Derinlemesine Güvenlik Stratejisi

Cyber Crime & Analiz

El Kitabı

SİBER SUÇ FAALİYET VE ANALİZİ

Massachusetts'te bir genç, bir liseye bomba tehdidinde bulunur. Standart prosedürün ardından, okul iki günlüğüne kapanır ve tehdide müdahale etmek için itfaiyeyi, Acil Sağlık Hizmetlerini ve bomba imha ekibi ve köpek ekibiyle birlikte kolluk kuvvetlerini aramak zorundadır. Aylar sonra, aynı genç büyük bir ulusal telefon servis sağlayıcısına gizlice girer ve birkaç kurbanın kişisel bilgilerini, tüm arkadaşlarının ve ailelerinin telefon numaraları da dahil olmak üzere çalar ve genç daha sonra bunları internette yayınlar. Genç, şirketten telefon hizmetini çalıyor ve aynı şeyi birkaç arkadaşı için yapıyor, bu arada lisedeki operasyonları daha fazla bomba tehdidiyle bozmaya devam ederken, her biri Acil Durum personelinin yanıtını gerektiriyor. Telefon şirketi hırsızlığı fark edip hizmeti kapattığında, genç tuhaf tehditler gibi görünen şeyler yayınlar, ancak şirketin pes etmeyi reddetmesinden on dakika sonra, bu genç başarıyla saldırır ve sağlayıcının ticari operasyonlarının önemli bir bölümünü sakatlar.

On beş ay boyunca, genç bir milyon dolardan fazla zarar veriyor. Genç, birden fazla suçtan hüküm giydiğinde, on bir ay gözaltı ve iki yıl denetimli salıverme cezasına çarptırılır. Bu süre zarfında, genç elbette yukarıdaki tüm suçların işlendiği silahtan uzak tutulmalıdır: bir cep telefonu. [25]

İnternet ve benzeri telekomünikasyon arenasında veya bunların yardımıyla veya bu arenada işlenen herhangi bir suç faaliyetini ifade eden "siber suç", hem eski suçların yeni bir araç aracılığıyla yeniden vücut bulması hem de kendi başına benzersiz bir varlıktır. Fiziksel veya "karasal" suçtan dört ana yönden farklıdır: işlenmesi kolay olması, büyük

potansiyel zarar için minimum kaynak gerektirmesi, failin fiziksel olarak bulunmadığı bir yargı alanında işlenebilir olması ve çoğu zaman tamamen yasadışı olmaması. [24] Vandalizmden hırsızlığa, gasptan telif hakkı ihlaline kadar hemen hemen her suç bir siber suç haline gelebilir.

Yeni teknolojinin sıklıkla yaptığı gibi, siber suç, suçluları yeni yollarla da güçlendirir; örneğin Massachusetts'li bu genç gibi bireylerin, daha önce kendi liglerinin çok dışında sayılan, ancak şimdi sadece telefon şirketi gibi varlıklara zarar vermelerine izin vermek gibi. doğru özel yeteneklere ve motivasyona sahip bir saldırgana karşı herkes kadar savunmasız. Aynı zamanda, sanattan devlete ve işletmeye kadar modern yaşamın tüm yönlerinin artan dijitalleşmesi, bahislerin büyük ölçüde artmasına ve dolayısıyla siber suç için teşviklerin artmasına neden oldu.

Bu makale, siber suç saldırılarının kısa bir tarihi ve buna karşılık gelen savunmalarla başlayarak siber suçları çeşitli perspektiflerden inceleyecektir. Bazı tipik saldırganların profilini çıkararak, onların çeşitli beceri seviyelerini ve motivasyon faktörlerini tanıtacağız. Üçüncü bölümde, siber suçluları yakalamak için kullanılan siber adli tıpla ilgili yasal ve teknik prosedürleri detaylandırarak kolluk kuvvetlerini ele alacağız. Dördüncü bölüm, siber suçlarla ilgili mevcut yasa ve politikalara ve bunun içerdiği sınırlara ve sorunlara ilişkin bir kılavuzdur. Son olarak, mevcut eğilimleri ele alacağız, yaygın güvenlik açıklarından bahsedeceğiz ve siber suçun ekonomi, tüketici güveni, askeri ve ulusal güvenlik üzerindeki etkisini değerlendireceğiz.

