

İÇ GÜVENLİK YÖNETİMİ VE POLİSLİK

Derleyen
İbrahim İrdem



POLİS AKADEMİSİ YAYINLARI

İÇ GÜVENLİK YÖNETİMİ VE POLİSLİK

Derleyen
İbrahim İrdem



POLİS AKADEMİSİ YAYINLARI

Polis Akademisi Yayınları: 111

Kitabın Adı: İç Güvenlik Yönetimi ve Polislik
Derleyen: Dr. Öğr. Üyesi İbrahim İrdem
ISBN: 978-605-7822-57-4
1. Baskı, 1.900 Adet, Ankara 2020
Tasarım: Muhammed Delibaş

© 2020 Polis Akademisi Başkanlığı

Bu kitabın basım, yayın ve satış hakları Polis Akademisi Başkanlığına aittir. Polis Akademisi Başkanlığının izni alınmadan kitabın tümü ya da bölümleri mekanik, elektronik, fotokopi, manyetik, kayıt ya da başka yöntemlerle çoğaltılamaz, basılamaz dağıtılamaz. Bu kitapta ifade edilen görüşler ve düşünceler hiç bir şekilde Polis Akademisi Başkanlığının resmi görüşü değildir. Bu görüş ve düşünceler ile ilgili her türlü sorumluluk tamamen kitabın yazar/yazarlarına aittir.

Basım Yeri

Polis Akademisi Başkanlığı Basım ve Yayın Şube Müdürlüğü
Fatih Sultan Mehmet Bulvarı, No: 218, Yenimahalle/ANKARA 06200

Polis Akademisi Yayınları Sertifika No: 45724

Polis Akademisi Başkanlığı, Necatibey Caddesi, No: 108, Anıttepe, ANKARA
Tel: +90 (312) 462 90 87-91-92-93 Faks: +90 (312) 462 90 95
www.pa.edu.tr

İÇİNDEKİLER

İÇ GÜVENLİK, KAMU DÜZENİ VE YENİ KAMU HİZMETİ PERSPEKTİFİNDEN GÜVENLİK YÖNETİMİ

İbrahim İrdem

GİRİŞ	17
1. Kavramsal Açıdan Güvenlik	18
2. İç Güvenlik Yönetimi	27
3. İç Güvenlik ve Kamu Düzeni.....	31
4. Yeni Kamu Hizmeti Çerçevesinde İç Güvenlik Yönetimi	36
SONUÇ	40

OSMANLI'DA VE TÜRKİYE'DE İÇ GÜVENLİK POLİTİKALARI

Hüseyin Arslan

GİRİŞ	47
1. Güvenlik ve İç Güvenlik Kavramları	49
2. Osmanlı'da İç Güvenlik Politikaları	52
3. Türkiye'de İç Güvenlik Politikaları	61
SONUÇ	80

İÇ GÜVENLİK YAKLAŞIMLARI VE MODELLERİ

Merve Reyhan Baygeldi

GİRİŞ	89
1. İç Güvenliği Kavramsal Olarak Değerlendirmeyi Mümkün Kılan Yaklaşımlar	90
2. İç Güvenlik Modelleri	100
SONUÇ	113

İÇ GÜVENLİK YÖNETİMİ VE SUÇ ÖNLEME STRATEJİLERİ

Ahmet Demirden

GİRİŞ	119
1. Suç Önleme Stratejileri	124
2. Suç Önleme Stratejilerinde Adli Risk Analiz Yöntemleri	134
SONUÇ	139

İÇ GÜVENLİK TEŞKİLATI

Begüm İsbir

GİRİŞ	147
1. İç Güvenlik Faaliyetleri ve Kolluk Kavramı	148
2. Türk İdari Teşkilatı Açısından Kolluk Makamı-Kolluk Amiri-Kolluk Personeli Ayrımı	159
3. Kolluk Türlerine Göre İç Güvenlik Teşkilatı	165
4. İç Güvenlik Teşkilatında Kendine Özgü (Sui Generis) Kolluk: Özel Güvenlik	174
SONUÇ	177

TÜRKİYE'DE VE DÜNYA'DA POLİSLİK UYGULAMALARI

Ülkü Nur Zengin

GİRİŞ	181
1. Polis Kavramı	182
2. Dünyada Polisliğin Tarihçesi	182
3. Türkiye'de Polisliğin Tarihçesi	186
4. Dünyada ve Türkiye'de Polislik Uygulamaları	189
SONUÇ	208

POLİS MESLEK ETİĞİ

Ozan Kavsıracı

GİRİŞ	215
1. Polis Kavramının Tanımı ve İşlevi	217
2. Etik ve Meslek	225
3. Polis Meslek Etiği	230
SONUÇ	235

İÇ GÜVENLİK VE İSTİHBARAT

Seda Öz Yıldız

GİRİŞ	241
1. İstihbarat Nedir?	242
2. İç Güvenlik İstihbaratı	248
3. İç Güvenlik İstihbaratının Üç Temel Seviyesi: Taktik, Operasyonel ve Stratejik İstihbarat	250
4. Suç İstihbaratı ve Suç Analizi	256
4.1. Suç Analizi	259
5. Türkiye’de İç Güvenlik İstihbaratı Kapsamında Polisin Görev ve Yetkileri	266
SONUÇ	273

İÇ GÜVENLİK VE PSİKOLOJİK HAREKÂT

Esra Çetinöz

GİRİŞ	277
1. Propaganda	279
2. Psikolojik Harekât	283
3. Psikolojik İkna Teknikleri	287
4. Psikolojik Harekât Aktörü Olarak FETÖ	292
SONUÇ	298

İÇ GÜVENLİK VE SİBER GÜVENLİK

Oğuzhan Yanarışık

GİRİŞ	303
1. Çeşitlenen Siber Saldırı Yöntemleri	305
2. Yaygınlaşan Siber Suçlar	310
3. Büyüyen Siber Terörizm Tehdidi	313
4. Sanal Dünyada Siber Savaşlar	315
5. Türkiye’de Siber Güvenlik	319
SONUÇ	321
Okuma Parçası: Çalışanlar İçin Siber Farkındalık	323

KOLLUĐUN SİVİL GÖZETİMİ VE DEMOKRATİK DENETİMİ

Hamit Emrah Beriř

GİRİř	329
1. KolluĐun Demokratik Denetiminin Nedenleri ve Araçları	331
2. Türkiye’de KolluĐun Denetimi	345
SONUÇ	358

MÜLKİ İDARE VE ADLİ YARGININ İÇ GÜVENLİK YÖNETİMİ ÜZERİNDEKİ GÖREV VE YETKİLERİ

Ali Rıza Töngür

GİRİř	363
1. Mülki İdarenin İç Güvenlik Yönetimi Üzerindeki Görev ve Yetkileri.....	365
2. Adli Yargının İç Güvenlik Yönetimi Üzerindeki Görev ve Yetkileri	371
SONUÇ	380

İÇ GÜVENLİK VE SİBER GÜVENLİK

Oğuzhan Yanarışik^{1*}

GİRİŞ

Günümüzde 4,5 milyardan fazla insan interneti kullanırken; küresel sosyal medya kullanıcı sayısı 3,8 milyarı ve cep telefonu kullanıcı sayısı da 5.1 milyarı aşmıştır. Dünya nüfusunun yaklaşık %60'ı hâlihazırda çevrimiçidir ve bu oran sürekli artmaktadır. Ortalama bir internet kullanıcısı günde yaklaşık 6 saat 43 dakikasını; yani yılda 100 günden fazla vaktini çevrimiçi olarak geçirmektedir. Bu süre Filipinler, Güney Afrika Cumhuriyeti ve Brezilya gibi ülkelerde günlük 9 saatin üzerine çıkarken; Türkiye yaklaşık 7.5 saatlik günlük kullanımla dünya ortalamasının üzerindedir. (WeAreSocial ve Hootsuiye, 2020)

İnternet, bilgisayarlar ve dijital teknolojiler dünyayı daha önce benzeri görülmemiş bir hızla dönüştürmektedir. Bu yeni teknolojilerin sağladığı imkânlar iletişim kurma, yaşama ve çalışma şeklimizi köklü bir şekilde değiştirmektedir. Veri işleme ve depolama teknolojilerindeki ilerlemelerle birlikte, yalnızca birkaç yıl içerisinde üretilen veri, o döneme dek üretilmiş olan bütün analog ve sayısal verilerin birkaç misline erişmektedir. Nesnelerin İnterneti (Internet of Things), dünyayı yeni yollarla birbirine bağlamaktadır. Hatta insan vücudunun fonksiyonlarını takip eden, sağlık durumuna ve diğer kişisel

^{1*} Dr. Öğretim Üyesi, Polis Akademisi, Güvenlik Bilimleri Enstitüsü, yanarisik@gmail.com

bilgilerine dair veri toplayan ve bu verileri internete yükleyen aletleri insanlar gönüllü olarak satın alıp kullanmakta ve böylece Bedenlerin İnternetini oluşturmaktadır (Internet of Bodies). Her ne kadar ‘sanal dünya’ olarak adlandırılrsa da bilgisayar sistemlerini birbirine bağlayan elektronik iletişim ağı olan internet, artık ‘gerçek dünya’ ile ayrılmaz bir bütün haline gelmiştir.

Daha önceleri ağırlıklı olarak çevrimdışı ortamda yürütülen birçok faaliyet, artık çevrimiçi ortamda gerçekleşmektedir. Ülkeler, şirketler ve bireyler için kritik öneme sahip olan alt ve üst yapılar büyük oranda bilgisayar sistemlerine bağımlı hale gelmiştir. Böylelikle siber âlemin siyasi, ekonomik, stratejik ve sosyal etkileri sürekli katlanarak artmıştır. Bazı tahminlere göre, internete bağlanan insanların sayısının 2015’ten 2022’ye kadar üç katına çıkacağı ve 6 milyara ulaşacağı öngörülmektedir. 2030 yılına kadar 6 yaş ve üzeri insan nüfusunun yüzde 90’ının çevrimiçi olacağı tahmin edilmektedir. (Morgan, 2020) Bu genişleyen sanal dünyada güvenliği sağlayabilmek, devletler, şirketler, kurumlar ve bireyler için daha fazla hayati önem arz etmeye başlamıştır. Siber güvenlik, hem iç hem de dış güvenliğin vazgeçilmez unsurlarından biri haline gelmiştir.

