İnsanın İçindeki Firewall ve Açıkları

Firewall Inside Human and Its Deficits

Cem Karakaya

Cem Karakaya / neue-medien@blackstone432.de

Almanya doğumlu Karakaya 1988-1992 yılları arasında İzmir Polis Koleji'nde okuduktan sonra 1996 yılında Polis Akademisi'nden mezun olmuştur. 2003 yılına kadar Emniyet Genel Müdürlüğü'nde, Dış İlişkiler Daire Başkanlığı'nda görev yapmıştır. 2003 yılında, Münih Emniyet Müdürlüğü'ne transfer olup, Müdürlük bünyesindeki, Suçların Önlenmesi Daire Başkanlığında göreve başlamıştır. Şu anda Münih Emniyet Müdürlüğü'nde, Siber Suçlar Dairesinde Şube Müdürü olarak görev yapmaktadır. 2008 yılında "Blackstone432" Siber Güvenlik Şirketini kuran Karakaya, bugün 148 çalışanıyla, Siber Güvenlik konusunda seminerler vermekte ve şirketlerin siber saldırılara karşı korunmasında etkin rol oynayabilmeleri için destek vermektedir. Çalışanlarıyla aynı zamanda okullara da gidip, daha güvenli bir gelecek için katkı sağlamaya çalışan Karakaya, 2018 yılında "Siber Güvenlik"konusunda bir kitap yayınlamıştır.

Cem Karakaya / neue-medien@blackstone432.de

Cem Karakaya was born in Germany. After studying at Izmir Police College between 1988-1992, he graduated from the Police Academy in 1996. He worked in the Turkish Republic Police General Directorate, Foreign Relations Department until 2003. In 2003, he was transferred to Munich Police Department and started to work in the Department of Prevention of Crimes. He is currently working at the Munich Police Department as the Branch Manager of the Department of Cyber Crimes. In 2008, he founded the "Blackstone432" Cyber Security Company. Karakaya, with its 148 employees, gives seminars on Cyber Security and supports companies to play an active role in protecting against cyber attacks. Karakaya, who goes to schools at the same time with his employees and tries to contribute to a safer future, published a book on "Cyber Security" in 2018.

Özet

Günümüzde internet ortamında işlenilen suçların oluşmasına olanak tanıyan sorunlar tanımlanmış durumdadır ve büyük çoğunluğu çözülmüştür. Ancak mevcut durumda da bu suçları işleyen kişiler, halihazırda büyük kazanımlar elde etmeye devam etmektedirler. Genel anlamda bunun iki sebebinden söz edilebilir; ilki insanların bilişim suçları ve tehlikeleri konusunda bilgi sahibi olmamasından kaynaklıdır. Diğeri ise insanların güvenlik tedbirlerini alabilmeleri için zamanlarının olmaması ile açıklanabilir. Özellikle ikincisi insanın tembelliğinden kaynaklı olarak ortaya çıkan koşullara işaret etmektedir. Kolay şifreler belirlemek de insanın kolaycılığının bir sonucudur. Şifreyi cihazın hatırlamasına, saklamasına onay verildiğinde sanal suçlulara yardım edildiği gerçeği göz ardı edilmektedir. Birçok insan, her bir hesap için aynı şifreyi kullanmak suretiyle, sanal suçlularının tüm bilgilerine erişmesini kolaylaştırmaktadır. Bu durumda herhangi bir hesabın giriş bilgileri ele geçirildiği zaman, sanal suçlularının tek bir düşüncesi vardır: "Acaba bu giriş bilgileri ile başka nerelere girebilirim?" Kullanılan şifre, şayet herhangi bir dilin sözlüğünde geçiyorsa veya sadece harflerden ya da sayılardan oluşuyorsa, böyle bir şifrenin kırılması, kapasitesi ve işlem hızı büyük bir bilgisayar için sadece birkaç dakika sürmektedir. Bir akıllı telefona giriş yapabilmek için parmak izini veya yüz hatlarını vermekten bile çekinmeyen birçok insan, başına ne gelebileceğini düşünmeden, özellikle sosyal ağ hesaplarında, kendileri hakkında her şeyi ifşa etmekte ve bu bilgileri kötü niyetli siber suçluların eline, altın bir tepsiyle sunmaktadır. Özellikle günümüzün çocuklarının kendi rızasına dayanmayan görüntülerinin paylaşılması ileride sorunlara neden olabilecektir. Geleceğin politikacılarını, hakimlerini, savcılarını, manipüle edebilmek veya şantaj yapabilmek için, sosyal ağ hesaplarına bakmak yeterli olacaktır. Ailelerin de bu konuda fazla bilgi sahibi olmamaları ve çocuklarına tehlikeler konusunda bilgi verememeleri, çocukların sanal alemdeki hareket ve davranışları, karanlıkta satranç oynamaya benzetilebilir. Herhangi bir şeyin dijitalleştirilmesinden önce sorulması gereken üç soru; İnsanlar buna hazır mı? Ne tip risklerin oluşabileceği konusunda bilgileri var mı? Bu riskleri engelleyebilmek için tedbirlerini aldılar mı? olmalıdır. Bu makale, internet ve güvenlik açıklarına ilişkindir. Gerekli güvenlik tedbirlerinin alınması ve insanların bilinçlendirilmesi için yapılması gerekenler ele alınmaktadır.

Abstract

Problems that lead to the crimes committed on the Internet platform have been defined and most of them have been resolved. However, in the given circumstance, those who have committed these crimes continue to derive great gains. Generally speaking, two reasons can be mentioned for this; the first one is that people do not know about cybercrimes and their dangers. The other can be explained by the fact that people do not have time to take security measures. Especially the second one signs the conditions based upon the laziness of the human being. Putting easy passwords is also a result of the simplicity of humans. When the device is approved to remember and store the password, the fact that virtual criminals are helped is ignored. Many people use the same password for each account, which makes it easier for virtual criminals to access all their information. In this case, when the login information of any account is getting hold, the virtual criminals keep only one thought: "I wonder where else can I enter with this login information?" If the password used is in the dictionary of any language or consists of only letters or numbers, it takes only a few minutes for a computer with a large capacity and processing speed to crack such a password. Many people who do not even hesitate to submit their fingerprints or facial features to log into a smartphone without considering what might happen to them reveal everything about themselves, especially on their social network accounts, and present this information with a golden tray in the hands of malicious cybercriminals. Especially, sharing the images of today's children, which are not based on their consent, would cause problems in the future. To be able to manipulate or blackmail future politicians, judges, prosecutors, it will be enough to look at their social network accounts. Families do not have much information on this issue and their inability to inform their children about the dangers, children's movements and behaviors in the virtual world can be associated with playing chess in the dark. The three questions that must be asked before digitalizing anything should be as follows: "Do the people ready for it?", "Do they have any information about what kind of risks can be occurred?", and "Did they take the precautions to prevent these risks?". This article is about internet and security flaws. The things to be done to take the necessary security measures and raise awareness of people are discussed.

DOI: 10.53478/TUBA.2020.017

İnsanın İçindeki Firewall ve Açıkları

Cem Karakaya
Münih Emniyet Müdürlüğü Siber Suçlar Dairesi

Giriş

Yaklaşık on iki sene önce, "iPhone 3" diye adlandırılan mucize alet, hayatımıza girdi ve yaklaşık on sene önce de birçok insan bu teknolojiyi satın aldı. Bugün akıllı telefonlar, çocuklar da dâhil herkesin elinde. Günümüzde sahip olduğumuz teknolojik imkânların en az %80'i sadece on senelik bir geçmişe sahip. Önümüzdeki on senenin bize ne getireceği ise belli değil. Burada temel sorun şu; gerçekten de bu teknolojik imkânlar sayesinde özgürlüğün tadını mı çıkartabiliyoruz yoksa özgürlüğümüzü feda mı ettik ve daha çok mu stres altındayız? İşten çıktınız ve otobüste yer bulabilmişseniz oturmuşsunuz; evinize gidiyorsunuz. Akıllı telefonunuza işinizle ilgili bir e-posta geldi ve siz bu maili cevaplıyorsunuz. Bu maili cevapladığınız süre fazla mesai süresi olarak hesaplanmamalı mıdır? Sadece iki dakika mı sürdü? O zaman iş yeri haricinde bir sene içerisinde cevapladığınız bu türden maillerin toplam süresi nedir? Maillerinizi ve yapmış olduğunuz işle ilgili telefon konuşmalarının sürelerini hesapladınız mı?

Akıllı telefonunuz aracılığıyla işiniz ile ilgili bir günde beş dakika, bir şey yaptığınızı düşününüz. Bu etkinlik, bir yılda yaklaşık 30 saat yapıyor. Neredeyse 4 iş günü. Hesaplama sadece beş dakika içindir; daha fazla olduğunu hepimiz biliyoruz. Bu basit hesaplama ile Tükenmişlik *(Burnout)* Sendromunun bu kadar sıklıkla yaşanması, hiç de sürpriz değil. Önceleri sadece belirli meslek gruplarında görülen bu sendrom, günümüzde çocuklar da dahil herkesin sorunu… Çocuk demişken çocukluk yıllarında okuduğum güzel bir kitabı hatırladım: *Tom Sawyer ve Maceraları*. Tom'un babası ya da büyükbabası, yapmış olduğu bir haylazlık sonucu onu cezalandırıyor ve ceza olarak bahçenin çitlerini boyamasını istiyor. Tom, çitleri boyarken, arkadaşları geliyor ve onunla dalga geçiyor. Sonra Tom, bu çitlerin boyanmasının ne kadar zor olduğunu, her çocuğun bunu başaramayacağını ve ne kadar eğlenceli olduğunu anlatıyor. Sonuçta bu çocuklar, Tom'a meyve ve para vererek çitleri boyarlar. Bu hikâyeden yola çıkarak soruyorum: *Aynı şey bizim de başımıza gelmedi mi?*

İnternet üzerinden, bankacılık işlemlerinizi kendiniz mi yapıyorsunuz? Banka çalışanlarının işini bu şekilde siz üstlendiniz mi? Seyahatlerinizi internet üzerinden, kendiniz planlamıyor musunuz? Seyahat acentasının işini siz üstlenmediniz mi? Avrupa'da yaygın olan self servisleri düşünün şimdi; paket istasyonundan paketinizi kendiniz almıyor musunuz? Kargo şirketleri… onlarin da işini siz yapmıyor musunuz? Havalimanında check-in işleminizi bir ekran üzerinden kendimiz yapmaya başlamadık mı? Havayolu şirketinin, yer hizmetlerinden sorumlu personelin işini de üstlenmedik mi? Peki bu noktada soru şu; size bu yüzden para veren var mı? Ya da uçak biletinizi bu hizmet karşılığında daha mı ucuza alıyorsunuz? Normalde teknolojinin işleri kolaylaştırması ve birçok işi üstlenmesi beklenir. Gelinen noktada insanlara daha çok iş vermesi ve insanların bir köle gibi, parasız çalışmasına neden olması, trajik komiktir. Teknoloji hepimizi bağımlı hale getirmiştir ve kölesi yapmıştır. Akıllı telefonun her çalışında, her ıslığında, her titremesinde ve her işaretinde onu, cebinizden çıkartıp, bakıyorsanız ona bağımlı hale gelmişsinizdir. Şayet o telefonu her zaman elinizde tutuyorsanız başka bir alemdesiniz demektir.