I. Tarih

Siber suçların yükselişi:

Elektronik Sayısal Entegratör ve Bilgisayar (ENIAC), İkili Otomatik Bilgisayar (BINAC), Evrensel Otomatik Bilgisayar (UNIVAC) ve diğer delikli kart tablolama makineleri gibi ilk bilgisayarların bazı doğal güvenlik avantajları vardı. Bunlar bağımsız sistemlerdi, devasa ve çok pahalıydı ve ayrıca pek çok insan bilgisayarın gerçekte ne olduğunu bilmiyordu. Programlanmış Veri İşlemcisi (PDP-1) gibi ticari bilgisayarlar, makineyi zaman paylaşımı temelinde şirketlere ve bireylere kiralama iş modeliyle 1960'larda tanıtıldı .[8] Bu, içinde depolanan verileri ve programları savunmasız hale getirdi ve böylece hacklemenin ilk kapıları açıldı. İlk bilgisayar korsanları grubu, MIT'nin ilk PDP-1'ini almasından kısa bir süre sonra, 1961'de Massachusetts Teknoloji Enstitüsü'nden (MIT) geldi. [8]

1970'lerde, bilgisayarlar yavaş yavaş tanıtılırken, telefon sistemi zaten iyi kurulmuştu. Ücretsiz telefon görüşmeleri yapma fikriyle gelişen ve onu kırmanın çeşitli yollarını arayan, dolandırıcılar olarak bilinen meraklı bir grup insan vardı. Bilinen ilk dolandırıcılardan biri, telefon şirketinin şehirlerarası hizmetine erişmeye ve ücretsiz aramalar yapmaya yardımcı olan tonlar üretmek için yazılım yazan MIT'den Stewart Nelson'dı. Dolandırıcılar, 2600 hertz sinyali üretecek şekilde programlanmış mavi kutulu bir cihaz yarattılar ve bu, ana hat oluşturmak ve ücretsiz uzun mesafe aramalar yapılmasını sağlayan operatör hattını başlatmak gibi kötü şeyler yapmalarına izin verdi. Steve Wozniak ve Steve Jobs'un (Apple Computer'ın gelecekteki kurucuları) benzer cihazların erken üretim ve dağıtımında yer aldıkları biliniyordu.

1970'lerde ilk uygun fiyatlı PC olan Altair 8800'ün piyasaya sürülmesi ile bireylerin bilgisayar sahibi olmaları ve programlamayı öğrenmeleri mümkün hale geldi. Bu öğrenme, kısa süre sonra bazı kişiler tarafından tam teşekküllü bir bilgisayar korsanlığı için bir susuzlukla takip edildi. Eşzamanlı olarak Radio Shack'in TRS-80'i ve IBM PC gibi diğer bilgisayarların ortaya çıkması, sistemin yeteneklerinden yararlanmanın yeni yollarını bulmaya hevesli insanlara daha güçlü bilgi işlem getirdi [8]. Ancak bu bağımsız sistemler, makine tehlikeye girdiğinde yapılabilecek hasar potansiyelini sınırladı. Yalnızca ağ oluşturma kavramlarının tanıtılmasıyla, bilgisayar korsanlığının taşkınları açıldı. İlk ağ modeli, kullanıcıların dosyaları paylaşmasına ve programları çalıştırmasına izin vermek için birçok terminalin bağlı olduğu güçlü bir ana bilgisayardan oluşuyordu. Bu, bilgisayar korsanlarının diğer ana bilgisayar kullanıcılarının dosyalarına erişmesine ve bunlardan yararlanmasına izin verdi.

Günümüzün ağ teknolojisi muazzam bir şekilde gelişti ve eşler arası iletişim gibi yeni kavramlarla ana bilgisayar modelinin ötesine geçti. Ethernet gibi standartlar, satıcıların bilgisayarları kolay ve ucuz bir şekilde birbirine bağlayan uyumlu ürünler yaratmasını sağladı. Birlikte çalışabilirlik, sağlıklı bir ekosistemi teşvik etmek ve ekonomik büyümeyi geliştirmek için herhangi bir iş perspektifinden önemli bir husustur . Ne yazık ki, bu açık standartlar, bilgisayar korsanlarının yaygın olarak bulunan protokolleri tersine mühendislik yaparak sistemlere girmesini de kolaylaştırdı .

