BİLGİSAYARLAR ARTIK YALNIZCA BİZİM DEĞİL, TERÖRİSTLERİN DE VAZGEÇİLMEZİ

SİBER-TERÖRİZM

Amerikan toplumu tarihte bağımsızlık, ırk ayrımı, sivil savaş, dünya savaşı, soğuk savaş, toplumsal ayrımcılık, terörizm, ölümcül salgın hastalıklar ve ana bilgisayar sistemlerindeki aksamalar gibi birçok tehditle karşı karşıya kaldı. Günümüzde bunların çoğu artık tarihe karışmış olsa da, yaşandıkları dönemde kamuoyunun ve basının yoğun ilgisini çekti. İçinde yaşadığımız bilgisayar çağıysa daha az tanıdık ve daha çok korkutucu bir tehdidi beraberinde getirdi: siber-terörizm.

Durmaksızın ilerleyen teknolojik gelişmeler, hayatlarımızı kolaylaştırmayı sürdürüyor. Olanaklarını önümüze sakınmadan sunan teknoloji, teröristlerden de kendini esirgemiyor. Bilgi çağıyla birlikte her geçen gün daha "akıllı" hale gelen teröristlerin teknolojiyle kurdukları ilişki geliştikçe, eylemlerdeki uzmanlıkları da artıyor. Bu durum terör eylemlerinin bombalama, gasp, uçak kaçırma, rehin alma gibi alışılmış eylemlerin ötesine geçerek "ileri-teknoloji terörizmi"ne terfi etmesi potansiyelini içinde barındırıyor.

Bilgisayarlar Tehdit Altında

Doğuşunu teknolojiye borçlu olan bu yeni terör biçimi, teknoloji merkezlerine yönelik terör eylemleri ve teknolojiyi kullanarak gerçekleştirilen terör eylemleri olmak üzere iki ayrı ana başlık halinde ele alınabilir. Teröristlerin herhangi bir bilgisayar merkezine yapacakları küçük bir bombalı saldırının herhangi başka bir saldırıdan çok daha fazla zarar getirebileceğinin farkında olmaları ciddi bir sorun. Geçmişte yaşanan örnekler, teröristlerin bilgisayar merkezlerini imha etmedeki kararlılıklarını koruduklarını gösteriyor. Teröristlerin ve eylemcilerin özel ya da resmi irili ufaklı 1.000'den fazla bilgisayar kuruluşunu bombaladığı göz önüne alınırsa, terörizm dünya genelindeki bilgisayar iletişimi için ciddi bir tehdit olarak ortaya çıkıyor.

Eskiden erim dışında olan yeni hedeflerin ortaya çıkması nedeniyle terörizm son yirmi yılda ciddi bir artış gösterdi. "Yeni hedefler" terimi gelişmiş sanayi toplumlarının terörist eylemler için uygun hedefler yarattığı anlamına geliyor. Uçaklar, büyük tankerler, uluslararası güç şebekeleri ve boru hatları, nakliye merkezleri, ticari iletişim merkezleri, otomobil konvoyları, mazot gemileri, nükleer güç merkezleri ve bilgisayarlı bilgi ve işletim merkezleri bu hedeflerden başlıcaları. Dünyadaki terörist eylemlerin % 60'ını bilgisayar merkezlerine yapılan eylemler oluşturuyor. Her ofisi ve fabrikayı korumaya kalkmak pahalı olsa da, bunları terörist saldırılara karşı daha güvenli hale getirmek için bazı değişikliklerin yapılması zorunlu. Boston'daki terör karşıtı bir birimin başkanlığını yürüten Federal Soruşturma Bürosu (FBI) ajanlarından Neil Gallagher, 1986'da şöyle söylüyordu: "Yalnızca Batı Almanya'da 24 merkezin bombalandığı gözönüne alınırsa, bilgisayar merkezlerine yönelik bombalı saldırılarda ciddi bir artış olduğu açık. Korkutucu olan şu ki, toplumumuzun bilgisayarlara olan bağımlılığı arttıkça risk de büyüyor. Toplumun normal işlemlerinde bilgisayarlara olan bağımlılığındaki artış, uğrayacakları zarar beyin ölümüne benzetilebilecek riskler barındıran kritik düğüm noktaları oluşturuyor. Bu nedenle, bilgisayarlara karşı girişilecek bir sabotaj sonucu ortaya çıkacak büyük bir toplumsal parçalanma ve ekonomik kayıp potansiyeli artmış durumda."