Siber saldırı, yaygın tanıma göre, bir bilgisayardan bir internet sitesine, ağa veya kullanıcı bilgisayarına yapılan ve o sistemin veya depolanan bilgilerin gizliliğini, bütünlüğünü veya kullanılabilirliğini tehlikeye atan saldırıdır. Dağıtılmış hizmet reddi (DDoS), kötü amaçlı yazılım, kimlik avı ve veri hırsızlığına yol açan sosyal mühendislik gibi pek çok yöntemi içermektedir. Koordineli aktörlerin karmaşık ve sistematik çabaları ile bu saldırılar uzun süre tespit edilemeyebilir. (Springer, 2017: 40-43) Bir siber saldırı, kötü niyetli olarak bilgisayarları devre dışı bırakabilmekte, verileri çalabilmekte veya ihlal edilen bir bilgisayarı diğer saldırılar için başlatma noktası olarak kullanabilmektedir. Siber suçlular, diğer yöntemlerin yanı sıra kötü amaçlı yazılım, kimlik avı, fidye yazılımı, hizmet reddi dâhil olmak üzere siber saldırı başlatmak için çeşitli yöntemler kullanmaktadır. Bu yönüyle siber saldırılar, hizmetleri kesintiye uğratma veya milyonlarca insanın refahını ve güvenliğini tehlikeye atma kapasitesine sahiptir. Bu saldırılarla acil servisler, elektrik dağıtım sistemleri, telekomünikasyon kanalları, su dağıtım ağları, finansal sistemler ve havaalanları kapatılabilmektedir. Hastane kayıtlarına ve hatta ulusal güvenlik bilgisayar programlarına müdahale edilebilmekte ve bunlar kalıcı olarak imha edilebilmektedir.

Siber suçlar, mali suç, çevrimiçi kumar, siber iftira, siber pornografi, virüsler ve e-posta yoluyla yürütülen veri sahteciliği gibi suçları kapsamaktadır.

Günümüzde siber suçlar genellikle farklı aktörlerin işbirliği içinde işlenmekte ve bu da siber suçları bütün dünya için ciddi bir sorun haline getirmektedir. Siber suçlular için ülkeler arası sınırların anlam ifade etmemesi, ekipmanlarının geleneksel suç ekipmanlarına nazaran daha ucuz olması, suçluların mağdurlarla yüzleşmek zorunda kalmaması ve internetin anonim/gizli kalma imkânı sunması gibi sebeplerle oldukça yaygınlaşmaktadır. Dünyada siber suçları önlemek için sürekli çalışan devlet kurumları, polis departmanları ve siber suç büroları bulunmaktadır. Sanal dünyada güvenlik ve özgürlük dengesi sağlama konusundaki tartışmalar ve kaygılar, siber suçlarla mücadelede atılabilecek adımların sınırlarını belirlemektedir.

Siber terörizm, ciddi bedensel zarar veya hatta ölümle sonuçlanabilen tehdit veya şiddet eylemlerini gerçekleştirmek için internetin ve bilgisayar sistemlerinin kullanılması anlamına gelmektedir. Siber terörizm eylemleri genellikle yıldırma, korku ve tehdit yoluyla siyasi veya ideolojik avantajlar elde etmeyi amaçlamaktadır. Siber terörizmin tanımını, solucanlar, virüsler, kimlik avı etkinlikleri ve diğer kötü amaçlı yazılımları kullanılarak bilgisayar ağlarının kasıtlı olarak bozulması gibi faaliyetleri kapsayacak şekilde genişletmek mümkündür.

Siber savaş, bir ülkeye saldırmak için dijital teknolojilerin kullanılmasıdır ve gerçek savaşa benzer zararlara neden olabilmektedir. Her ne kadar ‘siber savaş’ teriminin nasıl tanımlanacağı ve kullanılacağı konusunda tartışmalar olsa da birçok ülke saldırı ve savunma operasyonları için aktif siber yeteneklere sahiptir. Devletler siber operasyonların kullanımını araştırdıkça ve yetenekleri birleştirdikçe, siber savaş tehditleri sürekli artmaktadır.

Siber saldırı taktikleri terör örgütleri, bazı devletler, siyasi oluşumlar, organize suç örgütleri, özel firmalar ve bireyler tarafından kullanabilmektedir. Kitabımızın bu bölümünde siber saldırı yöntemleri incelenmekte; siber suç, siber terörizm ve siber savaş kavramları analiz edilmekte ve son olarak Türkiye’nin siber güvenlik konusundaki durumu üzerinde durulmaktadır.

1. Çeşitlenen Siber Saldırı Yöntemleri

İnternet, mobil ve dijital dünyada yaşanan baş döndüren dönüşüm, pek çok fırsat sunmakla birlikte; suç ve kötüye kullanım için de benzersiz riskler oluşturmaktadır. Klasik suçlular eylemlerinde bu yeni teknolojik imkânlardan sürekli artan oranda istifade etmektedir. Bununla birlikte, daha önce var olmayan yeni suç türleri ortaya çıkmaktadır. Suçlular daha önceleri mümkün olmayan

pek çok yöntemi ve taktiği hayata geçirebilmektedir. (Holt, Bossler ve Seigfried-Spellar, 2018: 21) Siber saldırılar, fiziksel, bilgisel ve algısal boyutlardan oluşan bilgi ortamında gerçekleşmektedir. Fiziksel boyut donanımdır ve bilgi boyutu yazılımdır. Algısal boyut ise insan düşüncelerinden oluşmaktadır. Bunu noktada şunu ifade etmek gerekir ki, ister kaza ile isterse kasıtlı olsun, insan faktörü genellikle siber saldırıların başarıya ulaşmasındaki temel nedenlerden biri olabilmektedir. Çeşitli yöntemler kullanılarak manipüle edilen kişiler, kurum ve kuruluşların en zayıf halkası olarak hedeflenebilmektedir. (Accenture Security, 2019)

Suçlular hedeflerine saldırırken oldukça farklı teknikler uygulamaktadır. *Kimlik avı (phishing)*, bu yöntemlerin en yaygınlarından biridir ve genellikle kredi kartı numaraları ve oturum açma bilgileri gibi kullanıcı verilerini çalmak için kullanılan bir tür sosyal mühendisliktir. Bu saldırı kurban güvenilir bir birey gibi davranan bir saldırgan tarafından gönderilen bir mesajı açtığında gerçekleşir. Kurban, fidye yazılımı saldırısının bir parçası olarak sisteminin donmasına, hassas bilgilerinin ifşa olmasına veya kötü amaçlı bir yazılımın yüklenmesine sebep olabilecek kötü amaçlı bir bağlantıyı açması için kandırılır. Bu saldırının kimlik hırsızlığı, paranın çalınması veya yetkisiz satın alımlar gibi ağır sonuçları olabilmektedir.

Kötü amaçlı yazılım (malware), kullanıcısının izni olmadan ele geçirilen bir bilgisayar sistemini gizlice etkilemek için üretilen bir koddur. Bu geniş tanım, virüs, solucan, Truva atı, casus yazılım, fidye yazılımı, korkutma yazılımı ve reklam yazılımı gibi birçok özel kötü amaçlı yazılım türünü içermektedir. Kötü amaçlı yazılım, bir ağa yayılması, sistemde değişikliklere ve hasara neden olabilmesi, tespit edilemez durumda kalabilmesi ve hatta kalıcı olabilmesi ile diğer yazılımlardan farklıdır. *Fidye yazılımı*, kurban verilerine erişimi engellemekte ve genellikle bir fidye ödenmediği takdirde verileri silmekle tehdit etmektedir. Fidye ödemenin verilere tekrar erişim sağlayacağını garanti bulunmamaktadır. *Casus yazılım*, gizlice yerleştiği sistemdeki kişisel bilgileri ve verileri takip eden ve kullanıcısına ileten bir programdır. Bu yazılım, kullanıcılarının hedef cihazdaki tüm iletişim türlerini izlemesine olanak sağlamaktadır. *Truva atları*, zararsız uygulamalar kılıfına girerek, kullanıcıları kendisini indirmeleri ve kullanmaları için kandırmaktadır. Çalışmaya başladıktan sonra ise kişisel verileri çalabilmekte, bir cihazı çökertebilmekte, kullanıcı etkinliklerini gözetleyebilmekte ve hatta ele geçirdiği sistem üzerinden bir sisteme karşı saldırı başlatabilmektedir. (McAfee, 2020)

Drive By Download saldırıları kötü amaçlı yazılımları yaymanın yaygın bir yöntemidir. Bu yöntemde siber suçlular güvenli olmayan internet sitelerinin koduna kötü amaçlı bir komut dosyası yerleştirmektedir. Bu komut dosyası, kötü amaçlı yazılımı doğrudan siteyi ziyaret eden kişinin cihazına yükleyebilmekte veya kurbanı siber suçlular tarafından kontrol edilen bir başka siteye yönlendirebilmektedir. Bu tip saldırılar mağdurun herhangi bir işlem yapmasını gerektirmediği için oldukça tehlikelidir. (Kaspersky, 2020)

Dağıtılmış Hizmet Reddi (DDoS) saldırıları internetteki en güçlü silahlardan biridir. Bir internet sitesini veya çevrimiçi hizmeti kapatmayı veya diğer kullanıcılar tarafından erişilemez hale gelmesini amaçlamaktadır. Bu saldırılar hedefi ziyaret trafiğine boğmaya veya veri bombardımanı ile çöktürmeye çalışmaktadır. Böylelikle kaynağın çalışan, müşteri veya üye gibi meşru kullanıcıları kaynağa erişememektedir. DDoS saldırıları genellikle ticari kuruluşlar, kamu kurumları, medya şirketleri veya finans kurumları gibi yüksek profilli kuruluşların internet sunucularını hedef almaktadır. Bu saldırılar her ne kadar veri kaybı veya hırsızlığı gibi sonuçlar doğurmasa da kurbanlara yüklü miktarda paraya ve zamana mal olabilmektedir. (Norton, 2020)