Bilgisayarlar daha ucuz hale geldikçe ve ana akım olmaya başladıkça, aralarında sorunsuz etkileşim için çaba sarf edildi. ARPANet böyle bir çabaydı ve tasarımı sırasında, ağdaki az sayıda düğümün güvenlik ihlallerinin oluşturduğu tehdidin kapsamını sınırladığını düşündükleri için, araştırma bilim adamları için güvenlik büyük bir sorun

değildi. Ancak, 1988'de Cornell Üniversitesi'nde yüksek lisans öğrencisi olan Robert T. Morris, UNIX sistemleri üzerindeki etkisini test etmek için hükümetin ARPANet'i üzerinde kendi kendini kopyalayan bir solucan başlattı. Solucan Amerika Birleşik Devletleri'nin her yerine yayıldı, binlerce ağa bağlı bilgisayara bulaştı, hükümet ve üniversite sistemlerini tıkadı ve İnternet'i durma noktasına getirdi. Bu, bazılarının kötü niyetli olduğunu fark eden İnternet kullanıcıları için bir uyandırma çağrısıydı.

1990'ların başında, İnternet erişiminin ticari olarak uygun bir fiyata erişilebilir hale gelmesiyle, saldırıların sayısı da arttı ve siber suçlar artık uluslararası sınırları aşıyordu. Uluslararası manşetlere çıkan ilk siber casusluk vakası arasında, Batı Almanya'daki bilgisayar korsanları ABD hükümetine ve kurumsal bilgisayarlara sızmak ve işletim sistemi kaynak kodunu Sovyet KGB'sine satmaktan tutuklandı. Başka bir olayda, Rus kraker Vladimir Levin, Citibank'tan 10 milyon doları çekti ve parayı dünyanın dört bir yanındaki banka hesaplarına aktardı [15] . Aynı zamanda, dolandırıcıların ve bilgisayar korsanlarının ticaret ipuçları hakkında dedikodu yapmasına, çalınan bilgisayar şifrelerini ve kredi kartı numaralarını paylaşmasına ve warez (korsan yazılım için hacker jargonu) dağıtmasına izin veren ilk elektronik bülten tahtası sistemleri (BBS'ler) ortaya çıktı.

Netscape Navigator ve Microsoft Internet Explorer gibi zengin tarayıcıların piyasaya sürülmesiyle, 90'ların ortalarında Web'deki bilgilere erişim kolaylaştı. Bilgisayar korsanları artık "nasıl yapılır" bilgilerini ve bilgisayar korsanlığı programlarını BBS'lerden yeni bilgisayar korsanlarının Web sitelerine taşımaya başladılar. Bilgi ve kullanımı kolay araçlar, Net erişimi olan herkes tarafından yaygın olarak kullanılabilir hale geldikçe , saldırıların sayısı da büyük ölçüde arttı . Genel Muhasebe Ofisi tarafından Savunma Bakanlığı

bilgisayarlarının devam ettiğine dair raporlar vardı. Yalnızca 1995'te bilgisayar korsanları tarafından 250.000 saldırı [11].

1990'ların sonlarında, Hacker'lar, zayıflıklarını göstermek için Microsoft'un Windows işletim sisteminde güvenliği deldi. Truva atı virüsü 1998'de Windows 95 veya Windows 98 çalıştıran bir makinede makineye yetkisiz uzaktan erişime izin veren 'Cult of the Dead Cow' grubunun hacklenmesiyle ortaya çıktı. Bu süre zarfında spam saldırısı da görüldü. Bunun bir örneği, günlerce yüz binlerce sahte bilgi talebiyle dolup taşan 1998 yılında Federal Çalışma İstatistikleri Bürosu'na yapılan saldırıdır. Web sitesi, en son ekonomik verileri almak için ona bağımlı oldukları için ekonomistleri ve yatırımcıları hayal kırıklığına uğrattı [16] . Ayrıca, Yahoo ve AOL gibi İnternet portalları da spam saldırılarının hedefiydi. Yahoo! 1997 yılının Noel Günü'nde kullanıcıların bilgisayarlarında bir "mantık bombası" patlayacağını iddia eden hackerlar tarafından vuruldu. megabaytlık e-posta bombaları ve sohbet odaları spam mesajlarıyla bozulacak.