Son yıllık izninizi veya tatilinizi düşünün; eğer çıkabilseydiniz izin ya da tatilde kaç kez işinizle ilgili bir şeyler yaptınız? Kaç tane e-posta cevapladınız ya da kaç telefon görüşmesi yaptınız? Senelik izninizden geldikten sonraki ilk iş gününüzü hatırlayın. E-posta programını açtıktan sonra kaç tane cevaplanmamış e-posta vardır? Bu e-postalar siz izindeyken gelmedi mi? Cevaplamak zorunda mısınız? Almanya'da bir televizyon sunucusu ve film yapımcısı olan Roger Willemsen'in, güzel bir sözü var: *Bir şey kaçıracağız diye hayatımızı hızlandırıyoruz. Ama hızlandırarak, hayatın ta kendisini kaçırıyoruz.*

En kötü ihtimalde, yani tanıdığınız birinin ölmesi halinde, yapabileceğiniz hiçbir şey yok. İstediğiniz kadar hayat öpücüğü verin, şahsın öldüğü gerçeğini değiştiremezsiniz. O zaman neden sürekli ulaşılabiliyoruz? Bir iş adamı olarak, müşterilerim için her zaman ulaşılabilir olmam mı gerekiyor? Müşteriler günümüzde, bu hizmeti artık bir özel hizmet olarak değil normal bir şeymiş gibi görüyorlar. Nihayetinde insanlar günümüzde ne özel alanın ne de senelik izinlerin tadını çıkartabiliyorlar. Sinemada tiyatroda, seyahatlerde vb. yerlerde hep akıllı teknolojilerin güdümü altındalar.

Akıllı Telefon Mu Akıllı Bilgisayar Mı?

Hemen ifade etmek lazım ki cep telefonu ile akıllı telefon arasında dağlar kadar fark var. Cep telefonu ile konuşabilir, mesaj (SMS) gönderebilir ve en fazla yılan oyununu oynayabilirsiniz. Hatta gelişmiş modellerde fotoğraf çekebilir ve müzik dinleyebilirsiniz. Akıllı telefonlar ile hem bunları hem de fazlasını yapabilirsiniz. Daha pek çok işi de yapabildiğimizden adına akıllı diyoruz. Bu teknolojiler ile maillerinizi cevaplayabilir, sosyal ağlarda kaç *like* aldığınıza bakabilir, haberleri okuyabilir, şu an nerede olduğunuzu ve ne yaptığınızı diğerlerine bildirebilir, sadece konuşarak telefona emir verebilir, randevularınızı düzenleyebilirsiniz. Bir yere nasıl gidebileceğinize bakabilir, okeyinizi oynayabilir ya da şekerleri patla-

tabilir, hava durumunu öğrenebilirsiniz. Film ya da dizinizi izleyebilir, internette boş biçimde dolaşabilirsiniz. Bütün bunları masa veya dizüstü başka bir aletle de yapabilirsiniz. Bilgisayarınızda da bir işletim sistemi var, akıllı telefonunuzda da. Akıllı bir telefon günümüzde artık bir bilgisayar gibi kullanılmaya başlandı. Zira bir bilgisayar üzerinden bir siber saldırıya maruz kalma şansınız neyse telefonda da aynı. Bilgisayar için hangi önlemler alınıyorsa, akıllı telefonlarda da aynı önlemlerin alınması gerekiyor. Özellikle, Android model akıllı telefonlarda mutlaka bir *Antivirus Yazılımı* gerekiyor. Her ne kadar iOS işletim sistemli telefonlar için hâlihazırda zararlı bir virüs olmasa da bu sistemler için, casusluk yazılımlarının olduğu akıldan çıkarılmamalıdır. Akıllı telefonlar için sadece oyun uygulamaları değil aynı zamanda birçok güvenlik uygulamaları da mevcut. Ancak, birçok insan halen evindeki bilgisayarına bile lisanslı bir virüs yazılımı yüklememiş durumda. Virüs yazılımını bırakın birçok bilgisayarda lisanslı bir işletim sisteminin bile olmadığını biliyoruz. Kullanılan diğer birçok yazılım da lisanslı değil. Hal böyle olunca ne işletim sistemi ne de yazılımlar güncellenemiyor ve açıklar, her zaman mevcut. İşte siber saldırı suçluları da tam olarak bu açıklıkları kullanarak, sisteminize giriş yapabiliyor. Bu yüzden de suçluların bilgisayarları hacklemesine gerek kalmıyor. Var olan açıktan sisteme sızıyorlar.

Akıllı Telefonlar ve Çocuklar

Konunun hemen başında akıllı telefonların çocuklar için kesinlikle uygun olmadığını söylemek lazım. İnsanlar, 8 yaşındaki çocuğuna arabanın anahtarını verip, "Çocuğum, bugün arabayı sen kullan. Bunu başarabilirsin." demiyorlar. Çünkü sonuç, büyük bir olasılıkla çok vahim olacaktır. Aynı şekilde ebeveynler, çocuklarının eline bir bira şişesi de vermiyorlar. Çünkü biliyorlar ki çocuğun sağlığı bundan olumsuz yönde etkilenecektir. Günümüzde çocuklar ve gençler tarafından en çok kullanılan akıllı telefon yazılımları: *TikTok* (Önceki ismi musical.ly ve Çinliler tarafından satın alındıktan sonra, sadece ismi değiştirildi), *WhatsApp* ve *Instagram*. Bu noktada çarpıcı bir hususu belirtmem lazım; TikTok, WhatsApp ve Instagram uygulamasından daha fazla telefonlara indirilmiş durumda. TikTok uygulamasıyla çocuklar bir şarkı eşliğinde dans edip bu videoları tüm dünyaya servis ediyorlar. Amaç çok sayıda beğeni toplamak *(like)* olduğu için de bazı videoları seyrederken akla, "acaba bu videolar sadece 18 yaşın üzerindeki kişiler için mi uygun?" sorusu gelmektedir. TikTok uygulamasının kendisi, kullanım sözleşmesinde, kullanım yaşını en az 13 olarak belirlemiştir. Instagram 13 ve WhatsApp ise bu yaşı 16 olarak saptamış durumdadır. O zaman neden çocuklar bu uygulamaları halen kullanabiliyorlar sorusu akla geliyor. Bu durumda büyük görev yine ailelere düşüyor.

Bazı yetişkinlerin, kendilerini çocuk gibi tanıtarak çocuklarla irtibatta geçtikleri en büyük ortamın Instagram olduğunu da söylemek lazım. Çocukların psikolojik sağlığını bozabilecek videolara, özellikle cinsel içerikli videolara erişimi, günümüzde o kadar kolay hale geldi ki endişe etmemek mümkün değil. Youtube ise kullanım yaşını en az 16 olarak belirlemiş durumda ve bunun sebebi ise tıbbî. Zira bir çocuk ancak 16 yaşından itibaren %100 gerçeklikle sanallık arasındaki

farkı ayırt edebiliyor. Diğer yandan akıllı telefonların meydana getirdiği manyetik alanın zararı, yetişkinlere nazaran çocuklarda daha fazla; çünkü çocukların kafatası bir yetişkine nazaran daha incedir. Çocukların yeni teknolojiler konusundaki bilgi ve becerileri ebeveynlerinden daha fazladır. Ailelerin bu teknolojik çağda, çocuklarına eşlik etmesi, akıllı telefonların yararları yanında zararlarının da olduğunu öğretmesi, istenilen ve tavsiye edilen bir durumdur. Ancak bu durum, çoğu zaman mümkün değildir. Ailelerin çoğu, neyi nasıl kullanması gerektiğini çocuklarından öğrenmektedir. Çoğu teknolojik işlem için onlardan yardım talep etmektedirler. Diğer bir husus ise bazı ailelerin çocuğunun sadece evde internete eriştiğine yönelik yanlış inanışıdır. Günümüzde restoranlarda, kafelerde, arkadaşının evinde, sokakta bile internete erişim mümkündür ve bu inanış doğru değildir. Bazı ailelerin bu kaygı ile çocuklarının cep telefonlarını kontrol ettikleri ve resimlere baktıkları da beyan edilmektedir. Ancak aileler, kendilerinin görmemesi gereken resimlerin başka bir yerde saklı olduğunun farkında değillerdir. Örneğin, *CalculatorVault* denilen bir uygulama sembolü ekranda aynı hesap makinası gibi görünmektedir. İlk bakışta görünen, uygulamanın hesap makinası olduğudur. Bu uygulama gerçekten, bir hesap makinası gibi hesaplamalar da yapabilmektedir. Ancak, belli bir sayıyı girip (Kod) "%" işaretine basıldığında, saklı olan resimlerin ortaya çıktığını ebeveynler bilmemektedir.