Bütün siber saldırılar dışarıdan gelmemektedir. *Dâhili saldırılar*, sisteme erişme yetkisi olan kötü niyetli bir kişi tarafından bir bilgisayar sistemi veya ağ üzerinde gerçekleştirilen saldırılardır. Bu saldırıları gerçekleştiren içeriden kişiler, yetkilendirilmiş sistem erişimine sahip oldukları ve sistem konusunda bilgili oldukları için dış saldırganlara göre bariz bir üstünlüğe sahiptir. Ayrıca, çoğu kuruluş dış saldırılara karşı savunmaya odaklandığından, içeriden gelebilecek saldırılara karşı daha az güvenlik önlemi bulunmaktadır. Her ne kadar bazı vakalar dikkatsizlik veya kaza sonucu olabilmekteyse de burada kastedilen kasıtlı bir şekilde verilerin çalınması veya yok edilmesi, sistemin çökertilmesi veya kaynakların tehlikeye atılması gibi durumları kapsamaktadır. (Homeland Security, 2020)

Geliştirilmiş Kalıcı Tehditler (Advanced Persistent Threat, APT) çok sayıda motivasyonla gerçekleşebilmektedir. Bunlar genellikle dört ana kategoride değerlendirilebilir: aktivizm, siber suç, şirket casusluğu ve siyasi/askeri casusluk. APT'ler ileri teknolojileri ve geniş kaynakları kullanarak aylarca ve hatta yıllarca belirli hedeflere odaklanmaktadır. Saldırgan hedefindeki sistemlere sızmak için genelde tek bir yöntem kullanmak yerine, pek çok farklı yöntemi aynı anda denemektedir. Ayrıca saldırgan sisteme hızlı bir şekilde girip veri çalmak yerine, uzun süre sistemde fark edilmeden kalıp kıymetli bilgileri toplamayı hedeflemektedir. Bunun yanında saldırgan bilindik ve otoma-

tik saldırı araçlarını kullanmanın yanında insan zaaflarından yararlanmaya da çalışmaktadır. Uzun süre ve geniş finans kaynağı gerektiren APT'ler genelde devletler veya onların sponsor oldukları aktörler tarafından gerçekleştirilmektedir. (Andress ve Winterfeld, 2014: 175)

Yapay Zekâ Destekli Saldırıları önümüzdeki süreçte oldukça tehlikeli boyutlara erişme potansiyeli taşımaktadır. Yapay zekâ hâlihazırda makine öğrenimi (machine learning) olarak adlandırılan algoritmik bir süreç aracılığıyla günlük uygulamalarda kullanılmaktadır. Pek çok kaynaktan akan bilgi yığınlarını kullanılabilir veri haline getirebilmektedir. Makine öğrenimi yazılımı, bir bilgisayarı belirli görevleri kendi başına gerçekleştirecek şekilde eğitmeyi amaçlamaktadır. Yapay zekâ, otonom araçlar ve insansız hava araçları dâhil olmak üzere birçok sistemi ele geçirerek bunları potansiyel silahlara dönüştürmek için kullanılabilir. Kimlik hırsızlığı, şifre kırma ve hizmet reddi saldırıları gibi siber saldırıları otomatik, daha güçlü ve verimli hale getirebilir. İnsanları öldürmek, yaralamak veya para çalmak için de kullanılabilir. Hatta daha büyük saldırılarla ulusal güvenliği tehlikeye atacak durumların oluşmasına yol açabilir. Her geçen gün dijitalleşen ve daha da birbirine bağlı hale gelen dünyada yapay zekâ kullanılarak gerçekleştirilebilecek saldırıların boyutları korkunç seviyelere ulaşabilecektir. (Kaloudi ve Li, 2020: 1-2)

Siber saldırıların kaynağı olarak bazı ülkeler ön plana çıkmaktadır. Örneğin, dünya üzerinde gerçekleştirilen siber saldırıların yaklaşık %30'unun kaynağı Çin'dir. Bu yüzden sık sık yabancı hükümetlere ve işletmelere yönelik devlet destekli siber saldırılar yapmakla suçlanmaktadır. Ayrıca Çin'in dünyadaki en büyük siber ordulardan birine sahip olduğu öngörülmektedir. Devlet destekli siber saldırılarda öne çıkan bir diğer ülke ise 30'dan fazla etkin siber suç örgütüne ve milyarlarca dolarlık siber suç karaborsasına ev sahipliği yapan Rusya'dır. Bu konuda dikkat çeken diğer ülkeler Romanya, Brezilya, Nijerya, Vietnam, Endonezya, Güney Kore ve ABD'dir.

Bazı sebeplerle siber saldırıları tespit edebilmek ve suçluları yakalayabilmek son derece zordur. Örneğin, bilgisayarların işlem gücü, internetin elektronik hızı ve birçok insanın evlerde, işyerlerinde, üniversitelerde, kütüphanelerde, sokaklarda ve neredeyse her yerde internete erişiminin olması siber suçların işlenmesini kolaylaştırırken, tespitini zorlaştırmaktadır. Dahası, birçok siber suç işlemek nispeten zahmetsizdir. Birkaç tuşa basarak veya birkaç tıklamayla hızlı bir şekilde gerçekleştirilebilmektedir. Elektronik cihazlar hemen hemen her zaman ve her yerde suç işlenmesine imkân tanımaktadır. Böylelikle siber uzayda zamansal ve mekânsal sınırlamalar ortadan kaldırılır.

labilmektedir. Siber ortamdaki eylemler yüz-yüze eylemlerle kıyaslandığında çok daha az duygusaldır. Bu durum, suçluların yaptıkları kötülükten duyacakları pişmanlık ve suçluluk hislerini azaltma etkisine sahiptir. Ayrıca internetin sunduğu şifreli anlık mesajlaşma programları, geçici e-posta hesapları, takma adlar, sohbet odaları ve sosyal ağ ortamları sayesinde suçlular kimliklerini nispeten kolayca gizleyebilmektedir. Bu gibi sebepler, siber suç vakalarını izlemeyi, tespit etmeyi, önlemeyi ve soruşturmaya tabi tutmayı zorlaştırmaktadır. (Hinduja ve Patchin, 2011: 181-182)

Yukarıda ifade edilen siber saldırı taktikleri karşısında bireylerin, kurumların ve devletlerin çeşitli savunma yöntemlerine başvurmaları gerekmektedir. Bireysel düzeyde ele alındığında, etkili ve güncel bir antivirüs programının kullanılması, güvenlik duvarının (firewall) etkinleştirilmesi, periyodik güvenlik taramaları yapılması, kırılması zor parolaların seçilmesi, verilerin düzenli aralıklarla yedeklenmesi ve kişisel verilerin güvenliğinin sağlanması gibi yöntemler öne çıkmaktadır. Ayrıca, şüpheli iletişime cevap verilmemesi, bilinmeyen bağlantılara tıklanmaması, sosyal medyadaki ilişkilerin iyi yönetilmesi ve internet kullanım şifresinin başkalarıyla paylaşılması gibi yöntemler de büyük önem taşımaktadır.

Kurum ve kuruluşların daha da dikkatli davranması gerekmektedir. Çünkü diğer kuruluşların, suçluların ve hatta devletlerin erişmek istediği bilgi veya varlıklara sahiptirler. Kurumlar açısından en önemli konular, yöneticilerin siber güvenliğin önemini kavraması, kurumsal siber güvenlik performansını iyileştirilmesi ve siber güvenlik için yeterli kaynağın ayrılmasıdır. Kuruluşların ayrıca personellerini siber güvenlik farkındalığı konusunda eğitmeleri, büyük miktarda veriyi korumaları ve siber güvenlik sistemlerini yönetmek için kalifiye personeli işe almaları gerekmektedir.

Devletler, bireylerin ve kuruluşların tüm savunma faaliyetlerine yardımcı olmalıdır. Siber güvenlik mevzuatının oluşturulması, siber güvenlik politikalarının ve alt yapısının geliştirilmesi büyük bir öneme sahiptir. Devletler ayrıca, yeterli sayıda kalifiye siber güvenlik uzmanı yetiştirildiğinden emin olmalı ve eğitim sistemini buna göre koordine etmelidir. Ayrıca siber güvenliği milli güvenliğe entegre etmeli, milli sınırları korumalı, ulusal komuta ve kontrolü her tür saldırı karşısında sürdürülebilir kılmalıdır.

2. Yaygınlaşan Siber Suçlar

Siber suçlar her geçen gün sayı, boyut, karmaşıklık ve maliyet bakımından büyümektedir. 2021 yılında siber suçların toplam küresel maliyetinin 6 trilyon doları bulacağı öngörülmektedir. Bu maliyet içerisinde verilerin zarar görmesi, para hırsızlığı, üretkenliğin azalması, fikri mülkiyetin çalınması, kişisel verilerin ele geçirilmesi, zimmete para geçirme, dolandırıcılık, iş akışının yavaşlatılması, adli soruşturma masrafları, saldırıya uğrayan verinin restorasyonu ve itibar kaybının maliyeti gibi unsurlar bulunmaktadır. (Cybercrime Magazine, 2020)

Kolluk kuvvetleri siber suçla mücadelede önemli rol oynamaktadır. Bu tür suçlarla mücadele özel kurumlarla kamu yetkilileri arasında dayanışma sağlamak önem taşımaktadır. Bu tür bir işbirliği için genel bir siber suç anlayışı oluşturulması ve bu kavramın kapsadığı suçların sınıflandırılması gerekmektedir. Genel itibariyle, siber suçları şu kategorilerde değerlendirmek mümkündür (Hinduja ve Patchin, 2011: 180):

1. Bilgi işlem cihazının bir suçun hedefi olduğu suçlar: Veri değişikliği, veri hırsızlığı, ağ müdahaleleri, hizmet reddi ve bilgisayar vandalizmi vb.
2. Bilgi işlem cihazının bir suçun aracı olarak kullanıldığı suçlar: Hizmet hırsızlığı, tahakkuk yoluyla hırsızlık, dolandırıcılık, tehdit, taciz ve takip vb.
3. Bilgi işlem cihazının bir suçta katkısının ikinci derecede olduğu suçlar: Bilgisayar teknolojisinin kullanımıyla desteklenen veya yataklık edilen kara para aklama, terör propagandası yapma veya organize suç girişimleri vb.
4. Donanım ve yazılımın yaygınlığıyla ilişkili suçlar: Fikri mülkiyet hırsızlığı, kimlik hırsızlığı ve bilgisayarlar, cep telefonları ve diğer elektronik cihazlardaki verileri, kaynakları ve hizmetleri içeren çeşitli beyaz yakalı suçlar vb.

