alkan," Siber Güvenlik ve Siber Savaşlar" , Siber Güvenlik Siber Savaşlar TBMM Internet Komisyonu, Mayıs 2012.
12. M. Goodrich, R. Tamassio, "Introduction to Computer Security", Addison-Wesley Publishing Company, USA. ISBN:0321512944 9780321512949, 2010.
13. M. H. Wrobleski - M.K. Hens , "Introduction to Law Enforcement and Criminal Justice", third edition, West Publiching Company, 1990.
14. M. N. Öğün, A. KAYA, "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler", Güvenlik Stratejileri Dergisi, Yıl:9, Sayı: 18, 2013.
15. NATO 2012. National Cyber Security Framework Manual. NATO CCDCOE. https://ccdcoe.org/multimedia/national-cyber-security-framework-manual.html (Access Date: 12.08.2017)
16. NATO 2017. Başarılı Bir Siber Savunma İçin Harcama Yapmak. NATO Dergisi. http://www.nato.int/docu/review/2017/Also-in-2017/nato-priority-spending-success-cyber-defence/TR/index.htm (Access Date: 12.08.2017)
17. N. F. Doherty, L. Anastasakis, H. Fulford, "The Information Security Policy Unpacked: A Critical Study of the Content of University Policies", International Journal of Information Management, 29(6), 449–457, 2009.
18. O. Değirmenci,"Bilişim Suçlar", (Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi), İstanbul, 2002.
19. O. Turhan, "Bilgisayar Ağları ile İlgili Suçlar", T.C. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşsavirliği, Planlama Uzmanlığı Tezi, Ankara, 2006.
20. R. A. Clarke, R.K. Knake, "Cyber War-The Next Threat to National Security and What to Do About It", New York: HarperCollins Publishers, 74-85, 2010.
21. R. Benzer. "Siber Suçlar ve Teorik Yaklaşımlar", Güncel Tehdit: Siber Suçlar, Birinci Baskı, Ankara, Seçkin Yayıncılık, 21-41, 2014.
22. S. E. Goodman, "Critical Information Infrastructure Protection", Terrorism (Ed.), Responses to Cyber Terrorism NATO Science for Piece and Security, IOS Press (Volume 34), Ankara, 25, 2008.
23. SiberBulten 2017. Kritik Rapor: Türkiye'nin Jeopolitik Durumu Siber Casusları Cezbediyor. Siber Bülten. https://siberbulten.com/sektorel/trky/kritik-rapor-turkiyenin-jeopolitik-durumu-siber-casuslari-cezbediyor/ (Access Date: 12.08.2017)
24. S. Jajodia and P. Liu, et all. (Ed.), Cyber Situational Awareness. New York, Springer, p. 5 2010.
25. STM 2016. 2016 Temmuz Eylül Dönemi Siber Tehdit Durum Raporu. Mühendislik Teknoloji Danışmanlık. https://www.stm.com.tr/documents/file/Pdf/Siber%20Tehdit%20Durum%20Raporu%20Temmuz%20-%20Eylul%202016.pdf (Access Date: 12.08.2017)

26. S. Yılmaz, Ş. Sağıroğlu, "Siber Saldırı Hedefleri ve Türkiye'de Siber Güvenlik Stratejisi" 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 323-331, Ankara. 2013.
27. Ş. Çelik, "Stuxnet Saldirisi Ve Abd'nin Siber SavaşStratejisi: Uluslararasi Hukukta Kuvvet Kullanmaktan Kaçinma İlkesi Çerçevesinde Bir Değerlendirme", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi Cilt: 15, Sayı: 1, 2013, s.137-175.
28. T. Jordan & P.Taylor, (2004). Hacktivism and Cyberwars: Rebels with a Cause?. Routledge.
29. T. Memiş, Hukuki Açıdan Kitlelere E-posta Gönderilmesi. Saarbrücken Hukuki Internet Projesi. 2005. www.jura.uni-sb.de/turkish/TMemis1.html
30. UDHB 2012. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı. T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Ankara, s. 9-47.
31. Y. Yazıcıoğlu, 2004. "Bilişim Suçlar Konusunda 2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi", Hukuk ve Adalet: Eleştirel Hukuk Dergisi, İstanbul, Y:1, S:1, Ocak-Mart 2004, ss. 172-185.