Çocukların akıllı telefonlarında ebeveynlerinde de olmadığı gibi bir koruma programı bulunmadığından telefonlarının kameraları genellikle, siber suçlularının kontrolü altına geçmekte ve bu kameralar, "Darknet" denilen, internetin karanlık bölgesinde hizmete sunulmaktadır. Bu kameralar günlüğü, 200 Euroya kadar kiralanmakta, hatta bazı sayfalar, en çok ziyaret edilen 10 Kamera (Top Ten) listesi bile yapmaktadırlar.

Sıfır yaştan itibaren tavsiye edilen bazı *ücretsiz* oyunlara baktığınızda dünyayı anlamakta zorlanıyorsunuz. Şu anda çocuklar tarafından çok sevilmekte olan *Coin Master* oyununu örnek alalım. Birkaç ay öncesine kadar sıfır yaştan itibaren tavsiye edilen bu oyunun amacı diğer köylere saldırmak ve kendi köyünü ileriye götürmektir. Oyun grafiğine bakıldığında, tamamıyla çocuklar için yapılmış olduğu izlenimi yaratılmıştır. Diğer köylere saldırabilmek ve kendi köyünüzü ileriye taşıyabilmek için sikkelerinizin olması gerekiyor ve belli bir zaman sonrasında, oyun tarafından hediye edilen sikkeler bittikten sonra, normalinde kumarhanelerde görebileceğiniz tek kollu makina ile sikke kazanmanız gerekiyor. Ama bu makina her zaman çalışmıyor. Çalışabilmesi için ya belli bir süre beklemeniz gerekiyor, ya da gerçek para karşılığında, sikke satın alabiliyorsunuz (Bir makinayı 80 defa döndürebilmek için, 5,49 € ödemeniz gerekiyor; 2800 defa için 109,99 €. Sikkeye ihtiyacınız varsa, 3 milyon sikke için 10,99 € ödüyorsunuz ya da 55 milyon sikke için 109,99 €). Beklemeyi seçerseniz bir saat beklemeniz gerekiyor ki, beş defa daha, makinayı kullanabilesiniz. Bu bir saat içinde oyun size sürekli mesajlar gönderiyor. Diğer taraftan oyun sizde merak da oluşturuyor; beklenilen süre içerisinde köye saldırı olmuş mu hayvan yavrularına yardım lazım mı vb. duygu sömürmeye yönelik iletiler gönderiliyor. Bu örnekte olduğu gibi oyun masum bir eğlence unsuru olmaktan çıkıyor. Coin Master'da olduğu gibi firma-

nın yöneticilerinin aynı zamanda bir spor iddia firmasının yönetim kurulunda olduğu başka amaçlara hizmet eden bir hal alıyor.

Bana Facebook/Google/Amazon/Oyun Konsolu Hesabını Ver, Sana Kim Olduğunu Söyleyeyim

İnsanlar, her şeyin gerçekten ücretsiz olduğuna inanarak, her yerde bilgilerini kısıt olmaksızın diğerlerinin erişimine açmaktadır. Şayet bir ürün için para ödemiyorsanız, ürün sizsiniz. Yani almış olduğunuz hizmetin karşılığını kendinize ait ve çok değerli olan şahsi bilgilerinizle ödemek durumunda kalıyorsunuz. Bu şekilde de dijital "Ben" oluşturmuş oluyorsunuz. Günümüzde neredeyse her insanın bir kendi benliği bir de dijital benliği var. Big Data (Büyük Veri) ve algoritmik hesaplamalar neticesinde bu şekilde insanların şahsi profilleri oluşturulmaktadır. Bu bilgiler, arama motorunuz (örneğin Google), sosyal ağlarınız (örneğin Facebook), resim veya video platformlarınız (örneğin Youtube ya da Instagram), arabanızdaki navigasyon aletiniz, kolunuzdaki akıllı saatiniz, alışverişlerinizde indirim alabilmek için kullanmış olduğunuz müşteri kartlarınız, akıllı telefonunuzda kullandığınız uygulamalar (ücretsiz), akıllı eviniz, vb. aracılığıyla toplanmaktadır. Hatta arabanızda bile 300'ün üzerinde sensor bulunması, arabanızı nasıl kullandığınız hakkındaki bilgileri bir yerlere aktarma amacına yöneliktir. Bütün bu bilgilerin çeşitli kaynaklardan gelip bir kovanın içine döküldüğünü düşünün. Hedefteki bir şahıs hakkında bu şekilde her türlü bilgi sahibi olabilirsiniz. Bu yüzden, dijital benliğinizin, sizin hakkınızda, sizden daha fazla bilgi sahibi olduğu ifadesi yanlış olmayacaktır. Hitler zamanında Yahudi kökenli insanların toplandığı bir bilgi bankası olduğunu düşünün. Ne kadar tehlikeli olurdu, değil mi? Bugün hangi bilgi bankasının 10 yıl sonra, 20 yıl sonra ya da 30 yıl sonra tehlikeli olabileceğini kim bilebilir? Örnek olarak sadece Google şirketini (Şirketin asıl ismi *Alphabet*) alalım:

- ***Picasa:*** *Google, bütün resimlerinize sahip.*
- ***Youtube:*** *Google, hangi videolara ve hangi konu hakkındaki videolara baktığınızı biliyor.*
- ***Google+:*** *Google, hangi insanların yakın arkadaşınız olduğunu biliyor.*
- ***Google Drive:*** *Google, dokümanlarınıza sahip.*
- ***Google Calendar:*** *Google, randevularınızı biliyor.*
- ***Google Maps:*** *Google, nerede olduğunuzu ve nerelerde bulunduğunuzu biliyor.*
- ***Google Mail:*** *Google, mailerinize sahip.*
- ***Google Play:*** *Google, akıllı telefonunuzda hangi uygulamaların olduğunu ve bu uygulamaları nasıl kullandığınızı biliyor.*
- ***Google Chrome:*** *Google, hangi internet sayfalarını ziyaret ettiğinizi biliyor.*
- ***Google Arama Motoru:*** *Google, en çok ne aradığınızı biliyor.*
- ***Google Fit:*** *Google, ne kadar sağlıklı olduğunuzu biliyor.*

Günümüzde 100'ün üzerinde ücretsiz Google Hizmeti mevcut. Sadece bir kişi hakkında bu kadar çok bilgiye sahip olmak, bir kişiyi veya bir firmayı, âlemin kralı yapmaz mı? Bir de geleceği düşünün; bugünkü çocuklar ve gençler, geleceğin devlet başkanı veya başbakanı, politikacıları, savcıları, hakimleri veya şirket yöneticileri değil mi? Gelecekte birisi devlet başkanı mı oldu? Aç dolabını veya çekmecesini, bak bakalım, bu kişi hakkında neler biliyorsun? Şirketin asıl isminin Alphabet yani Alfabe olması bir tesadüf mü? 2006 yılında *23andMe* diye bir şirket ortaya çıkıyor. Bu firmanın yatırımcılarına bakıldığında en büyük yatırım yapan şirketin Google olduğu görülüyor (yaklaşık 4 milyon dolar). Şirket sadece 99 dolara insanların DNA testini yapıyor. Fiyatın bu kadar ucuz olması, kimsenin merakına mucip olmuyor.

2010 yılında kurulan *Nest Labs* şirketi, 2014 yılında Google tarafından satın alınmıştır (3,2 milyar dolara). Net Labs, evinizi ve evinizdeki aletleri internete bağlıyor. Bu şirketin piyasaya sunduğu yangın alarmına yakından bakmak lazım; yangın alarmı, internete bağlı olmakla birlikte mekânın veya odanın içindeki nem oranını da ölçüyor. Yani Google programa tabi olan mekanda kaç kişinin olduğunu da bilme hakkını eline almış. Stratejik açıdan bakıldığında bu bilgi, çok önemli bir bilgidir. Eğer yatak odanızda nem oranı birdenbire yükseliyorsa Google bunu nasıl kaydediyor düşündünüz mü? Hatta cinsel yaşamınız hakkındaki bilginin bu şirketin eline geçmiş olması ya da ütü yapıyorsanız bunun yorumlanışı başka konuları akla getirmez mi? Bir akrabanız veya yakınınız için Google'un arama motorunda kanser ile ilgili bir ilacı aradığınızda Google, bunu akrabanız için aradığınızı nereden bilecek? İnsanlar, evlerini ellerinden geldiğince, akıllı yapmaya, yani internete bağlamaya çalışıyor. Dünyada bu konuda tam anlamıyla güvenilir hiçbir şirketin olmadığından emin olabilirsiniz. O zaman insanlar, bu riske niye giriyorlar? Bir şeyi unutmamak lazım: *Şayet herhangi bir şeyi internete veya bir ağa bağlıyorsanız, her zaman risk mevcuttur*. O yüzden de elektrik, su veya atom santrali gibi kritik kurumların bir ağa bağlanması büyük bir risk oluşturmaktadır. Güney Amerika olsun, Rusya olsun, bunun örnekleri yaşanmış durumda. *Halen niye her şeyi dijitalleştirmeye çalışıyoruz?*