Son yıllarda yaşanan hızlı dijital dönüşüm suçluların işini daha da kolaylaştırmıştır. Mevcut siber ortam, siber suçluların hedeflerine profesyonel veya kişisel nitelikte büyük zarar verebilmelerine imkân tanımaktadır. (Edwards, 2020: 1-2) Suçlunun bakış açısından, bir siber suçlu olmanın riskleri azdır. Bu suçlular yüksek finansal getiri sağlayan, düşük riskli bir model üzerinde çalışmaktadır. Mağdurların önemli bir kısmı itibar kaybı korkusu veya şantaj maruz kalma gibi çeşitli sebeplerle çoğu zaman kolluk kuvvetlerine başvurmadan çekinmektedir. Bu durumda, mağdurlar işlenen suçu ilgili polis birimlerine şikâyet etmek yerine, kendi araştırmasını yapmak, özel güvenlik

şirketlerinden yardım istemek veya olayı tamamen örtbas etmek gibi yolları tercih edebilmektedir.

Yeni teknolojik ürünler piyasaya sürüldükçe, suçlular bu ürün veya hizmetleri suç girişimlerini ilerletmek için nasıl istismar edilebileceklerine dair yaklaşımlar geliştirmeye çalışmaktadır. Suçlular bu becerileri geliştirdikçe, kolluk kuvvetleri de onlarla mücadele araç ve yöntemlerini güncelleştirmektedir. Siber suçlular, açık kaynak ve kapalı suç forumlarında bilgilerini diğer suçlularla paylaşabilmekte, engelle karşılaştıklarında birbirleriyle yardımlaşabilmektedir. Siber suçlular ayrıca bu alana ilgi duyan potansiyel suçlular için teknik eğitim imkânları sağlamaktadır. Gerekirse, bazı siteler aracılığıyla bire bir eğitim ve danışmanlık hizmetleri sağlayabilmektedir. Bu kapsamda siber suç, suçluların kullanabileceği birçok kaynağa sahip olduğu bir meslek olarak görülebilmektedir. Fakat bu mecralar aynı zamanda siber suçlarla mücadele eden kurum ve kişiler için de suçluların faaliyetlerini yürütme yollarını ve yöntemlerini anlamada yararlı olabilmektedir.

Kamu kurumlarına, şirketlere ve bireylere yönelik siber saldırılar onlarca yıldır gerçekleşmektedir. Bu saldırıların birçoğu o kadar başarılı olmuştur ki, mağdurların büyük bir kısmı saldırıya uğradığını bile fark edememiştir. Bu tip durumlarda daha önce saldırı yapıldığı ancak çalınan veriler istismar edilirken veya suç piyasalarında satılırken tespit edilebilmiş veya hiçbir zaman fark edilememiştir.

Siber suçların sayısı, boyutu, gizliliği ve karmaşıklığı sürekli artmaktadır. Bu da siber suçların yol açtığı problemlerin çözümü için gerekli olan zamanın artmasına ve ek maliyetlerin yükselmesine sebep olmaktadır. Veri hırsızlığı, siber suçların en maliyetli ve en hızlı yükselen türlerinden biridir. Veriler hedef olmaya devam ederken, hırsızlık her zaman tek amaç olmamaktadır. Yeni siber saldırı dalgalarında, verilerin artık sadece kopyalanmadığı, aynı zamanda imha edildiği veya değiştirildiği de görülmektedir. Böylelikle güven ve itibar kaybı gibi farklı zararlar da hedeflenmektedir.

Milyonlarca kullanıcıyı etkileyen veri ihlalleri çok yaygın hale gelmiştir. Dünyaca bilinen şirketlerin kullanıcı bilgileri pek çok kez ele geçirilip kötü amaçlarla kullanılmıştır. Örneğin, Yahoo 2013 yılında 3 milyar kullanıcısının tamamının isim, doğum tarihi, e-posta adresi ve şifresi gibi bilgilerinin çalındığını itiraf etmiş ve bu saldırının arkasında devlet-destekli aktörlerin olduğunu iddia etmiştir. Kredi kartı işlemleri sektöründe çalışan Heartland Payment Systems firmasında kayıtlı 134 milyon kredi kartının bilgileri 2008 yılında çalınmıştır. Şirket çalışma yetkisini kaybetmekle kalmamış, hileli ödemeler

için tahmini olarak 145 milyon dolar tazminat ödemiştir. İş dünyasının bilinen sosyal medya platformu olan LinkedIn sitesinin 165 milyon kullanıcısının bilgileri 2012’de çalınmış ve bir siber korsan forumunda satışa çıkarılmıştır.

Bir zamanların en popüler sosyal medya platformu olan MySpace sitesinin 360 milyon kullanıcısının bilgileri 2013’te çalınmış ve 2016’da dark webde satılmıştır. Marriott International otel firmasının yaklaşık 500 milyon müşterisinin verileri 2014 yılında çalınmaya başlanmış ve bu siber saldırı 2018 Eylül ayına kadar fark edilemeden devam etmiştir. Online satış devlerinden eBay 2014 Mayıs ayında 145 milyon üyesinin bilgilerinin ifşa olduğunu açıklamıştır. Saldırganların üç eBay üst düzey çalışanın giriş bilgilerini kullanarak 229 gün boyunca sistemlerine tam erişime sahip olduğunu itiraf etmiştir. Yetişkinlere yönelik içerik ve arkadaşlık hizmeti sunmayı vadeden Adult Friend Finder şirketi 2016’da yirmi yıllık verilerini oluşturan 412 milyon kullanıcı bilgisinin çalındığını açıklamıştır.

2017’de gerçekleşen WannaCry fidye yazılımı salgını 150 ülkede 200.000’den fazla bilgisayara bulaşmıştır. Bu yazılım Microsoft Windows işletim sistemini kullanan bilgisayarlardaki dosyaları şifrelemiş ve şifreyi kaldırma karşılığında fidye talep edilmiştir. Salgın esnasında bazı hastanelerde tıbbi cihazlar da dâhil olmak üzere bütün cihazlar şifrelenmiş ve bazı fabrikalar üretimi durdurmak zorunda kalmıştır. Toplam hasarı tam bilinmemekle birlikte, milyarlarca doları bulduğu tahmin edilmektedir.

ABD’nin en büyük kredi bürolarından Equifax 2017 yılında yaklaşık 147 milyon müşterisinin verilerinin ve kredi kartı bilgilerinin ifşa olduğunu açıklamıştır. Sağlıklı yaşam uygulaması olan MyFitnessPal’ın 150 milyon kullanıcısının ve video mesajlaşma servisi Dubsplash’ın 162 milyon kullanıcısının bilgileri 2018’de çalınmış ve bir yıl sonra internette satışa sunulmuştur. Eylül 2019’da popüler mobil oyun firması Zynga 218 milyon kullanıcısının şifre, telefon numarası ve e-posta adresinin çalındığını açıklamıştır. Çin’in Twitter benzeri sosyal medya şirketi olan Sina Weibo’nun 500 milyondan fazla kullanıcısının bilgileri 2020 Mart’ında çalınmış ve satışa sunulmuştur.

Kaspersky şirketinin verilerine göre yalnızca 2019 yılında dünya genelinde kullanıcı bilgisayarlarının %19,8’i en az bir kötü amaçlı yazılım sınıfı web saldırısına maruz kalmıştır. 273.782.113 adet farklı internet adresinin kötü amaçlı olduğu tespit edilmiştir. 755.485 adet kullanıcı bilgisayarı şifreleyiciler tarafından; 2.259.038 adet kullanıcı bilgisayarı da madenciler tarafından hedef alınmıştır. (Kaspersky, 2019)

Bilgi güvenliği harcamalarının 2020 yılında bir önceki yıla göre % 2,4 artarak 123,8 milyar dolara ulaşması beklenmektedir. (Gartner, 2020) Özel sektör yöneticilerinin % 68'i siber güvenlik risklerinin arttığını düşünmektedir. Siber saldırılar neticesinde ifşa edilen kayıt sayısı 2020'nin ilk çeyreğinde 2019 ilk çeyreğine kıyasla %273 artış göstererek ve tüm zamanların rekorunu kırarak 8,4 milyara ulaşmıştır. Bildirilen güvenlik ihlallerin yaklaşık %70'inin nedeni sistemlere veya hizmetlere yetkisiz erişim olmuştur. Açığa çıkan kayıtların yaklaşık % 90'ı çevrimiçi olarak ifşa edilmiştir. (RiskBased Security, 2020)

3. Büyüyen Siber Terörizm Tehdidi

Tıpkı bilgisayar korsanları gibi, teröristler de kendi hedeflerine erişebilmek için siber alanın teknolojik ilerlemelerinden istifade etmeye ve sunulan imkânları manipüle etmeye çalışmaktadır. Siber terörizm, genel itibarıyla bilgi işlem kaynaklarının başkalarını veya bütün toplumu sindirmek ve/veya zorlamak için kullanılması olarak tanımlanabilmektedir. Bir başka ifadeyle siber terörizm, bilgi ve bilgisayar sistemlerine, bilgisayar programlarına ve verilere yönelik olarak önceden tasarlanmış, politik olarak motive edilmiş saldırılar anlamına gelmektedir. Siber teröristler, diğer terörist türlerinden çok daha fazla zarar verme potansiyeline sahip yeni nesil teröristler olarak kabul edilmektedir. (Combs ve Slann, 2007: 71) Günümüzde terör örgütlerinin büyük bir kısmı bilgisayarları ve interneti iletişim, eleman devşirme, finansal yardım toplama, planlama, organizasyon, propaganda ve psikolojik savaş faaliyetlerinde aktif bir şekilde kullanmaktadır. Ayrıca siber altyapıyı istismar etmelerine imkân tanıyacak profesyonel yeteneklere erişmeye gayret etmektedir. Operasyonlarını desteklemek için dijital dosyalar, e-posta ve şifreleme gibi araçları kullanmaları gittikçe yaygınlaşmaktadır. Erişim kolaylığı, çok az sansür olması ya da hiç sansür olmaması, interneti bu grupların destekçileriyle iletişim halinde kalmaları, para toplamaları, saldırıları planlamaları ve yeni üyeler kazanmaları için ideal bir alan haline getirmektedir.