Yirmi birinci yüzyılda ortaya çıkan solucanlar ve virüsler, maddi hasar ve verimlilik kaybı açısından daha yüksek bir etkiye sahiptir. Bir örnek, Mayıs 2000'de yakalanan "Aşk Mektubu" solucanı, şirketlere 960 milyon dolarlık temizlik maliyetine ve 7,7 milyar dolarlık üretkenlik kaybına neden oldu [12]. 2001'deki Nimda ve Code Red virüsü, virüslerin herhangi bir kullanıcı etkileşimi olmadan İnternet'e yayılabileceği ve ardından otomatik olarak hizmet reddi (DoS) saldırısı gibi başka saldırılar başlatabileceği yeni tehditler başlattı. Microsoft, kullanıcıları bozuk bağlantılara götüren ve iki gün boyunca milyonlarca kullanıcının Microsoft Web sayfalarına ulaşmasını engelleyen DNS saldırısının hedefi oldu. Ocak 2002'de İnternet'e yayılan Slammer solucanı kısa süreli İnternet kesintilerine neden oldu. Bir dijital risk firması olan mi2g Intelligence Unit (mi2g.net) tarafından hazırlanan

bir rapora göre, 2004 yılında Mydoom virüsü 215 ülkede 43,9 milyar dolarlık ekonomik hasara neden oldu **.** Bu virüs, ağlarımıza gelmiş en kötü virüs olarak kabul edilir.

Bu saldırıların arkasındaki teşvikler ve motivasyon:

Erken saldırıları incelersek, ilk bilgisayar korsanlarının temelde makinelerde sırf zevk için programlayan programcılar olduğunu görebiliriz. Bu merak, orijinal anlamıyla hacklemenin özü olarak yorumlanabilir. Bazıları kişisel ün kazanmak için bu eyleme dahil oldu. *WarGames* ve Iain Softley'in *Hacker'ları* gibi filmler , bir bilgisayar korsanının karakterini asil amaçlar için yasaları çiğneyen parlak ve romantik bir adam olarak gördükleri için çok az kişiyi motive etti.

Günümüzün sofistike saldırıları daha büyük bir hasar potansiyeline sahiptir. Hacker gruplarının askeri yazılımları çalmak için Pentagon ağına sızma iddiaları ve ardından talepleri karşılanmazsa teröristlere satma tehditleri artıyor. Bu, saldırganların kapsamının ve niyetinin kontrol dışı bir şekilde arttığını gördüğümüz için siber suç faaliyetinin yüzünün değiştiğinin açık bir göstergesidir. Bilgisayar korsanları artık hevesli siberger profiline sahip gençler değil, parasal çıkarları ve bencil amaçları olan gerçek kötü niyetli adamlar. Bugün, siber suçları amaçlarını gerçekleştirmek, yani terörü yaymak için potansiyel bir mod olarak gören saldırganlar ve terör örgütleri arasında güçlü bir bağlantı görüyoruz. Aşağıdaki *"Saldırgan – Bir profil"* bölümü, çeşitli profiller ve bunların teşvikleri hakkında ayrıntılı bir tartışmaya sahiptir.

Savunmanın paralel gelişimi:

Saldırılara karşı korunmak için önleyici tedbirler, siber suç faaliyeti keşfedilip rapor edilir edilmez gelişti. Örneğin telefon şirketleri, cinlere karşı taarruza geçmek için Elektronik Anahtarlama Sistemini (ESS) kullanmaya başladı. ESS, sesin, alınmadığı sürece, aranan tarafın hattına doğrudan bağlanmadığı, bilgisayar tarafından oluşturulan yapay bir zil göndererek, telefonun fısıltısını son derece zorlaştırdı. ESS neredeyse tüm büyük şehirlerde kurulduğundan mavi boksu zorlaştırdı.

Federal Hükümet ayrıca siber suç faaliyetlerini durdurmak için adım attı ve bilgisayar korsanlarına karşı ulusal bir baskı uyguladı. Hükümet ve şirket bilgisayarlarına artan sayıda izinsiz girişin ardından, Kongre 1986'da bilgisayar sistemlerine girmeyi suç haline getiren 'Bilgisayar Dolandırıcılığı ve Kötüye Kullanımı Yasası'nı kabul etti. Ayrıca, aynı yıl kabul edilen 'Kapsamlı Suç Kontrol Yasası', Gizli Servis'e kredi kartı ve bilgisayar dolandırıcılığı konusunda yargı yetkisi verdi (Mevcut Kanun ve Politika Bölümü bu konuda ayrıntılı olarak konuşuyor). Ayrıca, Bilgisayar Acil Müdahale Ekibi, bilgisayar ağlarına yönelik artan saldırı hacmini araştırmak amacıyla ABD savunma teşkilatları tarafından oluşturulmuştur. Eşzamanlı olarak, FBI gibi istihbarat servisleri hızlandı ve siber korsanları avlamak için soruşturma başlattı. Hackerların ilk tutuklanmalarından birinde FBI, üyeleri Memorial Sloan-Kettering Kanser Merkezi'nden Los Alamos'a kadar 60 bilgisayar hırsızlığıyla suçlandıktan sonra Milwaukee merkezli 414'leri bastı.