Dijitalleşmenin elbette yararları var, ancak riskleri de göz ardı etmemek gerekiyor. Birçok evde, *Amazon Echo* veya *Alexa* gibi aletler bulunuyor. İnsanlar bu aletlerin 24 saat boyunca dinleme amaçlı kullanıldıklarını bilerek satın alıyorlar. Oturdukları yerden *Alexa, bana şu müziği çal* diye emir verebilmek için risk alıyorlar. Ancak, polis bir dinleme yapmak istese, mahkeme kararına ihtiyac duyuluyor. Bu biraz trajikomik bir durum. 2013 yılında, eski NSA *(National Security Agency)* çalışanı Edward Snowden, o kadar çok şey anlattı ki normalinde kanımızın donması gerekirdi. Ama yine de çok şey değişmedi. İnsanlar bilgilerinin mahremiyetini tercih eden her şeyi kullanmaya devam ettiler ve ediyorlar. 2016 yılında, Facebook'un, Amerika'daki üyelerinin bilgilerini başkanlık seçimleri için suiistimal ettiği *(Cambridge Analytica)* ortaya çıktı, değişen yine bir şey olmadı. Özellikle; Facebook, Instagram, Snapchat veya WhatsApp gibi sosyal ağlar hayatımıza girdikten sonra, *herkesin bir sırrı vardır* ifadesi tarihe gömülmüştür. Kimin, nerede, ne yaptığı, en çok neden ve ne düzeyde hoşlandığı, arkadaşlarının ve

akrabalarının kim olduğu, hangi politik düşünceye sahip olduğu, en çok hangi marka elbise veya ayakkabıyı giydiği, hangi kampanyaları desteklediği alenileşmiştir. En son hangi kitabı okuduğu ve en son hangi filmi izlediği, ne iş yaptığı ve hangi okullara gitmiş olduğu, hangi şarkıcıyı sevdiği, bir hayvan sahibi olup olmadığı sosyal medya hesaplarında açık olarak yazar hale gelmiştir. Bu sosyal ağlar üzerinden gönderilen bütün fotoğraf veya videoların kullanım hakkını, bu şirketlere verdiğinin kimse farkında değil. Bu durum, kabul etmiş ve okumuş olduğunuz, kullanım sözleşmesinde, gayet açık bir şekilde ifade edilmiştir. İnternette dolaşan en büyük yalan ise "Bu sözleşmeyi okudum ve kabul ediyorum" ifadesidir. 2011 yılında Avusturya'da bir hukuk öğrencisi olan ve bugün bir avukat olarak görev yapan, Max Schrems, Facebook'tan, kendisi hakkında kaydedilmiş bilgilerini talep etti. Kendisine 496 MB *(Megabyte)* büyüklükteki bir PDF-Dosyası ile 1222 sayfalık, şahsi bilgilerinin olduğu bir doküman gönderildi ve bu sadece dev bir buz dağının görünen kısmıydı. Çünkü Facebook hesabına yüklemiş olduğu videoların veya fotoğrafların bilgisi veya kime beğeni *(like)* vermiş olduğu gibi bilgiler bu dosyalarda yoktu. Bu bilgiler arasında ne zaman giriş yaptığı ne zaman mesajlar yazdığı, yazıştığı kişilerin kimler olduğu, nerelerde yaşadığı ve ne zaman iletişim kurulduğu, gibi bilgilerin yanı sıra, mesajlarında en çok hangi kelimeleri kullandığı bilgisi mevcut idi.

Facebook ve Google dışında çok sayıda site ve uygulama kullanıcıların bilgilerini toplamaya devam ediyor *Amazon, Playstation* veya *Xbox* oyun konsolları bunlardan bazıları. Amazon ve diğer online alışveriş sayfaları da, hakkımızda profil oluşturuyorlar. Satın alma profiline bakılarak, hedefteki kişinin yaşam tarzı, hobileri, satın alma gücü, marka veya teknoloji düşkünü olup olmadığının yanı sıra sözünde durup durmadığı da tespit edilebiliyor. Yani, tüketici, almış olduğu malı ödüyor mu yoksa 14 gün içerisinde (Tüketici yasasına göre) hep geri mi gönderiyor? Bazı firmalar hatta bir adım daha ileri giderek şayet komşunuz aldığı malları ödemiyorsa sizin de ödemeyebileceğinize ilişkin ön yargıya sahip olabiliyor.

Amazon *Dash Button* denilen ve bir kapı zili büyüklüğünde bir alet çıkartmıştı. Bu aletleri banyonuza ya da çamaşır makinası gibi makinalara yapıştırıp, örneğin deterjanınız bittiğinde, sadece bu küçük alet üzerindeki düğmeye basarak, internet üzerinden, bilgisayarınızı açmadan, ısmarlayabiliyordunuz. Diş macunu, şampuan, tıraş köpüğü ve hatta kondom bile bu aletler üzerinden ısmarlanabiliyordu. Her ne kadar bu aletlerin yaşam süresi kısa olduysa da bu şekilde, tüketim ihtiyacına göre, evde kaç kişinin yaşadığı, sağlıklı ürünler kullanıp kullanmadığı, evde çocukların olup olmadığı gibi bilgilerin toplanmasını mümkün kılıyordu.

Oyun konsolları da günümüze ayak uydurarak, çok gelişmişlerdir. Artık sadece iki çizgi ve kare şeklindeki bir topla birlikte tenis oynanmıyor, bazı oyunlar o kadar gerçekçi görünüyor ki bir film mi seyrediyorsunuz, yoksa bir oyun mu oynuyorsunuz belli değil. Ancak konsol üzerinde oynanan oyunların çoğu, bu oyunu piyasaya sunan şirket ile birlikte oyunu oynadığınız süre içerisinde, hep bir iletişim halindedir. Yani oyun esnasında almış olduğunuz bütün kararlar bu

şirkete iletilmektedir. Örnek olarak *Assassins Creed* serisinin son oyununu ele alalım. Oyun eski Yunanistan'da geçiyor. Oyunun birkaç yerinde bir erkek sizinle cinsel bir ilişkiye girmek istiyor. Oyunda siz de bir erkeksiniz ve oyun size bir soru soruyor: *Bu erkekle cinsel ilişkiye girmek ister misiniz?* Evet ya da hayır biçiminde iki seçenek sunuluyor. Hangi kararı almış olursanız olun şirket, hangi kararı verdiğinizi kaydediyor. Diğer taraftan teknolojinin var olmadığı bir hayat artık söz konusu değildir. Ama 24 saat boyunca, teknolojinin kullanılması zorunluluğu da yoktur. Teknolojinin ve sosyal ağların, insanların hayatını kolaylaştırdığı ifadesi ne kadar gerçekse suçluların ve özellikle siber suçluların hayatını da kolaylaştırdığı ifadesi de o kadar gerçektir.

Dark Net

İnsanların çoğunun kullandığı internet; sosyal ağlar, online alışveriş siteleri, arama motorları veya online haber siteleri internetin görünen tarafıdır ve bunları tüm ağın sadece %10'unu oluşturur. İnternetin yaklaşık %90'ı "Deep Web" ya da "Dark Net" denilen bir bölgeden oluşmaktadır. İnternetin bu karanlık bölgesinde her şeyin bulunabileceğini vurgulamak gerekir. Uyuşturucu, çalınmış olan kredi kartı veya banka hesapları bilgileri, proxy server hizmeti sunan sayfalar, hacker programları veya belli sayfalar için kullanıcı giriş bilgileri internetin bu alanında yer alır. Dark Net'te bulunan sayfaların %25'i bu bilgilerden teşekkül etmişken büyük bir kısmında çocuk pornosu yer alır. Dark Net'te bir de çeşitli topluluklar bulunmaktadır:

- ***Crush-Community:*** *Cinsel ilişki sırasında; tavşan, köpek, kedi veya fare öldüren insanların camiası (En başta olmasının sebebi en büyük topluluk olduğu içindir)*
- ***Cam-Community:*** *Hackerların kontrolü altında olan ve gençlere veya çocuklara ait olan akıllı telefon, dizüstü, tablet veya bilgisayar kameralarının kiralandığı sayfalar*
- ***Hitman-Community:*** *Kiralık katillerin topluluğu (Bir kişiyi illaki öldürtmenize gerek yok. Sadece yaralamaları için de bu insanları kiralayabilirsiniz)*
- ***Pedo-Community:*** *Pedofillerin topluluğu*
- ***Drug-Community:*** *Uyuşturucu tacirlerinin ve kullanıcılarının topluluğu (Şu anda kapatılmış olan, ancak zamanında en büyüğü olan bu sayfanın ismi "Silk Road" idi)*
- ***Fake-Community:*** *Sahtecilerin (sahte para veya sahte belge) topluluğu*
- ***Money-Laundering-Community:*** *Kara para aklama sayfaları (online casinolar gibi)*
- ***Doxing-Community:*** *Ünlü kişilerin veya şirketlerin, gizli bilgilerinin bulunduğu ve açığa çıkartıldığı sayfalar (Panama Papers gibi)*

Yukarıda sayılanlara ilave olarak e-posta adresinin ve şifrelerin bulunduğu sayfaları da unutmamak gerekir. Şimdi adını söylemeden bir sayfanın toplam 12,3 milyar adet adrese ve şifrelerine sahip olduğu örneği ile bir sorgulama yaptığımızda "sonu bmw.de" ile biten 6287 adres bilgisi rapor edilmektedir. Bunun an-

lamı; Almanya'da, BMW şirketinde çalışan 6287 kişinin olduğu bilgisine erişmiş olmam ve onların ön isimlerini, soy isimlerini ve şifrelerinin bilinmesi demektir. Nedenini bilmememize rağmen ilgin bir şekilde büyük şirketlerde birçok e-mail adresinin yapısı önisim.soyisim@şirket.de şeklindedir. Bu bilgiler BMW şirketinin hacklendiği anlamına gelmese de BMW çalışanlarının iletişim bilgilerinin alenileşmesi anlamına gelmektedir. Diyelim ki, bir çalışanın şifresi "nico1964". Sadece şifresine bakarak şahsın kaç yaşında olduğunu bile bulabiliyorsunuz. Bu noktada şifrelemenin önemine de değinmek lazım. İlginç bir şekilde bu dünyadaki insanların yarısından çoğu, doğum yıllarını şifrelerinde kullanmaktadır. Bu çalışanın ön ve soy ismini de bildiğimiz için, özel olarak kullandığı, ücretsiz E-Mail adresini de (Yahoo, Hotmail veya Gmail gibi) internette bulabiliyoruz. Diyelim ki önisim.soyisim@yahoo.de. Bu ücretsiz e-mail adresi ve "nico1964" şifresi ile daha nerelere giriş yapılabileceğini bir düşünün.