Siber dünyada terörist grupların varlığı yeni bir durum değildir. Teröristler ilk kuruluş aşamalarından bu yana internetin imkânlarından yararlanmaya çalışmaktadır. 1998 yılında ABD tarafından terör grupları listesinde yer alan 30 örgütün yaklaşık yarısının kendi internet sitesinin olduğu bilinmektedir. Günümüze ise hemen hemen bütün faal terör örgütleri, büyüklükleri, faaliyet yerleri ve kabiliyetleri ne olursa olsun siber dünyada bir şekilde varlığını sürdürmektedir. Bazılarının çok dilli ve farklı alanlara odaklanan çeşitli internet siteleri bulunmaktadır. Ayrıca, hemen hemen hepsi sosyal ağ sitelerinde, sohbet odalarında,

forumlarda ve gizlice topluma ulaşmalarına yardımcı olacak diğer halka açık etkileşimli platformlarda yer almaktadır. (Dilipraj, 2019: 77-83)

Hem hükümetler hem de özel sektör, siber terörist faaliyetleri engellemek için yoğun bir çaba göstermektedir. Fakat şunu ifade etmek gerekir ki bilgisayar teknolojisine eşlik eden hızlı değişiklikler göz önüne alındığında, hiçbir sistem hatasız ve tamamen güvenli değildir. Son yıllarda dünyanın çeşitli yerlerinde birçok misali yaşanan siber saldırılar, devletlerin ve kuruluşların altyapıları için kritik öneme sahip ağların ve sistemlerin fonksiyonlarının durmasına ve hatta toptan mahvolmasına yol açabilmektedir. Bu çerçevede, bu saldırılar siyasi, iktisadi ve toplumsal alanlarda tahrip edici etki yapma potansiyeline sahip tehditlerdir.

Profesör Gabriel Weimann interneti terör örgütleri için cazip kılan unsurlar şu şekilde sıralamaktadır: Kolay erişim sunması. Düzenleme, sansür veya diğer hükümet denetimi biçimlerinin çok az olması veya hiç olmaması. Potansiyel olarak büyük kitlelere erişim sağlaması. İletişimin anonimliği ve hızlı bilgi akışı. İnternette yer almanın ucuz olması. Etkileşimli bir multimedya ortamı sunması. Geleneksel kitle iletişim araçlarına bağımlılığını azaltması. (Weimann, 2006: 624)

Teröristlerin interneti kullanmaktaki öncelikli amaçlarından biri propaganda yapmaktır. Propaganda genellikle ideolojik veya pratik talimatlar, açıklamalar veya terörist faaliyetlerin tanıtımını kitlelere aktarmaya çalışan multimedya iletişimi biçimini almaktadır. Bunlar, terör örgütleri veya sempatanları tarafından geliştirilen sanal mesajları, sunumları, dergileri, bilimsel incelemeleri, ses/video dosyalarını ve video oyunlarını içerebilmektedir. İnternet teröristlerin kendilerine destek toplamak, fikirlerini duyurmak ve yaymak amacıyla halka ulaşmaları için yeni kanallar sunmaktadır. Şiddetin teşvik edilmesi, terörizmle ilgili propagandada ortak temalardan biridir. İnternetin sağlamış olduğu imkânlar, terör örgütlerinin propaganda konusunda geleneksel medya mecralarına olan bağımlılığını azaltmıştır.

Teröristlerin artık kamuoyuna sundukları mesajların içeriği üzerinde doğrudan kontrol sahibi olmaları, onlara söylemlerinde kendi imajlarını ve düşmanlarının imajlarını istedikleri gibi şekillendirme fırsatı vermektedir.

İnternet erişimi aynı zamanda terör örgütlerine sempatanlara ve potansiyel militanlara erişme imkânı sağlamaktadır. Bu kişilerin terörist örgüt hakkında bilgilendirilmesi, radikalleştirilmesi, desteklerinin kazanılması ve hatta doğrudan eylemlere yönlendirilebilmesi için elverişli bir alan sunmaktadır.

Çizgi film, popüler müzik videoları ve bilgisayar oyunları gibi araçları kullanarak küçük yaş gruplarını hedefleyebilmelerini mümkün kılmaktadır.

Terörist gruplar interneti aynı zamanda faaliyetlerini finanse etmekte de kullanabilmektedir. İnternet üzerinden doğrudan bağış toplayarak, elektronik ticaret yaparak, çevrimiçi ödeme sistemlerini manipüle ederek, çevrimiçi kumar faaliyetleri yürüterek, dark webde uyuşturucu ve illegal ürünleri satarak, dijital para hırsızlığı yaparak veya yardım kuruluşu görünümlü yapıları istismar ederek önemli finansal kaynaklara sahip olabilmektedir. İnternet ve mobil teknolojilerin sağlamış olduğu teknik imkânlar, terör örgütlerinin kara para aklamalarını da kolaylaştırmaktadır. Bitcoin benzeri dijital paralar, bu örgütlerin para transferlerini gizlice yapabilmelerini sağlamaktadır.

Son dönemde internet terör örgütleri için elemanlarını yetiştirme konusunda da alternatif bir platform haline gelmiştir. Bu örgütler bomba üretimi, silah kullanımı, terör örgütüne katılım yolları, terörist saldırı düzenleme yöntemleri gibi konularda hazırladıkları multimedya materyalleri vesilesiyle militanlarını kolayca ve risksiz bir şekilde eğitebilmektedir. Terör örgütleri ayrıca interneti eylemlerinin çeşitli aşamalarında planlama faaliyetlerinde kullanabilmektedir. Militanlarının uzak mesafelerden bir araya gelmeden iletişim halinde kalabilmeleri önemli bir avantaja dönüşmektedir.

4. Sanal Dünyada Siber Savaşlar

Günümüzde ülkeler için tehditler devletler ve devlet dışı aktörlerden gelebilmektedir. Asimetrik tehditler ve hibrit savaş taktikleri konvansiyonel savaş anlayışını dönüştürmektedir. Siber uzaydaki tehditler gerçektir, karmaşıktır ve sürekli gelişmektedir. Bunlardan belki de en önemlisi, ulus devlet aktörlerinin neden olduğu artan siber tehditlerdir. Siber yeteneklere sahip devletlerin sayısı, dünya genelinde yeni siber ordular kuruldukça artmaya devam etmektedir. Bu ülkeler yalnızca siber suç veya casusluk yapma potansiyeline değil; günlük yaşamımızda doğal gördüğümüz temel hizmetleri ve güvenliği etkileyebilecek yıkıcı saldırılar başlatma potansiyeline de sahiptir:

“Gelecekte, savaşlar sadece silahlı askerler veya bomba atan uçaklarla yapılmayacak. Ayrıca, dünyanın diğer ucunda bir fare tıklamasıyla, kamu hizmetleri, ulaşım, iletişim ve enerji gibi kritik endüstrileri bozan veya yok eden bilgisayar programları ile savaşılacak. Bu tür saldırılar, birliklerin hareketini, jet avcılarının yolunu, savaş gemilerinin komuta ve kontrolünü kontrol eden askeri ağları da devre dışı bırakabilecek. Güvenlik uzmanı Liam O’Murchu’nun da dediği gibi bir dahaki sefere savaş

açmak istediğimizde bir ülkeyi bombalamamız bile gerekmeyecek. Belki de sadece elektriğini ve güç kaynaklarını kesmek yetecek.” (Clayton, 2011)

Konvansiyonel savaşlarda fiziksel savaş alanının sınırlarını belirlemek genellikle kolaydır. İki ülke savaşa girdiğinde, iki ordu arasında aktif çatışmanın gerçekleştiği bir savaş alanı oluşur. Savaşlar geleneksel olarak kara, hava ve deniz üzerinde yapılmıştır. Ancak siber savaşlarda, nedenler ve sınırlar daha az tanımlanabilmektedir. Bu savaşlarda, kuvvetlerin çatıştığı belirli bir savaş alanı bulunmamaktadır. Taraflar gerilla taktiklerini ve asimetrik yöntemleri, geleneksel komuta kademesi veya doktrinler olmadan yürütmektedir. (Andress ve Winterfeld, 2014: 1-17)

Kinetik saldırıda hedef fiziki güç kullanılarak imha edilmektedir. Elektronik saldırıda hedefin lazer gibi bir odaklanmış enerjinin yönlendirilmesiyle imhası söz konusudur. Siber saldırıda ise bilgisayar sistemlerini veya yazılımları kontrol etmek için (akıllı) bir elektronik mesaj veya yazılım kodu kullanılmaktadır. (Porche, 2020: 22-23) Siber savaşlarda özellikle kritik altyapı ağları hedeflenmektedir. Çünkü bu altyapılar günümüzde komuta ve kontrol sistemlerini çalıştırmada, lojistiği yönetmede, personel planlaması yapmada, operasyonları yürütmekte ve istihbaratı sağlamada hayati öneme sahiptir. Silah sistemleri ve komuta kontrol sistemleri uydu ve internet ağlarına bağlıdır. Hava savunma sistemleri ve güdümlü füzeler GPS ağlarıyla çalışmaktadır. Hatta askeri personelin önemli bir kısmında yine iletişim, GPS, izleme, kamera ve gece görüş aletleri bulunmaktadır. Dolayısıyla orduları güçlendiren pek çok teknolojik yenilik, siber saldırı sonucu çökmesi halinde, orduların en zayıf noktası haline gelme potansiyeli taşımaktadır.

Siber casusluk, devlet ve devlet dışı aktörlerin askeri, politik veya ekonomik çıkar için kullanılabilecek hassas bilgileri çalmak için, kamusal ve özel bilgisayar sistemlerine ve ağlarına yönelik sızmalarını kapsamaktadır. Siber casusluk, gizli bilgileri elde etmeyi amaçlayan geleneksel istihbarat toplama operasyonlarına benzemektedir. Fakat burada uygulama platformu farklılık göstermektedir. Siber casusluk, devletlerin birbirlerine karşı kullandıkları yöntemlerden biri olarak gittikçe yaygınlaşmaktadır.