Kritik noktalardaki 100 bilgisayara karşı akıllıca düzenlenmiş bir terör eylemi, Amerika'nın ekonomisini bir anda sekteye uğratabilir. Bu düşünceyi paylaşan Bilgisayar Terörizmi'ne Karşı Uluslararası Birlik'in yöneticisi Winn Schwartau'nun yazdığı "Terminal Compromise" adlı roman, bugün belki de gerçeğe dönmüş durumda: "Bilgisayarlara karşı gerçekleştirilen terör eylemleri uzaktan kontrol edilen görünmez alanlarda savaşmak, çok büyük zararlar vermek ve ardında hiç iz bırakmadan kaç-

mak için ideal bir mekanizma sağlıyor. Devlet politikaları ve eylemleri, ABD enformasyon toplumunun temel dayanağı olan 70.000.000 bilgisayarla bu ülkenin olası bir saldırıya karşı savunmasız, en derin zaafını yarattı." 1978 yılında Londra Dışişleri Araştırma Enstitüsü, Dominic Baron'ın hazırladığı "akıllı teröristler" adında 10 sayfalık bir rapor yayınladı. Bu raporda modern bir sanayi devletinin bilgisayar sistemlerine yönelik bir terörist eylemle nasıl felce uğratılabileceği açıklanıyordu. Baron, özetle, şöyle diyordu: "Belli başlı bilgisayar kurumlarına giriş bir suçlu için de, iyi bir vatandaşa olduğu kadar açık. Bu nedenle "elektronik teröristler" için bazı güvenlik sistemlerinin en zayıf noktalarına yönelik stratejik planlar kurmak zor olmayacaktır."

Bilgisayarlar Teröristlerin Emrinde

Teknolojik gelişmelerle birlikte daha "akıllı" hale gelen teröristler, bilgisayar merkezlerine yapacakları saldırıların etkinliğini farketmekle kal-

CIA'in kırılan web sitesinde kurumun adı "Merkezi Aptallık Kurumu" olarak değiştirilmişti.

mayıp, eylemlerini düzenlerken bilgisayarlardan yardım almayı akıl edecek kadar zekiler. Hedefin bilgisayar olduğu eylemlerde yöntem sabotaj yoluyla bilgisayara zarar verilmesi ya da kullanımının tamamen durdurulmasıyken, bilgisayar eylem aracı olarak kullanılmaya kalkıldığında uygulanacak yöntem, bilgisayardaki verilerin değiştirilmesi ya da kopyalanması. Bu senaryonun başrolünü oynayan "hacker"lar, birinci yöntemi uygulayan teröristlerin yaptığı gibi bilgisayar merkezlerini bombalamak yerine sistemin merkezine virüs göndererek ya da sistemi kırıp içine girme yoluyla bilgi çalarak saldırmayı tercih ediyor. Bilgisayar virüslerinin heryıl % 47 oranında artış gösterdiği göz önüne alınırsa, geleceğin "Carlos"unun Çek yapımı bir VZ61 makineli tabanca yerine, bir IBM PC ile silahlanmış olması pek de şaşırtıcı olmaz.