Siber Suçlular ve Siber Saldırıları

Evinizdeki bütün pencere ve kapıları açık bırakarak tatile gittiğinizde dönüşte evinizin soyulmuş olduğunu görmek büyük bir sürpriz olmayacaktır. Bilgisayarınızda da gerekli önlemleri almazsanız aynı şey olacaktır. Siber suçlularının bu kadar büyük bir başarı elde etmesinin tek sebebi, ya insanların bu konudaki yetersiz bilgileri ya da insanların tembelliğidir. Her "Hacker"ı aynı tencereye koymak doğru değildir. Hackerlar kendi aralarında üç sınıfa ayrılmaktadır:

- ***Beyaz Hackerlar (White-Hats):*** *Bu hackerlar, kanunların belirlemiş olduğu sınırlar ve Hacker-Etiği çerçevesinde hareket ederek, örneğin görevlendirilmek suretiyle, bir şirketin bilgisayar ağının güvenilirliğini test ederler (Penetrations-Test).*
- ***Gri Hackerlar (Grey-Hats):*** *Bu hackerlar, büyük ihtimalle, kanunlara karşı her ne kadar, bir suç işleseler de amaçları bir sistemdeki açıklıkları ortaya koyup sorumluların bir an önce tedbirlerini almalarını istemektedirler.*
- ***Siyah Hackerlar (Black-Hats):*** *Bu hackerlar, büyük bir suç işleme enerjisine sahip olup hükümetler veya suç şebekeleri tarafından görevlendirilmektedirler. Tek amaçları, hedef sisteme zarar verip bilgi çalmaktır. Aynı zamanda, hedef sistemi çalışamaz duruma getirip şirketlere şantaj da yapmaktadırlar.*

1983 yılında Amerika'da, bir grup genç *(The 414s)*, birçok bilgisayar sistemine illegal bir şekilde giriş yapmıştır. Sonra kongre üyesi Glickman tarafından bu konuda bir kanuni düzenleme yapılması için girişimlerde bulunulmuştur. O zamanlar 17 yaşında olan ve bu gruba ait olan Neal Patrick, kongre oturumu esnasında kongre üyelerini bilgilendirmiş ve aynı senede bu konuda 6 adet kanun çıkartılmıştır. Sadece bazı illegal programları kullanmak suretiyle bir sisteme giriş yapmaya çalışan kişileri Hacker olarak tanımlamak da yanlıştır. Hackerlar, çok derin programcılık, bilgisayar ve bilgisayar ağları konusunda bilgilere sahip iken sadece bu programları kullanan kişiler, programcılık konusunda en ufak bir bilgileri bile yoktur. Bu tip kişilere verilen isim: *Scriptkiddie*'dir.

Her saniye dünyanın herhangi bir yerinde bir siber saldırının gerçekleştirildiğini söylemek yanlış olmayacaktır. Tüm dünyada en çok saldırıya uğrayan ülkeler arasında Almanya 3. sıradayken, Türkiye 19. sıradadır (23.03.2020 itibariyle). Neredeyse her gün, birinci sırada olan ülke ise Rusya'dır. Siyah Hackerlar, bu saldırılarını gerçekleştirirken sadece kendi bilgisayarlarını değil kontrolleri altında olan bilgisayarları da kullanarak saldırılarını gerçekleştirmektedirler. O yüzden de bazı insanlar, kendi bilgisayarlarının niçin birdenbire yavaşladığını düşünürken bilgisayarlarının bir saldırı için kullanıldığının farkında bile değildirler. Yani işlenilen suça ortak olduklarını bilmezler. Hackerlar, birçok bilgisayarı kontrol altına alabilmek için bu bilgisayarlarda öncelikle bir virüsün (Trojan) yerleştirilmesini sağlarlar. Böylece kontrolün hackerlara geçmesi sağlanır. Bu virüslerin en çok yayıldığı sayfalar, erotik sayfalar ya da sinema filmlerinin ve dizilerin, belli bir ücret ödemeden seyredildiği illegal sayfalardır. Günümüzde gerekli tedbirler alınmazsa hiçbir yere tıklamadan veya herhangi bir dosya indirmeden, sadece bir internet sayfasını ziyaret etmek suretiyle, bu virüs kapılabilir. Profesyonel hackerlar, artık Bitcoin denilen dijital para yöntemi ile değil daha çok şahsi bilgi içermeyen hediye kartları ile (örneğin Apple için Itunes-Card) ödeme yaptırmaktadırlar.

En çok kullanılan Siber Saldırı Yöntemleri

***Spear-Phishing*:** Dünyadaki bütün siber saldırılarını ele aldığımızda, bu saldırıların en az %80'i, bir Phishing-Emaili ile başlamaktadır. Örneğin, her ne kadar bir e-posta, bankanızdan geliyormuş gibi gözükse de aslında bankanızdan gelmemektedir. Siber suçluların buradaki amacı, online bankacılık giriş bilgilerinize ulaşmaktır. O yüzden bu yönteme *sazanlamak* demek, yanlış olmayacaktır. Bu tip Phishing e-postaları eskiden "Sayın müşterimiz" diye başlarken, günümüzde Phishing mağdurları isimleri ile hitap edilmektedir. Bu yöntemin ismi de *Spear-Phishing*dir. Bu da siber suçluların hedefteki mağdurlar hakkında daha çok bilgiye sahip olduklarının bir göstergesidir. Bu konuda mağdur olmamak için gönderici e-posta adresinin iyice kontrol edilmesi gerekmektedir. Sadece bir "nokta" veya - işareti ile e-mail adresinin manipüle edilmesi mümkündür. Bazı durumlarda görülen "gönderici e-mail adresi" ile arka planda olan gerçek e-posta adresi farklılık gösterebilir. Bunun tespit edilebilmesi için bilgisayar faresini tıklamadan gönderici e-adresinin üzerine getirmek yeterlidir. Teknik olarak günümüzde, gönderilen e-postaların bir sertifika aracılığıyla, dijital olarak imzalanması da mümkündür. Bu şekilde gönderici e-mail adresi, teyit edilmiş olmaktadır. Bunu her kullanıcı yaptığında siber saldırılarının en az %80'i engellenmiş olacaktır.

Şifreleme ve şantaj (***Ransomware):*** Bu tip zarar verici programlar, bilgisayarınıza bulaştıktan sonra, bilgisayarınızda bulunan bütün dosyalar şifrelenmektedir. Dosyalarınızı kurtarabilmek için de hackerlara belli bir miktarda para ödemeniz gerekmektedir. Hackerlara parayı ödedikten sonra ise dosyalarınızın kurtulacağının %100 garantisi yoktur. Hackerlar ya daha çok para istemektedirler ya da size dosyalarınızın kurtulabilmesi için şifreyi vermemektedirler. Bazıları ise

şifreyi iletmekte ve hatta, mağdur olmuş şirketin bilgisayardan sorumlu bölümü arayarak ileride bu tip saldırılardan korunabilmek için, nelerin yapılması gerektiği konusunda bilgi de vermektedirler. Bu konuda alınabilecek en iyi korunma yöntemi, tabii ki burada standart tedbirlerin (Bu yazının son bölümü olarak ele alınacaktır) alındığını varsayıyoruz, yedekleme deposu olarak kullanılan aygıtların (harici harddisk veya USB-Stick gibi) ana bilgisayar ile her zaman bağlantı halinde olmamasıdır. Bu tip zararlı programlar genellikle bir internet sayfasının ziyareti esnasında, ekrana gelen ve size sözde bilgisayarınızın virüs kaptığını bildiren bilgi pencereleri (Pop-up) üzerinden gelmektedir. Bazıları ise size az önce 1 milyonuncu ziyaretçi olarak bir Iphone veya başka bir şey kazandığınızı bildirir.

Call-ID-Spoofing: Bu yöntem ile telefon ekranında gösterilen telefon numarası istenilen başka bir numara ile değiştirilmektedir. Bu şekilde, "155-Polis imdat" gibi bilinen numaraların bile ekranda gösterilmesi mümkündür. Telefonda polis ile görüştüğüne inanan mağdur, hal böyle olunca, istenilen bilgileri de vermekte veya suçluların istedikleri şeyleri (kapının önüne, bir torba içerisinde evde bulunan paraları koymak gibi) yapmaktadırlar. Şu an Almanya'da en çok yaşanan hikâye ise şudur: "Polis tarafından bir hırsız yakalanmıştır. Bu hırsızın cebinde sizin adresinizin de olduğu bir liste ele geçirilmiştir. Eviniz de kıymetli eşyalar ve para var ise lütfen bunları bir torbaya koyup, biraz sonra gelecek olan polis arkadaşa teslim ediniz ki eşyalarınızı ve paralarınızı koruyabilelim.". Türkiye'de ise mağdurların banka hesaplarının bir terör organizasyonu tarafından kontrol edildiği yalanı kullanılmaktadır. Çok sık rastlanılan "CEO-Fraud" olayında da bu yöntem kullanılmaktadır. Bu olayda bir firmanın muhasebe bölümü aranarak telefon ekranında şirket sahibinin numarası gösterilerek büyük miktarda bir paranın yurtdışına gönderilmesi sağlanmaktadır. Oluşan zarar bazı firmalarda o kadar büyüktür ki mağdur firmaların bazıları artık işlevsel değildir.

Sözde Destek-Servisi: Burada yine "Call-ID-Spoofing" yöntemi ile her defasında değişik numaraların ekranda gösterilmek suretiyle mağdurlar, belli bir markanın ya da ünlü bir firmanın temsilcisi ile görüştüklerine inandırılarak suçluların hedef bilgisayara girişleri sağlanmaktadır. Hedef sistemde olan suçlular bu şekilde bilgisayara zararlı bir program yükleyerek kullanıcının (mağdurun) çeşitli platformlardaki giriş bilgilerine (özellikle online bankacılık giriş bilgileri) ulaşmaktadırlar. Almanya'da mağdur olan vatandaşlar şimdiye kadar en fazla sözde Microsoft firması ile görüşme yaptıklarını ifade etmişlerdir. Suçlular, kendilerini Microsoft çalışanı olarak tanıtarak sadece mağdurların bilgisayarına girerek zararlı bir program yüklememekte aynı zamanda, sözde Microsoft Lisans Yazılım süresinin de bittiğinin tespit edildiğini bildirerek, mağdurların kendilerinin para göndermesini de sağlamaktadırlar. Microsoft'un yanında suçlular, Apple veya Google gibi firmaların isimlerini de istismar etmektedirler. Burada bilinmesi gereken şey; bu firmaların hiçbir zaman kullanıcılarını veya abonelerini aramadıklarıdır. Bir telefon görüşmesinde, şayet kendiniz aramadıysanız, şahsi bilgilerin verilmesi zaten yanlıştır.