Bu tip tehlikelerle baş edebilmek adına siber caydırıcılık kavramı özellikle devletler bakımından son dönemde öne çıkmaktadır. Siber caydırıcılık, sahip olunan imkân ve teknikler sayesinde potansiyel düşmanların bir aktöre saldırı düzenlemeyi riskli görmesi ve karşı saldırıdan çekinmesi durumudur. Caydırıcı aktörün verebileceği cevaplar arasında doğrudan saldırganı hedef alan karşı

siber saldırı düzenlemek; saldırganın kullandığı altyapıyı, ekipmanı ve teknikleri ele geçirmek, etkisiz hale getirmek veya ifşa etmek bulunmaktadır. Ayrıca saldırgana verilen cevaplar siber alanla sınırlı kalmayıp, askeri, ekonomik, diplomatik ve yasal alanlarda da gerçekleşebilmektedir. (Springer, 2017: 53)

Günümüze dek ülkeleri hedef alan ciddi siber saldırılar gerçekleştirilmiştir. Bir devletin desteğiyle gerçekleştirilip kamuoyuna duyurulan ilk büyük siber saldırı 2003 yılından itibaren gerçekleştirilen ve Titan Rain ismi verilen geliştirilmiş Kalıcı Tehdit saldırılar dizisidir. Bu saldırılarda ABD ve İngiltere hükümetlerine ait bir dizi kurum hedef alınmıştır. Çin devletinin desteklediği iddia edilen aktörlerin gerçekleştirdiği saldırılarda ABD Dışişleri, Ulusal Güvenlik ve Enerji Bakanlıkları ile İngiltere Savunma ve Dışişleri Bakanlıklarının ağırları ihlal edilmiştir. ABD 2003'te başlayan saldırıların varlığını 2005 yılında açıklamış; İngiltere 2007 yılına kadar devam ettiğini bildirmiştir.

2007 yılında Estonya'nın parlamentosunun, bakanlıklarının, bankalarının ve medya organlarının internet siteleri siber saldırılar neticesinde çökertilmiştir. Saldırıların büyük bir kısmı Dağıtılmış Hizmet Reddi (DDoS) saldırıları şeklinde gerçekleşmiş ve Estonya yönetimi saldırılardan Rusya'yı sorumlu tutmuştur. Bu saldırı dünyada pek çok askeri kurumu harekete geçirmiş ve ağ güvenliğinin modern askeri doktrindeki yerini yeniden düşünmeye sevk etmiştir.

2008'de gerçekleşen Rusya-Gürcistan savaşı esnasında düzenlenen siber saldırılarda Güney Osetya, Rusya, Azerbaycan ve özellikle de Gürcistan'da bulunan çeşitli kurumların internet siteleri hedef alınmıştır. Böylelikle ilk defa ülkeler arasında fiziki alanda gerçekleştirilen savaşa siber saldırılar da eşlik etmiştir. Gürcistan'ı hedef alan siber saldırıların Rusya tarafından düzenlenen kara saldırısından hemen bir gün önce başlaması, saldırıların koordineli bir şekilde yürütüldüğünü düşündürmüştür. Saldırıların ilk kısmı DDoS saldırıları şeklinde gerçekleşmiş ve Gürcistan hükümeti ile medya organlarını etkilemiştir. İkinci aşamasında ayrıca finans kurumları, şirketler, eğitim kurumları ile CNN ve BBC gibi batılı medya kuruluşları hedef alınmıştır. (Shakarian, 2011: 63)

2010 yılında ortaya çıkan Stuxnet isimli solucan, siber savaş tekniklerinin geldiği aşamayı göstermesi bakımından bir dönüm noktası olmuştur. Bu kötü amaçlı solucan karmaşıktır ve yalnızca belirli bir sistemi hedef alacak şekilde tasarlanmıştır. Hedefin konumunu, sistem türünü ve daha fazlasını algılama yeteneğine sahiptir. Stuxnet, hedeflenen bilgisayarları basitçe ele geçirmek veya onlardan bilgi çalmak yerine; dijital ortamdan çıkıp bilgisayarların kontrol ettiği ekipmanlarda fiziksel yıkıma yol açmıştır. 15'ten fazla İran

tesisi Stuxnet solucanı tarafından saldırıya uğramıştır. Bu saldırının bir işçinin USB sürücüsü tarafından başlatıldığına inanılmaktadır. Etkilenen endüstriyel tesislerden biri Natanz nükleer tesisidir. Saldırı sonucunda tesisteki pek çok uranyum zenginleştirme santrifüjünün dönüş hızı oldukça yüksek bir seviyeye ayarlanarak, bu santrifüjler fiziksel olarak kullanılamaz hale gelmiş ve ülkenin nükleer programı birkaç yıl yavaşlamıştır.

2016 yılında ortaya çıkan Petya isimli kötü amaçlı yazılım özellikle Ukrayna'daki bakanlık, banka, medya ve elektrik şirketlerini hedef almıştır. Saldırı esnasında Ukrayna'daki Çernobil Nükleer Tesisinin radyasyon izleme sistemi kapanmıştır. Etkilenen bilgisayarlardaki dosyalar zarar görmüştür. Ayrıca bilgisayarlar çalışmaz hale gelerek ekranlarında fidye isteme mesajı çıkmıştır. Saldırı Ukrayna'nın Anayasa Günü'nün hemen öncesinde başlamış ve Ukrayna Milli Güvenlik ve Savunma Konseyi Sekreteri saldırılarda Rusya'nın rolü olduğunu öne sürmüştür.

Zaman zaman siber savaşlar konusunda düzenlemelere gidilmesi ve ülkeler arasında anlaşmalar yapılması konusu gündeme gelmektedir. Örneğin Rusya Devlet Başkanı Vladimir Putin 2020 Eylül'ünde Amerika Birleşik Devletleri'ne siber alanda ateşkes yapmayı teklif etmiştir. Yaptığı yazılı açıklama Putin şöyle demiştir:

“Günümüzün en büyük stratejik zorluklarından biri, dijital alanda büyük ölçekli bir çatışma riskidir. Uluslararası bilgi güvenliğini sağlama alanındaki kilit oyuncular, bunun önlenmesi konusunda özel bir sorumluluk taşımaktadır. Bu bağlamda, bilgi ve iletişim teknolojilerinin kullanımında güvenlik alanındaki ilişkilerimizi yeniden başlatmak için kapsamlı bir pratik önlemler programı üzerinde anlaşmaya varma önerisiyle bir kez daha ABD'ye çağrı yapmak istiyoruz. ABD de dâhil olmak üzere tüm ülkelere hitap ederek, bilgi güvenliği teknolojileri kullanarak ilk saldıran taraf olmama konusunda siyasi taahhütte bulunmaya davet ediyoruz.”
(Putin, 2020)

Siber saldırıların en önemli aktörlerinden olan Moskova yönetiminin bu çağrısı pek samimi bulunmamıştır. Çin gibi ülkelerin internette oturum açan herkesin gerçek kimliğini kullanması zorunluluğu getirilmesi gibi teklifleri de olumlu karşılanmamaktadır. Ayrıca genel olarak 1960'lardan itibaren silahların azaltılmasına yol açan anlaşmaların siber uzayda işe yaramayacağı düşünülmektedir. Nükleer silahlar az sayıda devletin elindeyken; siber silahlar devletler, suç grupları, aktivistler ve hatta gençler tarafından kontrol edilebilmektedir. Çoğu zaman, devletler siber faaliyetlerini suç örgütleri üzerinden yürütmektedir. Böyle bir ortamda yapılacak anlaşma girişimlerinin boşa çıkacağı aşikârdır.

5. Türkiye’de Siber Güvenlik

Dijital ve teknolojik gelişmeleri yakından takip eden ve internet kullanım oranı oldukça yükselen Türkiye de siber saldırıların önemli hedeflerinden biri haline gelmiştir. Hem kamu kurumları hem de özel şirketler ve bireyler bu saldırılardan payını almaktadır. Örneğin, bütün siber suçlardan Türkiye’de sadece 2019’da işlem yapılan toplam hesap sayısı 30.617 ve bu suçlardan yakalanan şahıs sayısı 17.102’dir. Bu suçların büyük çoğunluğunu terör propagandası yapma suçu teşkil etmektedir. Aşağıdaki tabloda da görüldüğü üzere, işlem yapılan hesapların %98.7’si, yakalanan şahısların ise %89.7’si terör propagandası suçu ile ilişkilidir.

Tablo 1. Türkiye’de 2019 Yılı Siber Suçlara İlişkin İşlem Yapılan Hesap ve Kişi Sayıları

	Terör Propagandası	Yasadışı Bahis	Phishing (Oltalama)	Kart Kopyalama
İşlem Yapılan Hesap Sayısı	15.333	1.323	249	197
Yakalanan Şahıs Sayısı	30.205	173	40	199

Kaynak: İç Güvenlik Stratejileri Dairesi Başkanlığı, 2020

Türkiye siber güvenliği sağlama noktasında birçok önlemleri ve yapılanmayı hayata geçirmiştir. Örneğin, Bakanlar Kurulu Kararı ile 2011 yılında Emniyet Genel Müdürlüğü bünyesinde Bilişim Suçlarıyla Mücadele Daire Başkanlığı kurulmuştur. Daha sonra 2013 yılında ismi Siber Suçlarla Mücadele Daire Başkanlığı olarak değiştirilmiştir. Başkanlık temel hedeflerini “siber suçlarla mücadele etmek, siber suçlar konusunda toplumda farkındalık oluşturmak, bu konuda uluslararası işbirliklerini artırmak” olarak belirlemiştir. Ayrıca “Türkiye’ye yönelik siber suç tehditlerini değerlendirmeyi, gerekli analizler yapmayı, bu tehditlerle mücadele etmeyi ve siber suçlarla mücadelede alanında uzman soruşturmacı ve adli bilişim personelleri yetiştirmeyi” amaç edinmiştir. (Siber Suçlarla Mücadele Daire Başkanlığı, 2020)

Bakanlar Kurulu tarafından 2012 yılında “Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar” yayınlanmıştır. Bu karar ile “kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda yer alan sistemlerin güvenliğinin sağlanmasına ve gizliliğinin korunmasına”

yönelik tedbirlerin alınması hedeflenmiştir. Ayrıca “bilgi ve iletişim teknolojilerine ilişkin kritik altyapıların işletiminde yer alan gerçek ve tüzel kişilerce uyulması gerekli usul ve esaslar düzenlenmiştir.” Bu karar kapsamında “siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak” maksadıyla Siber Güvenlik Kurulu kurulmuştur. Bu kurul, Dışişleri, İçişleri, Milli Savunma, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı müsteşarları, MİT Müsteşarı, BTK Başkanı, Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı, Telekomünikasyon İletişim Başkanı, TÜBİTAK Başkanı, Mali Suçları Araştırma Kurulu Başkanı ve diğer bazı bakanlık ve kamu kurumu üst düzey yöneticilerinden oluşmaktadır. (Bakanlar Kurulu, 2012)