Nükleer silahların geliştirilmesine yardımcı olan Ulusal Laboratuvar . [11]

Teknolojinin siber suça tepkisi, IP katmanında yerleşik kimlik doğrulama, entegrasyon, gizlilik ve erişim kontrolünü destekleyen IPv6 protokolünün icadıydı. Norton ve MacAfee gibi şirketlerin antivirüs ürünleri , ev bilgisayarlarında kullanım için daha

belirgin hale geldi . Ayrıca Windows İşletim Sistemi ve diğer Microsoft ürünlerinde güvenlikten yararlanan bir dizi saldırı gerçekleştiren Bill Gates, Güvenilir bilgi işlem vizyonunu özetledi [17]. Bu, mevcut Microsoft sürümlerinde daha güvenli ürünlerle sonuçlandı. Yazılım şirketleri, piyasaya sürülen bir üründe güvenlik açığı keşfedilir keşfedilmez tavsiyeleri ve yamaları yayınlamaya çalışır . Güvenlik, güvenlik incelemelerinin yapıldığı, çeşitli potansiyel tehditlerin derinlemesine risk analizini yapmak için tehdit modellemesinin yapıldığı yazılım geliştirme yaşam döngüsünde günümüzde önemli bir husustur.

Ne öğrenilir?

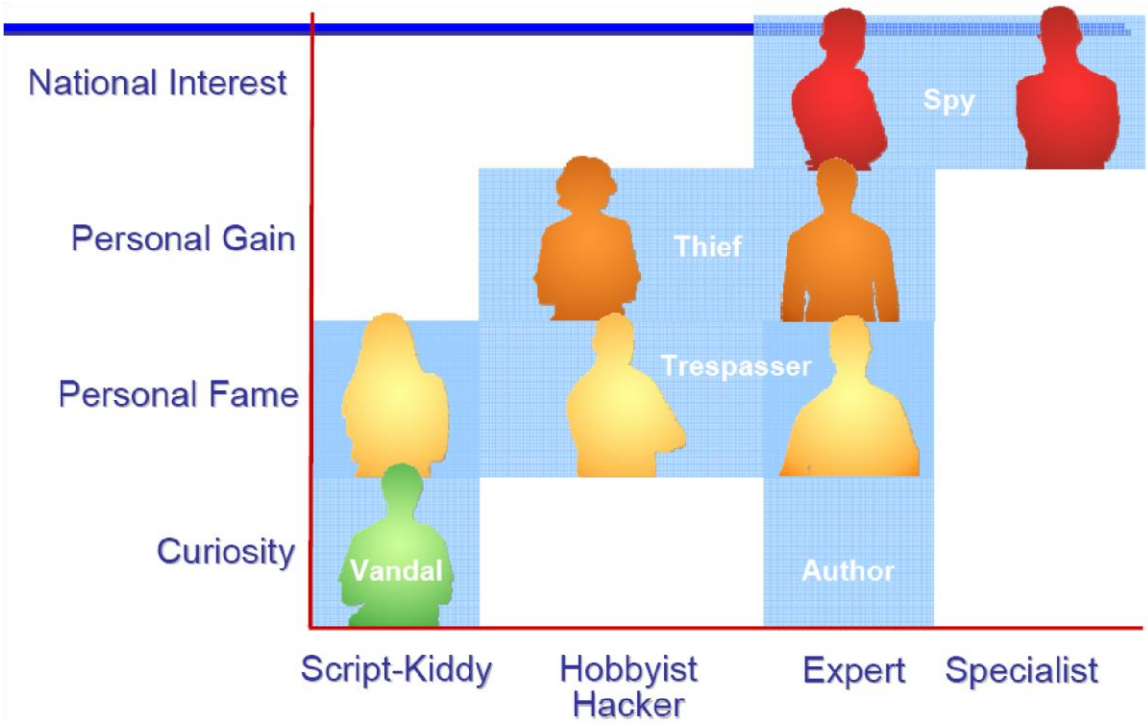
İlk bilgisayar ağları kurulduktan kısa bir süre sonra, bazı insanların istismar etmenin yollarını aradıklarını ve böylece siber suçları doğurduğunu ilan etmek güvenlidir. Bununla birlikte, siber suçlar bir gecede tamamen gelişmiş bir sorun olarak ortaya çıkmadı. Bu sorun, bilgi işlem daha kolay, daha ucuz ve daha kolay erişilebilir hale geldikçe ortaya çıktı ve büyüdü. Teknoloji ilerledikçe, güvenlik açıkları keşfedilir ve ardından bu güvenlik açıklarına karşı savunmalar gelişir. Ancak daha sonra yeni ürünler piyasaya sürülür, yeni güvenlik açıkları kısa sürede keşfedilir ve bu kısır döngü asla sona ermez. Siber saldırı yıkımının zaman içinde test edilmiş örnekleri ve son birkaç yılda terörizmin yükselişi ile Siber suçlar, ülkeler ve kuruluşlar için ciddi bir tehdit olarak ortaya çıkmıştır. Terör örgütünün siber suçları benimsemesi, hayal gücünün ötesinde bir zarar potansiyeline sahiptir.