***Online satış sayfalarının istismarı ve sahte alışveriş sayfaları*:** Normalde pahalı olan bir şeyi ucuza kapatmak herkesin hoşlandığı bir durumdur. Suçlular da bunu çok iyi bir şekilde kullanmaktadırlar. Birçok sahte alışveriş sayfası oluşturarak mağdurların bu sayfalar üzerinden alışveriş yapmalarını sağlamakta (reklam pencereleri veya SPAM-e-postaları ile) ve sözde bir mal için önce paranın gönderilmesini istemektedirler. Parayı gönderen mağdurlar ya satın almış oldukları malı görmemekte ya da satın alınan mal yerine başka bir şey ile yüzleşmektedirler. Örneğin bir akıllı telefon yerine birkaç tane salatalık almak gibi. Suçlular aynı zamanda mevcut olan, tanıdık ve gerçek alışveriş sayfalarını istismar etmek suretiyle de mağdurlarına zarar vermektedirler. Örneğin ucuz emlak ya da otomobil satın alma veya kiralama sayfaları üzerinden bunlar yapılmaktadır. Almanya'da en çok görülen olay, ev kiralama sayfaları üzerinden gerçekleştirilmektedir (Immobilien-Scout). Immobilien-Scout üzerinden sözde ucuz bir ev bulan mağdur, evi kiralayan, sözde ev sahibi ile irtibata geçtikten sonra bir e-posta almaktadır: "İlginiz için çok teşekkür ederim. Münih'te bir firmada çalışan bir mühendisim ve beni iki yıllığına çalıştığım firmanın Londra şubesine, geçici olarak tayin ettiler. Ev kendime ait olup, tamamen mobilyalıdır ve her şey bulunmaktadır. Evi iki sene kullanamayacağım için iki seneliğine kiralamak istedim. Şu anda Londra'dayım ve ne yazık ki gelmem mümkün değildir. Ancak, depozito ücreti olan 2000-€ parayı hesabıma gönderirseniz bu konuda ciddi olduğunuzu gösterirsiniz. Para hesabıma geçtiği an apartman görevlisine bilgi vereceğim. Siz de anahtarı ondan alarak eve bakabilir ve şayet hoşunuza giderse, taşınabilirsiniz.". Örneğin, 102 m² bir evi 500-€'ye bulan mağdur (normalinde bu büyüklükteki evlerin kirası Münih şehrinde 1.500-€'dan başlamaktadır), bu şekilde evi kapabilmek için parayı hemen göndermektedir. Bu olayda zarar görmüş olan kişiyi "mağdur" olarak nitelemek de ayrı bir konudur. Bu noktada "paranın gönderildiği banka hesabının sahibine, polis ulaşamıyor mu?" sorusu akla gelebilir. Pek tabii ki de böyle bir olayda polis, banka hesabı sahibine ulaşabilmektedir. Ama suçluya değil. Hemen hemen bütün polisiye soruşturmalarda ulaşılan kişiler normal vatandaşlar olup sadece banka hesaplarını hizmete sunmuş olan kişilerin olduğu ortaya çıkmaktadır. Ama bu kişilerin çoğunluğunun bilmediği bir şey vardır: Yaptıkları işin ismi, kara para aklamaktır. Yani bu durumda kendilerini suçlu duruma düşürmektedirler. Bu kişiler, suçlu duruma düşmeden önce bir e-posta (SPAM) almaktadırlar: "Oturduğun yerde, haftada 3.000,-€ 'ya kadar para kazanmak ister misin? Yapman gereken tek şey, bize banka hesap numaranı göndermektir. Biz de senin hesabına para göndereceğiz. Sen bu paranın, %80'ini hesabından çekip, bize, bir Western Union hesabı üzerinden göndereceksin. Paranın %20'si ise tamamen sana ait. Emin ol ki yapacağın bu işlemler, kanuna aykırı değildir." Bu şekilde yürüyen süreçte polis, parayı Western Union şubesinden teslim alan kişiye ulaşmakta sorun yaşamaktadır. Polisin öncelikle parayı teslim alan kişinin, hangi şubeden teslim aldığını bilmesi gerekmekte ve çok hızlı bir şekilde hareket etmesi zorunluluğu ortaya çıkmaktadır. Zira paranın yatırıldığı dakika içerisinde dünyanın herhangi bir yerindeki bir şubeden para çekilebilmektedir. Yani çoğunlukla, parayı teslim alan kişiye ulaşılamamaktadır. Ulaşılabilse bile parayı teslim alan kişi yine suçlunun kendisi değil bu suç şebekesi için çalışan başka bir kişidir. Bu kişi de yine e-posta

yoluyla işe alınmıştır. Yapması gereken tek şey, bir şubeye gidip parayı teslim almaktır. Paranın yine %20'si ona aittir ve paranın geri kalan kısmı ile ya hediye çeki (Paysafe ya da ITunes gibi) alıp numaralarını suçlulara, elektronik ortamda ulaştırmak (şifreli mesajlar ile) ya da suç şebekesinin kontrolünde olan bir online casino sayfasında parayı yatırmaktır. Bazı durumlarda, paranın geri kalan kısmıyla, elektronik eşyaların alınması ve posta yoluyla, paket istasyonları (DHL Packstation gibi) üzerinden yurtdışına gönderilmesi istenmektedir. Paketin ülke sınırını geçmesi halinde paketin çıkış ülkesinin polisinin yapabileceği bir şey bulunmamaktadır. Bu şekilde suç şebekesi için çalışan hiçbir kişi, asıl suçlunun kim olduğunu bilmemektedir.

Erotik sayfalar üzerinden şantaj: Bu yöntemle erotik sayfaların ziyaretçilerine, kamera aracılığıyla, canlı olarak görüşme yapma talebi gönderilmektedir. Görüşme talebini kabul eden bir kişi, kamera karşısında yapılmaması gereken şeyleri yaptıktan sonra belli miktardaki bir parayı ödememesi halinde videonun tüm arkadaşlarına ve iş yerine gönderileceği yönünde şantaja uğramaktadır. Böyle bir olayda en azından, şantaja uğrayan kişi, gerçekten bir şey yapmıştır. Ancak, yaklaşık altı aydan beri Almanya'da birçok kişi, sözde hackerlardan bir e-posta almışlardır. Bu e-postada alıcı kişinin sözde hacker tarafından hacklendiği iddia edilerek, erotik bir sayfayı ziyareti sırasında videoya kaydedildiği bildirilerek şantaj yapılmaktadır. Bu iddiayı kuvvetlendirmek için de e-postada mağdur kişinin kullanmış olduğu halen aktif veya eski bir şifresi bulunmaktadır. Şifre eski olsa bile birçok kişi bu e-postaya inanıp para göndermişlerdir. Hâlbuki bu maili suçlunun kendisi değil bir bilgisayar programı göndermektedir. Suçlunun yapması gereken tek şey, programa elinde olan e-posta adresleri ve şifrelerini girmektir. Bu tip şantaj olaylarında, paranın kesinlikle ödenmemesi gerekmektedir. Paranın ödenmesi halinde yapılan tek şey, suçluları devam etmeleri için motive etmektir.

Sahte aşk ilişkileri (Love Scamming): Her ne kadar birçok erkek bu yöntem ile mağdur edilmişse de mağdur olan kadınların sayısı, erkeklere nazaran çok daha fazladır. Mağdur olan kişiler, genellikle yalnız yaşayan, bir ilişki arayan ve belli bir yaşı geçmiş olan kişilerdir. İstismar platformları ise başta Tinder olmak üzere çeşitli flirt sayfalarıdır (Parship, ElitePartner vb. gibi). Normal sosyal ağlarda (Facebook gibi) bu yöntem için kullanılmaktadır. Suçluların amacı, öncelikle mağdurla tanışmak, flört etmek ve güveni kazandıktan sonra da mağdurların kendilerine para göndermesini sağlayabilmektir. Bunu sağlayabilmek için de çeşitli hikâyeler uydurmaktadırlar:

- *Şu an Irak'ta bir Amerikan üssünde görevliyim. Saddam'ın gizli evinde birçok para ve altın bulduk. On asker, bunu aramızda paylaştık. Benim payıma düşen miktarı Irak dışına çıkartabilmem için, buradaki bazı kişilere rüşvet vermem gerekiyor. Benim ancak bu kadar param yok. Bana para gönderebilir misin? Memleketime geri döndükten sonra, seninle evlenmek istiyorum ve bana vermiş olduğun paranın hepsini sana geri vereceğim.*

- *Tam seni ziyaret edebilmek için, senin ülkene gelecektim ki tek başıma baktığım kızım, bir trafik kazası geçirdi ve bir an önce ameliyat edilmesi gerekiyor. Ameliyat için gerekli olan paraya ne yazık ki sahip değilim. Bana para gönderebilir misin?*

Bazen para istemeyip, mağdurların hesabına para yatıranlar da var:

- *Seni, ülkende ziyaret etmeyi, o kadar çok istiyorum ki. Emin ol, senin yanına gelirsem evden en az bir hafta çıkmak istemiyorum. Ama ne yazık ki seyahat masraflarımı karşılayabilecek kadar bir param yok. Merak etme, senden para istemiyorum. Üç sene önce benim köyümden bir bayan arkadaşım Fransa'ya gitti. Oraya gidebilmek için de benden borç aldı. Şimdi bu borcumu ödeyebilecek durumda ve bana olan borcunu da ödemek istiyor. Arkadaşım bana bu parayı gönderirse başım maliye ile derde girebilir. O yüzden arkadaşım bu parayı senin hesabına gönderebilir mi? Sen de bu parayı çektikten sonra, bana Western Union üzerinden gönderebilirsin. Ben de en sonunda seni ziyaret edebilirim. Öpücük.*

Pek tabii ki böyle bir durumda mağdurlar sadece kandırılmakla kalmıyor, aynı zamanda da kara para aklama yüzünden kendilerini suçlu duruma sokmuş bulunuyorlar.