Modern elektronik teknolojisi teröristlerin şantaj, adam kaçırma, cinayet ve bombalama gibi bazı eski tekniklerinin üzerinde yeni değişiklikler yaratmalarına da yardımcı oluyor. Örneğin modern dijital elektronik saatler, aylar ya da yıllarca sonrasına ayarlanabilecek dijital saatli bombalar yapılmasına olanak sağlıyor. Güney Amerika, Avrupa ve Filipinler'de teröristlerin saklandıkları yerlere yapılan baskınlar, çoğunun birer bilgisayar, modem ve veritabanı yazılımına sahip olduğunu gösterdi. Bu da geleceğin teröristlerinin tek bir bilgisayar tuşuna basarak, bombayla gerçekleştirilebilecek bir zarardan çok daha fazlasına neden olabilecekleri anlamına geliyor. Bilgisayarlar birer silah olmasalar da yanlış kişilerce kullanıldıklarında kendi enformasyon sistemlerimiz, namluları kendi üzerimize yönelmiş silahlar haline gelebilir.

Tarihten Bazı Örnekler

1996 yılının Eylül ayında yaşanan CIA web sitesi'nin kırılması olayında kurumun gizli dosyalarına giriş sağlanamamış olsa da, sitenin içinde yer alan tüm bilgilerin değiştirilmesi bile oldukça büyük etki yarattı. CIA'ye telefon ederek bu olaydan haberdar olmalarını sağlayan ses, siteyi kıran kişiye aitti. Bu olaydan bir ay önce de ABD Adalet Bakanlığı'nın sitesine girilmiş ve siteye Adolf Hitler'in fotoğrafı yerleştirilmişti.

1999 yılının Ocak ayında San Antonio'daki Kelly Hava Kuvvetleri Üssü'nün bilgisayarları iki gün boyunca sürekli olarak hacker saldırısına uğradı. NBC'nin verdiği haberlere göre bu eylem Kanada, Norveç ve Tayland'daki ağlar üzerinden deneyimli kişiler tarafından düzenlenmiş koordineli bir saldırıydı. Hackerlar önemli gizli bilgilere ulaşamamış olsalar da, ABD Savunma Bakan Yardımcısı John Hamre'ye göre bu olayla ABD kendini oldukça ciddi bir siber savaşın içinde buldu. Bu olaydan sonraki aylarda Pentagon'daki bilgisayarlar dünya genelindeki yaklaşık 15 ayrı merkezden, günde yaklaşık 100 saldırıya uğradı. Bu saldırılar sonucunda oldukça endişeye kapılan Pentagon, konuyla ilgili olarak FBI'yı görevlendirdi. Resmi görevlilere göre saldırıların nereden geldiğinin belirlenmesi, özel bir teknoloji geliştirilmesini gerektiriyordu. Gerekli bu teknoloji Deniz Kuvvetleri tarafından geliştirildi. Ancak Kelly Hava Üssü'ne yapılan saldırıların nereden geldiğini belirleyen bu teknoloji, hackerların kendilerini bulmakta yetersiz kaldı. Pentagon'daki görevliler askeriyenin en gizli sırlarının hala güvende olduğunu düşünseler de, bilgisayar teröristlerinin uzmanlıkları arttıkça bunun daha çetin bir savaşa dönüşeceğini kabul ediyorlar.

Siber-terörden Korunmanın yolları

Dünya genelindeki tüm bilgisayar profesyonelleri kendi bilgisayar sistemlerini korumak ve olası bir terör eyleminin durdurulmasına yardımcı olabilmek için siber-terörizmin tehlikelerinin ve sınırlarının farkında olmalı. Bir sistemi korumanın %100 güvenilir bir yolu yoksa da, tam güvenli bir sisteme dışarıdan kişilerin girmesi neredeyse imkansız. Birçok askeri sistemin bilgileri, siber-teröre karşı önlem olarak hiçbir dış bağlantısı olmayan bilgisayarlarda saklanıyor. Böyle bir izolasyon dışındaki bir diğer yöntemse şifreleme. Yaygın kullanımı hükümetler tarafından sınırlandırıldığından, korunma şifreleme yöntemiyle sağlandığında kıtalararası iletişim daha az güvenli. Sistemi çökertmek için yapılan bir saldırının (örneğin virüs gönderme) şifrelemeden etkilenmiyor olması, yani şifrelemenin sistemin tümünü koruyamıyor olması bu yöntemin en önemli eksikliği. İkinci bir yöntemse sisteme gelen e-posta, mesaj gibi tüm iletişimi kontrol eden "kontrol duvarları" kullanmak. Kontrol duvarı, ağa girişi filtreleme yöntemlerinin geneline verilen bir ad. Bu yöntemde kullanılacak konfigürasyon bir bilgisayar ya da ağ yapısından oluşabilir. Koruma duvarları her kullanıcı için izin verilen girişleri kontrol etme görevini yapar. Bu duvarlarda kullanılan yöntemlerden biri kullanıcı taleplerinin daha önceden tanımlanmış bir Internet Protokol (IP) adresinden gelip gelmediğini kontrol etmek. Diğer