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından 2013 yılında bütün Bakanlıklar ve diğer tüm kamu kurum ve kuruluşlarına kendi bünyelerinde Siber Olaylara Müdahale Ekipleri (SOME) kurmalarına dair tebliğ gönderilmiştir. Bu ekipler “kurumlarına doğrudan ya da dolaylı olarak yapılan veya yapılması muhtemel siber saldırılara karşı gerekli önlemleri alma veya aldırma, bu tür olaylara karşı müdahale edebilecek mekanizmayı ve olay kayıt sistemlerini kurma veya kurdurma ve kurumlarının bilgi güvenliğini sağlamak ya yönelik çalışmaları yapma veya yaptırmakla” görevlendirilmiştir. Kurumsal ve sektörel SOME’lerin eşgüdümünü sağlamak üzere Bilgi Teknolojileri ve İletişim Kurumu bünyesinde Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT) kurulmuştur. Bu merkezin temel amacı, “Türkiye’nin siber güvenliğine karşı siber ortamda ortaya çıkan tehditlerin belirlenmesi, muhtemel saldırı ve olayların etkilerini azaltılması veya ortadan kaldırılmasına yönelik önlemlerin geliştirilmesi ve belirlenen aktörlerle” paylaşılması olarak belirlenmiştir. (Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, 2013)

Son dönemde artan siber terör tehdidi ve yaşanan büyük çaplı felaketlerin ülkeleri kritik altyapıların korunması ile ilgili politika, strateji, mevzuat, plan ve programlar yapmaya itmektedir. Bu kapsamda, 5902 sayılı kanun gereğince; afet ve acil durumlar ile sivil savunmaya ilişkin hizmetlerin ülke düzeyinde etkin bir şekilde gerçekleştirilmesinden sorumlu kılınan İçişleri Bakanlığı Afet ve Acil Durum Yönetimi Başkanlığı (AFAD), teknolojik afetlerin etkin yönetimi amacıyla “Kritik Altyapıların Korunması Yol Haritası Belgesi” hazırlamıştır. Bu belge çerçevesinde, “endüstriyel, maden, ulaşım ve taşımacılık, nükleer ve radyolojik, deniz kirliliğine neden olan kazalar, büyük yangınlar, biyolojik olaylar, kritik altyapılar ve siber tehditler ile çevresel tehlikeler

gibi... afet ya da acil durumlar” olarak tanımlanan teknolojik afetlerle mücadelenin yol haritası çizilmiştir. (AFAD, 2014)

2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planında siber savunmanın kuvvetlendirilmesi, siber tehditler konusunda farkındalığın yükseltilmesi, kritik altyapıların tehditlere karşı korunması, siber alanda çalışacak kalifiye insan kaynağı yetiştirilmesi, siber güvenlik ekosisteminin güçlendirilmesi ve siber güvenlik ile milli güvenlik anlayışının bütünleşmesi hedeflenmiştir. “Toplumun refahı ve güvenliği ile ülke ekonomisinin büyümesine ve verimliliğine katkı sağlamak üzere bilgi ve iletişim teknolojilerinden en etkin şekilde faydalanılabilmesi için, siber güvenlikle ilgili tüm paydaşların işbirliği içinde siber uzaydaki riskleri yetkin bir biçimde yönettikleri, siber güvenlik alanında uluslararası rekabet gücüne sahip bir ekosistemin oluşması” vizyonu benimsenmiştir. (Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, 2020)

Türk Silahlı Kuvvetleri (TSK) Siber Savunma Komutanlığı, öncelikle TSK’ya yönelebilecek siber tehditleri önceden tespit etmeye ve önleyebilmeye yönelik faaliyetler yürütmektedir. Ayrıca, diğer kurum ve kuruluşlarla bilgi paylaşımı yaparak, Türkiye’nin siber savunma ağını güçlendirmeyi hedeflemektedir. Komutanlık bünyesindeki Siber Savunma Harekât Merkezi, dünyadaki siber olayların gerçek zamanlı takibini yapmaktadır. Komutanlık genel itibarıyla mevcut risk ve tehditlere karşı TSK’nın siber savunma yeteneklerini geliştirmeye odaklanmaktadır. Ayrıca gelecek dönem ihtiyaçlarının karşılanması amacıyla kaynak tahsisleri planlamakta ve milli siber savunma projeleri geliştirmektedir.

Cumhurbaşkanlık Savunma Sanayii Başkanlığı himayesinde ve Dijital Dönüşüm Ofisinin desteğiyle 2018 yılında Türkiye Siber Güvenlik Kümelenmesi kurulmuştur. Bu proje temel olarak ulusal bir siber güvenlik ekosistemi kurmayı; yerel/ulusal siber güvenlik ürünleri geliştirmeyi ve bu ürünlerin kullanımını yaygınlaştırmayı amaçlamaktadır. Bu misyon doğrultusunda, siber güvenlik alanında teknoloji üreten ve dünya ile rekabet edebilen bir Türkiye hedeflenmektedir. Türkiye’nin siber güvenlik ihtiyaçlarının tespit edilerek, özel sektör girişimlerinin sağlıklı bir rekabet ortamında gelişebilmeleri bu noktada önem taşımaktadır.

SONUÇ

Dijital, mobil ve sosyal medya tüm dünyadaki insanlar için günlük yaşamın vazgeçilmez bir parçası haline gelmektedir. Dünya nüfusunun yaklaşık yüzde 60’ı hâlihazırda çevrimiçidir ve dünya nüfusunun yarısı sosyal medyayı kullanmaktadır. Mobil aktiviteler içerisinde mobil uygulamalarda geçirilen

sürenin payı %90'ı aşmıştır. Ocak 2019 ila Ocak 2020 arasındaki bir yıllık süreçte dünya nüfusu sadece %1.1 artmışken, cep telefonu kullanıcısı sayısı %2.3, internet kullanıcısı sayısı %7 ve aktif sosyal medya kullanıcısı sayısı %9.2 artmıştır. (WeAreSocial ve Hootsuiye, 2020) Dolayısıyla dünya nüfusu hızla dijital dünya ile bağlanmaktadır. Akıllı termostatlar, sesle etkinleştirilen asistanlar ve web özellikli televizyonlar gibi internete bağlı cihazlar evlerde yaygın hale gelmektedir. Bu teknolojiler, tüketiciler ve işletmelerin kolaylık, verimlilik ve eğlence için akıllı cihazlara akın etmesiyle son yıllarda gelişen Nesnelerin İnternetinin bir parçasıdır. Bedenlerin İnterneti insanlar ve cihazlar arasında daha da yakın bir etkileşim sağlamaktadır. Bu cihazlar insanların fiziki konumunu takip etmekte; vücut fonksiyonlarını izlemekte; mahrem bilgilerini toplamakta ve internet üzerinden depolamaktadır.

Siber saldırılar, belirli bir siyasi, ekonomik veya toplumsal amaca ulaşabilmek için bilgisayar sistemlerinden istifade ederek, devlet kurumlarına, özel sektöre veya bireylere saldırıp, onları yıpratma, yıldırma, korkutma, sindirme ve zorlama gayesi taşıyan eylemlerdir. Bu saldırılar nedeniyle ulaşım ve telekomünikasyon hizmetleri aksayabilmekte, doğalgaz/elektrik/su şebekeleri zarar görebilmekte, bankacılık ve finans sektörü manipüle edilebilmektedir. Barajlar, kimyasal fabrikalar ve nükleer tesisler gibi kritik yapılar çalışmaz hale getirilebilmektedir. İtfaiye, sağlık ve emniyet gibi kamu hizmetleri akamete uğratılabilmektedir. Bunun yanında, kritik sitelere erişim engellenerek, toplumda karışıklık veya panik havası oluşmasına yol açılabilmektedir. Siber altyapılar kullanılarak terör örgütlerinin propaganda yapma, finans kaynağı toplama, terör saldırısı organize etme, militan devşirme ve eğitme gibi faaliyetleri yürütülebilmektedir. Hatta devlet aktörleri arasında gerçekleşen siber saldırılar, geleneksel savaş konseptini dönüştürebilmektedir.

Önümüzdeki süreçte siber suç, kolluk kuvvetlerinin iç güvenliği sağlama bakımından giderek daha fazla mücadele edeceği büyük bir sorun olmaya devam edecektir. Bilgi teknolojilerindeki küresel büyüme, üretkenlik, ticaret, iletişim, eğlence ve bilginin yayılmasında benzersiz ilerlemeler sağlamaktadır. Fakat aynı zamanda, yeni yasadışı davranış biçimlerinin ortaya çıkışını da hızlandırmaktadır. Giderek daha fazla kullanıcı dijital teknolojiye adapte oldukça, sorunun kapsamı ve yaygınlığı artmaktadır.

Türkiye’de ve dünyada siber tehditlerin seviyesinin hızla artması, kolluk kuvvetlerinin toplumu ve devleti bu tür tehlikelerden korumadaki rolünü artırmaktadır. Dolayısıyla bu kurumlar bünyelerinde siber saldırılarla mücadele-den sorumlu uzman birimler oluşturmaktadır. Bu alandaki faaliyetlerin başa-

rısı, bu tür birimlerin etkinliğinin yanı sıra, yurtdışı aktörlerle ve özel sektörle işbirliği yapılmasına bağlıdır.

Okuma Parçası: Çalışanlar İçin Siber Farkındalık²

Bilişim teknolojilerinin gelişimi ile beraber siber saldırılar da artmaktadır. Özel ve tüzel kişiler, bu saldırılara teknoloji kullanarak karşılık koysalar da yapılan çalışmalar, kurumlardaki veri sızıntılarının çoğunlukla çalışan kaynaklı olduğu gerçeği, siber güvenlikte “insan faktörünün” önemine dikkat çekmektedir. Siber saldırılarda en büyük hedefi oluşturan çalışanlar, daha çok e-posta ve sosyal medya kanalları üzerinden hedef alınmaktadır. Bu nedenle çalışanlar için siber güvenlik farkındalığı oluşturmak hayati önem taşımaktadır.