Sosyal Mühendislik (Social Engineering): Bu yöntem ile bir bilgisayar veya bir ağ değil sadece insanın kendisi hacklenmektedir. Daha doğrusu kandırılmakta veya yönlendirilmektedir. Suçlular, çeşitli yöntemlerle mağdurlarını etkisi altına almakta ve mağdurların kendilerinin istediklerini yapmasını sağlamaktadırlar. Bunu yapabilmek için de öncelikle mağdurlarının güvenini kazanmak zorundadırlar. Suçlular, bu saldırıda başarılı olabilmek için hedefteki mağdur hakkında bilgi toplamak mecburiyetindedirler. Günümüzde neredeyse her insan kendisi hakkındaki bilgileri sosyal ağlar üzerinden paylaştığı için bu durum suçlular için hiç de zor değildir. Hatta mağdurlarının en son hangi kitabı okumuş olduklarını bile bulabilmektedirler. Sosyal mühendislik yöntemini kullanan suçluların hedef firma hakkında bilgi toplayabilmek için firma kantinine ya da öğle paydosu sırasında çalışanların en yoğun bulundukları ve firma yakınında olan restorana gidip çalışanların yapmış oldukları konuşmaları dinledikleri de bilinmektedir. Kapalı alanlarda sigaranın içilmesinin yasak olması ve çalışanların sigara içmek için dışarı çıkmaları, bu suçlular için ayrı bir bilgi kazanma kaynağıdır. Kendi firmanızda neler olup bittiğini öğrenmek mi istiyorsunuz? Dışarıda sigara içen meslektaşlarınızın yanına gidiniz. Sigara içmenize gerek bile yoktur. Bir mağdura istenilen bir şeyin yaptırılması için sadece hedef şahıs ile direkt irtibata geçmeye gerek yoktur. Mağdurlar, suçlular tarafından bir e-posta ya da bir telefon konuşması ile irtibata geçilmektedir. Örneğin telefondaki saldırgan, kendisini firmanın ağ yöneticisi olarak tanıtarak, çalışanın sisteme giriş bilgilerini elde edebilmektedir. Bunun için yapması gereken tek şey, gerçek ağ yöneticisinin ismini bilmektir. Gerçek ağ yöneticisinin çalışanlar ile senli benli olup olmadığının bilgisi ise kilit öneme sahiptir. Her ne kadar özellikle firmalara zarar verebilmek için hedef sisteme yüklenen zararlı programlar, yapılan saldırılarda kullanılan yöntemler arasında, birinci sırada ise de sosyal mühendislik yöntemi, tüm

dünyada ikinci sıradadır. Hatta hedefteki bir bilgisayara zararlı bir programın yüklenebilmesi için bile çoğunlukla sosyal mühendislik yönteminin kullanıldığı göz önünde bulundurulursa bu konunun ne kadar ciddi olduğu ve çalışanların sosyal mühendislik yöntemleri konusunda bilinçlendirilmeleri gerektiği hususu ayrı bir önem kazanmaktadır. Hiçbir yazılım veya koruma programı, bir firmayı bu yönteme karşı koruyamayacağı için çalışanların meslek içi eğitimlerinde bu konuya da yer ayrılması çok önemlidir. Bir insanın bir makina gibi psikolojik olarak optimize edilebileceği ve bu şekilde manipüle edilebileceği unutulmamalıdır.

Alınması Gereken Standart Tedbirler

Siber suçlar alanında en büyük risk, insanın kendisidir. İnsanlar, hackerların hayatını oldukça zorlayabilecek tedbirleri alsalar bu kadar çok siber mağdurun olmayacağını vurgulamak gerekir. Bu tedbirlerin alınması için belli bir miktarda paranın harcanması ve belli bir zamanın ayrılması gerekmektedir. Ama şu hususun da unutulmaması gerekmektedir: Siber suçlarda maddi olarak mağdur olan sadece şahıslar değil aynı zamanda bir ülkenin kendi ekonomisi de olmaktadır. Çünkü gönderilen paraların büyük bir çoğunluğu yurtdışına çıkmaktadır. Aşağıdaki tedbirleri bilgisayar kullanan her insanın alması gerekmektedir. Bu tedbirler alınmadığında mağdur olmak ya da mağdur olunduğunun farkında olmak güçtür. "Bana bir şey olmaz" düşüncesi ise mağduriyete zemin oluşturmaktadır. Aşağıdaki önlemler, mağduriyetlerin önüne geçmekte katkı sağlayıcı özelliklere sahiptir:

Hardware/Software güncellemeleri: Bilgisayarınızda bulunan işletim sistemi (Windows veya MacOS-Apple) ve kullanmış olduğunuz bütün programların en hızlı şekilde güncelleştirilmesinin yanında bilgisayarınıza takılı olan yazıcının *(printer)* veya kameranın da unutulmaması gerekmektedir. Bir güncelleme demek sisteminizde bu güncellemeyi yapana kadar bir açığın, her zaman mevcut olması demektir. Bu durumda Hackerların yaptığı tek bir şey vardır: Hangi sistemin bu güncellemeyi henüz yapmadığını bulmak (IP-Scan). Birçok program bir güncellemenin olup olmadığını kontrol etse de bazı programlar bunu yapmamaktadır ya da söz konusu programın "ayarlar" kısmından özelliğin aktif hale getirilmesi gerekmektedir. Bilgisayar ekranına "xy programının güncel bir versiyonu mevcuttur" gelmesinin ardından "sonra hatırlat"ın tıklanması kasten "gelin, benim bilgisayarıma girin" demektir. Sadece insanların tembelliği yüzünden ve sözde zamanlarının olmamasından kaynaklı olarak hackerların kontrolü altında olan birçok bilgisayar bulunmaktadır. Hackerlar, saldırılarını gerçekleştirirken tam olarak da bu bilgisayarları kullanmaktadırlar. Şayet bilgisayarınız, birdenbire çok yavaşlıyorsa biliniz ki bilgisayarınız çok büyük bir ihtimalle bir saldırı için kullanılıyordur. Yani suça ortak oluyorsunuzdur. Bu saldırılar için en çok kullanılan bilgisayarlar listesinde Türkiye, tüm dünyada, üçüncü sıradadır. Özellikle "WLAN" fonksiyonu olan yazıcıların bir güncellemesi olup olmadığının sıklıkla kontrol edilmesi gerekmektedir. Bu fonksiyona sahip yazıcıların içinde bir ağ kartının olduğu ve ağ sisteminize bağlı olduğu unutulmamalıdır. Bir

yerde böyle bir yazıcı, yazıcı olarak değil, ağınıza bağlı bir bilgisayar gibi algılanmalıdır. Günümüzde artık, her türlü işlemi üstlenen (fotokopi, tarayıcı, yazıcı) büyük ofis yazıcıları mevcuttur. Bu yazıcılar, genellikle firmaların koridorlarında bulunmakta ve içlerinde, çalışanların basmak için göndermiş olduğu dokümanların saklandığı, 1 TB *(Terabyte)* büyüklüğünde bir hard disk bulunmaktadır. Yani birazcık rol yapabilme yeteneği olan biri, tamirci kılığına girerek bu hard diski yazıcıdan çıkartabilir ve yerine boş bir harddisk takabilir *(Social Engineering)*. Hâlbuki bu sabit disklerin şifrelenmesi mümkündür. Öbür taraftan, bu tip yazıcıların ayarlar kısmında bir şifre ile korunan *ağ yöneticisi* bölümü bulunmaktadır. Buradaki şifre, üretici firma tarafından konulmuş bir şifredir. Hangi yazıcının ve hangi yazıcı modelinin hangi şifreye sahip olduğu ise Darknet'te bir Excel-Listesi olarak bulunabilmektedir. Bu yüzden, bu tip yazıcıların kurulmasının ardından, şifrelerin, şirketin ağ yöneticisi tarafından değiştirilmesine gerek vardır. Aksi takdirde suçluların bu yazıcılar üzerinden, şirketin ağına girebilmeleri mümkün olabilmektedir. Özellikle bu yazıcılarda bulunan USB girişlerinin kapatılması gerekmektedir. Böyle bir yazıcı bir firma için satın alınacaksa *firewall* özelliği olan modellerin seçilmesi önerilir.

Güvenli ve çeşitli şifreler: Bir kişi şifre olarak "123456" ya da "şifre" kelimesini kullanıyorsa bu kişilerin bilgisayar kullanması yasaklanmalıdır. Bu şifrelerin dünyada en çok kullanılan şifreler listesinde ilk iki sıraya yerleşmiş olması, tehlikenin açık göstergesidir. "123456" şifresinin kullanılması ne kadar tehlikeliyse güvenli bir şifre olmasına rağmen aynı şifrenin her yerde kullanılması da o kadar tehlikelidir. Suçlular, herhangi bir yerde bir şifrenize ulaşmışlarsa ve siz bu şifreyi her yerde kullanıyorsanız, bütün hayatınız, suçluların eline geçmiş olacaktır. Ama bu suçlular, yani hackerlar da insandır. Onlar da hata yaparlar. Örneğin onların en çok kullandığı şifre "Hack"tır. Bir şifrenin güvenli olması için, öncelikle kullandığınız bilgisayarın temiz olması gereklidir. Şayet bilgisayarınız Hackerların kontrolü altındaysa, yani bir virüs (Troja) kapmış ise, şifrenizi her gün değiştirmeniz, fayda etmeyecektir. Bu durumda Hackerlar sisteminize bir *Keylogger* programı yerleştirmekte ve bu program sayesinde, bilgisayarınızın klavyesinde yapmış olduğunuz her giriş, girdiğiniz her harf ve sayı bir dosyada saklanmaktadır. Bu dosya ya her gün arka planda, otomatik olarak, suçlulara e-posta üzerinden gönderilmekte ya da Hacker, bilgisayarınıza girerek, bu dosyayı almaktadır. Her yerde başka bir şifrenin kullanılması, düşünüldüğü kadar zor bir şey değildir. Bu konuda yardımcı olabilecek, Password-Manager denilen programlar mevcuttur. Bu programların yardımıyla siz yine, her zamanki gibi, her yerde aynı şifreyi giriyorsunuz, ama bu program sizin için her yerde başka bir şifre giriyor. Bu şifreler de sabit disk üzerinde, özellikle bu program için oluşturulmuş ve şifrelenmiş bir bölgesinde saklanıyor. Güvenli bir şifre için, günümüzdeki standart (2020), şifrenin on iki haneli olması ve büyük/küçük harf, sayı ve ünlem işaretinin kullanılmasıdır. Şifrenizin veya şifreniz içindeki bir bölümün, bir sözlükte bulunabilecek, belli bir kelimenin (çocuğunuzun ismi, tutmuş olduğunuz takım veya bir nesne ismi gibi) olmaması gerekmektedir. Hackerların elinde, tüm dünyada konuşulan bütün dillere ait sözlükleri içeren, birçok dosya bulunmaktadır. Bu şekilde belli bir yöntem kullanarak *(Dictionary Attack)* şifre-

nize ulaşılabilmektedir. Lütfen doğum yılınızı, şifrenizin içinde kullanmayınız. Bunu, tüm dünyada, insanların %60'ı yapıyor ve doğum yılınıza ulaşmak gerçekten çok kolay:

Çok faktörlü kimlik doğrulaması (Multi-***Factor-Authentication***)**:** Birçok sosyal ağ, e-posta sunucuları ve alışveriş sayfaları, iki faktörlü kimlik doğrulaması hizmetini sunmaktadır. Bu hizmeti alabilmek için kullanıcının kendisinin, bu seçeneği aktif hale getirmesi gerekmektedir. Bu yöntem ile kullanıcı bir sayfada giriş yapabilmek için e-mail adresini ve şifresini girdikten sonra cep telefonuna SMS yoluyla bir şifre daha gönderilmektedir. Bu sayede sadece bu şifre girilirse söz konusu sayfaya giriş yapmak mümkün olmaktadır. İkinci şifrenin gönderilmesi sadece SMS yoluyla değil aynı zamanda, anahtarlığınıza takabileceğiniz bir aletle de *(Security-Token)* mümkündür. Siber suçlular, bazı kullanıcıların giriş bilgilerini çaldıktan sonra şifreleri değiştirmektedirler. Böyle bir durumda da bu yöntem ile yeni şifre SMS yoluyla gönderildikten sonra mağdurların kendi hesaplarını tekrar kontrol altına almaları mümkün olabilmektedir. Sonuç olarak çok faktörlü kimlik doğrulaması, birbirinden bağımsız iki aletin (bilgisayar ve cep telefonu), bir sisteme güvenli bir şekilde giriş yapılmasını sağlamaktadır. Birçok banka da bu yöntemi kullanarak müşterilerinin sisteme giriş yaparken klavyeyi nasıl kullandıklarını, hangi hızla tuşlara bastıklarını bile kontrol etmektedirler (*Behavioral Analysis* veya *Keystroke Biometrics*). Bu hizmeti sunan firmaların başında, Almanya'daki *KeyTrac* ya da İsveç'te bulunan *BehavioSec* gelmektedir. Şayet müşteri giriş bilgilerini, her zamanki gibi hızlı değil de yavaş girdiyse online-bankacılık sayfası, müşterinin bilgilerini tekrar girmesini istemektedir. Bazı şirketler, iki değil, hatta üç faktörlü kimlik doğrulaması da kullanmaktadır:

- *Sahip olduğunuz bir şey (Cep Telefonu gibi)*
- *Vücudunuzda olan bir şey (Parmak izi gibi)*
- *Bildiğiniz bir şey (Şifreniz gibi)*

Yetkileri kısıtlı (misafir) hesaplar ve WLAN-modemler: Evinize bir misafirinizin geldiğini düşününüz. Günümüzde, misafirlerin sorduğu ilk soru: *İnternet şifresi ne?* Sonuçta bu soruyu soran kişiyi tanıdığınız için şifrenizi veriyorsunuz. Belli bir zaman sonra, misafiriniz, dizüstü bilgisayarınızı istiyor. Yine veriyorsunuz. Burada bilinmesi gereken bir şey vardır: Az önce misafirinize, her şeyinizi verdiniz. Hele bir de misafiriniz bilgisayarlar ve ağlar konusunda, bilgi sahibi ise hayatınızın kararması bile söz konusu olabilir. Çocuklarınızın olduğu ve çocuklarınızın arkadaşlarına da şifreyi verdiğini göz önünde bulundurursak şifrenizi bilen kişi sayısı oldukça büyüktür. Teknik olarak aynı ağ üzerinde bulunan bütün aletlerle (Bilgisayarlar, cep telefonları, tabletler, televizyon, oyun konsolları, vb.) yani aynı modem üzerinden internet ile bağlantıya geçen her alet ile bağlantı kurmak mümkündür. Pek tabii ki bunu herkes yapamaz, ancak bir kişi bu işlerden anlıyorsa modeminizin şifresini bildikten sonra, her yere girmesi mümkündür. Akıllı ev konseptini de düşündüğünüzde bütün hayatınız teknik olarak şifrenizi bilen her kişinin eli altındadır. Şifrenizi kimseye vermiyorsanız, peki

modeminizin şifresini ve ağınızın ismini değiştirdiniz mi? Çünkü modeminizin, yani ağınızın ismi ve şifresi, genellikle modeminizin arkasında veya altında yazıyor. Modem kurulumunun ardından bu bilgilerin değiştirilmesi gerekmektedir. Eğer değiştirmezseniz, marka ve model bilgileri ve nasıl girileceği bilgisi DarkNet'te mevcuttur. Hoteller, restoranlar veya cafeler gibi halka ve müşterilere açık olan ağları düşünmek, insanın tüylerini ürpertiyor. Bazılarında ağa girebilmek için şifre bile bulunmuyor. Bu tip yerlerde internete girmek gerekiyorsa gerekli önlemlerin alınması şarttır. Örneğin, bir VPN *(Virtual Private Network)* Tüneli açarak bağlantı, güvenli bir hale getirilebilmektedir. Bu hizmeti sunan programlar ve akıllı telefon uygulamaları bulunmakla birlikte virüs yazılımları da bu opsiyonu sunmaktadır. Bir bilgisayara bir programın yüklenebilmesi için yönetici *(Administrator)* yetkisinin olması gerekmektedir. Böyle bir yetki yoksa herhangi bir şeyin sisteme yüklenmesi mümkün değildir. O yüzden de bilgisayar ile internette dolaşılacak ise misafir hesabıyla dolaşmak, alınabilecek en güzel tedbirdir. Bu şekilde şayet tehlikeli bir sayfada iseniz, bunun farkında değilseniz ve bu sayfa arka planda sisteminize zararlı bir program yüklemeye çalışırsa, başarılı olamayacaktır. Diğer bir deyişle dizüstü bilgisayarınızı misafiriniz bir şeye bakmak için kullandığında misafir hesabını açıp, öyle veriniz. Misafir hesabı, modeminizde de oluşturulabilir. Bu şekilde misafirlerinize, kendi internet şifrenizi değil, misafir hesabı şifresini verebilirsiniz.

Virüs koruma yazılımları: Bir bilgisayarda virüs koruma yazılım programı yoksa o bilgisayar ve kullanıcısı için yapılabilecek hiçbir şey bulunmamaktadır. Her gün yaklaşık 300.000 adet yeni virüs veya virüs versiyonlarının ortaya çıkmasına rağmen böyle bir tedbire lüzum hissedilmemişse bilgisayarınızı internete bağladığınız saniye içerisinde bilgisayarınız artık virüslüdür ve başkalarının kontrolü altındadır. O yüzden, yeni bir bilgisayar alınırsa, USB üzerinden öncelikle bilgisayara güncel bir virüs yazılımının kurulup, ondan sonra ağa alınmalıdır. Akıllı telefonlarda da özellikle Android işletim sistemli akıllı telefonlarda, bir virüs uygulamasının kurulması gerekmektedir. Bir virüs yazılım programının veya uygulamasının sadece kurulması da yeterli değildir. Programın, kullanıcının ihtiyacına göre, doğru ayarlanması gerekir. Sadece programın kurulmuş olması, %100 yeterli değildir. Günümüzde evde kullanım için Windows tabanlı bir işletim sistemine sahip iseniz Microsoft firmasının kendi virüs yazılımı *(Defender)* yeterlidir. Defender'ın aktif olması halinde, başka bir virüs yazılımının kurulması doğru değildir. Kurulması halinde Defender'ın pasif hale getirilmesi gerekmektedir. Yoksa iki program, karşılıklı olarak, sürekli birbirlerini engellemeye çalışıp, sisteminizin yavaşlamasına sebep olabilecektir. Bütün bunların olabilmesi için tek bir şart vardır: lisanslı bir işletim sistemi ve lisanslı programlar kullanmak.

***Diğer tedbirler*:** Şayet bir e-postayı şifrelemeden gönderirseniz bunun mektup zarfı olmadan gönderilen bir posta kartından farkı yoktur. Yani göndermiş olduğunuz mesaj herkes tarafından okunabilir, mesajınız yoldayken alınıp değiştirilebilir *(Man-in-the-middle attack)* ve bütün komünikasyonunuz denetlenebilir. O yüzden, özellikle şirketlerde, mesajların şifrelenmesi, en azından dijital olarak

imzalanması, güvenli bir iletişim için çok önemlidir. Bulut *(cloud)* sistemlerinin kullanılması halinde de dosyaların veya resimlerin öncelikle kendi sistemlerinde şifrelenmesi ve daha sonra bir Cloud Server'ına yüklenmesi, bazı şirketler ve özellikle kamu kurumları için casusluk faaliyetleri veya sanayi casusluğu açısından önleyicidir.

Son olarak, insanların artık bilgi tasarrufu yapmaları ve hoşlandıkları veya hoşlanmadıkları herşeyi, durmadan bildirmeyi, arkadaşlarının kim olduğunu göstermeyi, hayallerini veya umutlarını herkese anlatmayı bırakmaları, düşüncelerini ve umutlarını açıklarken bunu herkesin okuyabileceğini unutmamaları gerekmektedir. Bazı şeyleri kendinize saklayınız, güven içerisinde yaşayıp, yaşamınızın keyfini, aileniz ile birlikte çıkarınız.