bir yöntemse, sisteme Telnet girişini engellemek. Kolay tahmin edilebilir şifre kullanmamak, herhangi bir kuşku duyduğunuzda ağ sisteminizi yenilemek, sisteminizi sürekli izlemek ve şifrelerinizi kontrol etmek, güvenliğinden kuşku duyduğunuz bir siteye girmemek ve bilmediğiniz adresten gelen e-postaları açmamak gibi önlemlerse bilgisayarınızı siber-terörden korumak için kendi kendinize uygulayabileceğiniz basit önlemler.

Yukarıdaki önlemler size çok paranoyak bir yaklaşım gibi geliyorsa bir de şu senaryoyu düşünün: Bildiğimiz bilgisayar teknolojisini kullanarak bir terörist ABD'nin en büyük bankalarının, finansal kurumlarının ve borsasının iletişimini parçalayabilir. Bu da bildiğimiz kadarıyla tüm dünya ekonomisini uçuruma yuvarlar. Aynı teknolojiyi kullanarak teröristler bir ilaç firmasının formüllerini uzaktan kontrol ederek bileşimin içine zararlı kimyasallar katabilir. Alerjik enfeksiyonlar ve doz aşımı sonucu binlerce kişi ölebilir. Aynı teröristler paralelde kentin yeraltı gaz şebekelerindeki basıncı değiştirerek bir patlamaya neden olabilirler. "Benim yakınımda böyle şeyler olmaz" deyip rahatça arkamıza yaslanmak, günümüz şartları göz önüne alındığında çok da doğru bir yaklaşım değil. Çünkü hızla büyüyen siberterörizm alanındaki uzmanlar ve yazarlar, bu eylemlerin artık bir Hollywood fantezisinden öteye gittiğinde hemfikir. Teröristler bu fantezileri henüz gerçekleştirememiş olsalar da, günümüz teknolojisi sayesinde buna yaklaştıkları kesin. Ancak yaşananlar gösteriyor ki dünyanın en büyük teknolojik gücü olan ABD ve teknolojik açıdan gelişmiş diğer uluslar için siber-terör oldukça yakın bir tehdit. Komşularda yaşanan bu siber sakatlanma dalgasının etkileri teknolojik açıdan daha az gelişmiş ülkelerin kıyılarına kadar da ulaşacaktır. Belki de oyun kuruldu ve alan seçildi, bizler de oyuna ilk kimin başlayacağını görmek için bekliyoruz.

Ayşenur Topçuğlu

Kaynaklar

http://www.cs.georgetown.edu/~denning/inffosec/pollitt
http://www.zdnet.com/filters
http://kyl.senate.gov/pterror
http://www.syneca.com/terror
Crime, Terror and War: National Security and Public Safety in the Information Age; United States Committee on the Judiciary Subcommittee on Technology, Terrorism, and Government Information; Report Submitted by Majority Staff; November 1998
Prof. Susan Brenner; Overview of Cyberterrorism; University of Dayton School of Law
http://www-cs.etsu.edu/gotterbarn/stdntppr/#Define
http://www.cybercrimes.net/Terrorism/overview
http://www4.cnn.com/TECH/9609/19/cia.hacker/index.html
http://www.kaspersky.com/news.asp?tnews=0&nview=8&id=214&page=0