Çalışanlara Bilgi Güvenliği Farkındalığı Eğitimi

Bilgisayar sistemine saldırılar sadece internet üzerinden yapılmamaktadır. Ofisinize ziyaretçi, temizlikçi, bilgisayar teknik destek uzmanı gibi çeşitli üvanlarla gelen kimseler ya da art niyetli çalışanlar da teknolojik saldırıların parçası olabilir. Bu nedenle masa üzerinde ya da Monitör yanına iliştilirilmiş Wi-Fi parolası, bilgisayar parolaları ya da kredi kartı bilgisi gibi bilgi kırıntıları saldırganlar için fırsat oluşturmaktadır. Bu nedenle bir saldırı esnasında kullanılabilecek bilgilerin ortada bırakılmaması, çalışma masaları üzerinde kıymetli evrak bırakılmaması, bilgisayar ve telefon gibi ekipmanların yanından ayrılırken mutlaka ekran kilidi uygulanması hayatidir. Benzer biçimde parola ve pin giriş ekranlarını kullanırken omuz üstünden kimsenin görmediğinden emin olunmalıdır.

Sistemin korunduğu gibi giriş bilgilerinin de korunması önemlidir. Sisteme yetkisiz kişilerin girmesini önlemek için bütün girişler herkese ayrı atanmış kişisel kullanıcı adları ve parolalar ile yapılmalıdır. Böylece bir aksilik olduğunda kimin hesabının probleme neden olduğu net şekilde tespit edilip izlenebilir hale gelecektir; paylaşılan parolalar tehlikelidir.

Bilgisayarlar ve programlar için parola seçerken parolaların kolayca tahmin edilemeyecek sözcükler seçilmesi önemlidir; harf, rakam ve noktalama işaretlerinin karışımından oluşan asgari 8 basamaklı parolaların kullanılması önerilir. Bu parolalar akılda tutulmalı, kağıda ya da bir bilgisayar dosyasına not edilmemelidir.

² Siber Suçlarla Mücadele Daire Başkanlığı, <https://www.siberay.com/calisan-farkindaligi> (10/11/2020).

Çalışanlara bu temel konuları aktarmak üzere “Bilgi Güvenliği Farkındalığı” eğitimleri verilmelidir. Görevinden bağımsız tüm çalışanlara verilecek birkaç saatlik temel eğitimler ile çalışanların da kuruluşun güvenliğini sağlamaya katkısı sağlanabilir; bugün harcanacak birkaç saat yarın kuruluş açısından hayat kurtarıcı olabilir.

Zararlı Yazılımlar ile Mücadele

Siber saldırılar sıklıkla virüs vb. zararlı yazılımlarla yapılmaktadır. Zararlı yazılımlar bilgisayarlara (kişisel bilgisayarlar ve sunuculara) USB flash bellek takılması, mail yoluyla gelen dosya/dosyaların açılması, internetten program/dosya indirilmesi, anlık mesajlaşma ile gelen dosya eklentileri ve ziyaret edilen siteler aracılığı ile bulaşabilir. Bu nedenle kaynağı belirsiz flash bellekler kullanılmamalı, bilgisayarlar üzerinde sürekli güncellenen bir koruma yazılımı çalıştırılmalı (anti-virüs, endpoint protection vb.), bilgisayarların güncellemeleri sürekli güncellenmelidir. Özellikle sunucu bilgisayarlarda web tarayıcısı çalıştırarak internette gezilmemeli, USB bellek ile dosya aktarmak yerine yerel ağdaki bir bilgisayardan dosya taşınması sağlanmalıdır.

Oltaama ile Mücadele

Oltaama (phishing), kuruluş çalışanlarından bir ya da daha fazlasına yem olarak nitelendirilen e-posta mesajlarının gönderilmesi ve onların mesajdaki yemi yutarak beklenen davranışı sergilemesi üzerine kurulmuş basit ancak etkili bir saldırı tekniğidir. Yanlışlıkla iletilmiş bir ‘Yıllık Maaş Artışları Planı’ eki pek çok çalışanı cezbedebilirdi. Ekli dosya zararlı yazılım barındırabilir ya da maaş artış planlarına ilişkin bir yem linki çalışanları tıklamak için cezbedebilir.

Oltaama saldırıları tüm çalışanlara yaygın olabileceği gibi dikkat çekmemek üzere az sayıda çalışanı da hedef alabilir. Unutulmaması gereken kuruluştaki bir bilgisayara sızmayı başaran saldırganın diğer bilgisayarlara sıçramasının artık çok daha kolay olacağıdır. Bu bağlamda kaynağı belli olmayan veya olağan dışı mesajlar alınması halinde mesajın açılmadan kuruluşun siber güvenlik uzmanlarına iletilmesi sağlanmalıdır.

Çalışanlar İçin Yetki Sınıflandırılması

Kuruluşlar tüm çalışanlarının bilgisayarları ve programları aynı yetki seviyesi ile kullanmasına imkan vermemelidir. Her çalışana özel ve ayrı birer kullanıcı girişi ve şifresi tanımlanmalı, hangi çalışanın hangi program üzerine hangi işlemleri yapabileceği net olarak tanımlanmalıdır.

Kimin hangi program üzerinde ne yapıp ne yapamayacağı net şekilde tanımlandığında hem çalışanların hatalarından kaynaklanabilecek riskler azaltılır hem de bir çalışanın hesabını ele geçiren saldırganın yapabilecekleri kısıtlanmış olur.

Lisanslı Ürün Kullanımı Eğitimi

İşletme ve kurumlar, bilgisayar ve sunucularını siber saldırılardan korumak için güvenlik yazılımları ve programları kurmaları önemli bulunduğundan bu sektörde deneyimli ve alanında uzman firmalarla anlaşma yapmaları gerekmektedir. Bu firmalardan yardım-destek alınarak sistemler güvenli hale getirilebilir ve bu firmalardan personel eğitimi de alınabilmektedir.

Kurum ve çalışanların lisanssız ürünlerden uzak durmaları gerekmektedir. Lisanslı olmayan bir programın kurulması ve crack yapılması, bilgisayarın kötü niyetli kişiler tarafından ele geçirilmesine veya çökmesine yol açabilir!

KAYNAKÇA

- Accenture Security (2019). Ninth Annual Cost of Cybercrime Study, https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf (23/10/2020).
- Afet ve Acil Durum Yönetimi Başkanlığı (2014). 2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi.
- Andress J. ve S. Winterfeld (2014). Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. New York: Elsevier.
- Bakanlar Kurulu (2012). Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar, <https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf> (25/10/2020).
- Clayton, M. (2011). "The new cyber arms race". Christian Science Monitor. <https://www.csmonitor.com/USA/Military/2011/0307/The-new-cyber-arms-race> (01/10/2020).
- Cockcroft, Tom, Shan-A-Khuda, Mohammad, Schreuders, Z Cliffe, Trevorrow, Pip. (2018) "Police Cybercrime Training: Perceptions, Pedagogy, and Policy" Policing: A Journal of Policy and Practice
- Combs, C. C. ve M. W. Slann (2007). Encyclopedia of Terrorism. New York: Facts On File, Inc.
- Cybercrime Magazine (2020). Cybercrime Damages \$6 Trillion By 2021, <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016> (07/10/2020).
- Dilipraj, E. (2019). Cyber Enigma: Unravelling the Terror in the Cyber World. London: Routledge.
- Edwards, G. (2020). Cybercrime Investigators Handbook, New Jersey: John Wiley & Sons, Inc.
- Gartner (17 Haziran 2020). "Gartner Forecasts Worldwide Security and Risk Management Spending Growth to Slow but Remain Positive in 2020" Basın Açıklaması.
- Hinduja, S. ve J. Patchin (2011). The Future of Crime. The Future of Policing: A Practical Guide for Police Managers and Leaders. (Ed. J. A. Schafer, M. E. Buerger, R. W. Myers, C. J. Jensen ve B. H. Levin) New York: CRC Press.
- Holt, T.J., A. M. Bossler ve K. C. Seigfried-Spellar (2018). Cybercrime and Digital Forensics: An Introduction. London: Routledge.
- Homeland Security (2020). Insider Threat, <https://www.dhs.gov/science-and-technology/cybersecurity-insider-threat> (08/11/2020).
- İç Güvenlik Stratejileri Dairesi Başkanlığı (2020). İç Güvenlik Gelişmeleri Raporu 2019 Yıllığı. Ankara.

- Kaloudi, N. ve J. Li (2020). "The AI-Based Cyber Threat Landscape: A Survey". *ACM Computing Surveys*, 53(1).
- Kaspersky (2019). Kaspersky Security Bulletin 2019, <https://securelist.com/ksb-2019> (03/11/2020).
- Kaspersky (2020). Drive-by attack, <https://encyclopedia.kaspersky.com/glossary/drive-by-attack> (05/11/2020).
- McAfee, (2020). What is malware?, <https://www.mcafee.com/en-us/antivirus/malware.html> (28/10/2020).
- Morgan, S. (2020). Cybercrime Infographics: Illustrations Of The Past, Present, And Future Threats We Face. *Cybercrime Magazine*, <https://cybersecurityventures.com/cybercrime-infographic> (05/11/2020).
- Norton (2020). What is a Distributed Denial of Service Attack (DDoS) and what can you do about them?, <https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html> (18/10/2020).
- Porche, I. R. (2020). *Cyberwarfare: An Introduction to Information-Age Conflict*. Boston: Artech House.
- Putin, V. (2020) "Statement by President of Russia Vladimir Putin on a comprehensive program of measures for restoring the Russia – US cooperation in the field of international information security", 25 Eylül.
- RiskBased Security (2020). "2020 Q1 Report: Data Breach QuickView", <https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Q1%20Data%20Breach%20QuickView%20Report.pdf> (18/10/2020).
- Shakarian, P. (2011). "The 2008 Russian Cyber Campaign Against Georgia". *Military Review*. November-December.
- Siber Suçlarla Mücadele Daire Başkanlığı, <https://www.egm.gov.tr/siber/hakkimizda2> (01/11/2020)
- Springer, P. J. (2017). *Encyclopedia of Cyber Warfare*. California: ABC-Clío.
- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, 2016-2019 Ulusal Siber Güvenlik Stratejisi, <https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/2016-2019guvenlik.pdf> (04/11/2020).
- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev Ve Çalışmalarına Dair Usul Ve Esaslar Hakkında Tebliğ, <https://www.resmigazete.gov.tr/eskiler/2013/11/20131111-6.htm> (22/10/2020).
- We are Social ve Hootsuite (2020). Digital 2020: Global Digital Overview, <https://wearesocial.com/digital-2020> (10/11/2020).
- Weimann, G. (2006). "Virtual Disputes: The Use of the Internet for Terrorist Debates". *Studies in Conflict & Terrorism*, 29.



P O L İ S A K A D E M İ S İ