II. Saldırgan – Bir Profil

Hacker profiline bakış açısının değişimini belirtmek için 1990'da bilgisayar korsanlarına yönelik ilk federal baskıya katılan en yüksek rütbeli federal yetkilinin sözlerinden daha güçlü hiçbir söz yoktur: yatak odalarında bilgisayarlarıyla oyun oynuyorlar. Bazıları artık yasa dışı davranışlarda bulunmak için bilgisayar kullanan yüksek teknolojili bilgisayar operatörleri." [19] Tipik bir bilgisayar korsanının daha önceki hesapları, şu basit profilden oluşuyordu: gençliğinde beyaz erkek, genellikle zeki ve üst orta sınıf bir aileden [18] . Orijinal hacker profilindeki basitlik, bilgisayarları yalnızca belirli bir sınıf için ekonomik hale getiren ve ırksal geçmişle güçlü bir şekilde ilişkili olan ekonomi de dahil olmak üzere birçok faktöre atfedilebilir. Önemli hasar potansiyelinin olmaması ve algılanan finansal kazanç da bu faktörler arasında sayılabilir. Tüm bu faktörlerin 1980'lerde büyük ölçüde değişmeye başlaması ve internetin metalaşmasıyla birlikte, hacker profili gelişmeye ve çeşitlenmeye başladı.

Hacker profilinin kökleri, Geçmiş bölümünde açıklanan telefon tasavvuruna kadar uzanır. Telefon dolandırıcılığı, bilgisayar korsanlığının öncülü olarak görülebilir ve bilgisayarların ve modemlerin açıkça kullanılabilir hale gelmesinden önce de vardı. Phreaking bu güne kadar çok canlı ve telefon ile bilgisayar arasındaki hatların bulanıklaşması göz önüne alındığında, ilkinin dijital alana girmesi ve daha sonra bir telefon cihazı olarak kullanılması nedeniyle bilgisayar korsanlığı olarak kabul edilebilir. Elbette yüksek düzeyde bağlantı ve bant genişliği bolluğu ile bilgisayar korsanlarının hacklemek için sadece telefonlardan daha fazlası var.

Niyete, hasar potansiyeline, beceri setine vb. dayalı birkaç hacker sınıflandırması var gibi görünüyor. İnsanlar, bilgisayar korsanlarını iyi ve kötü niyetli bilgisayar korsanlarına atıfta bulunarak beyaz şapkalı ve siyah şapkalı olarak sınıflandırdı. Diğer sınıflandırmalar, bilgisayar korsanlarını meraklı, her şeye burnunu sokan ve suçlu olarak ayırır [18] . David Aucsmith tarafından daha kapsamlı bir sınıflandırma ileri sürülmüştür. Aucsmith sınıflandırması, beceri düzeyi ve motivasyona dayalı çok boyutlu bir sınıflandırmadır. Model aşağıdaki şemada gösterilmiştir (David Aucsmith'in izniyle)



Beceri ve motivasyon basamakları, çok az veya hiç önemli programlama geçmişi olmayan nispeten deneyimsiz 'Vandal' tarafından başlar. Bu kategorideki bilgisayar korsanları genellikle meraklarından motive olurlar ve kişisel ün kazanma veya en azından akranları arasında övünme hakları elde etme arzusuyla yönlendirilirler. Bu bilgisayar korsanlarına bazen komut dosyası gibi daha yüksek seviyeli programlama dilleri kullanmalarından kaynaklanan komut dosyası çocukları denir. Çoğunlukla daha deneyimli

bilgisayar korsanları tarafından üretilen bilgi ve araçlara güvenirler. Yaş grupları ve göreceli deneyimleri göz önüne alındığında, daha az sorumlu olma eğilimindedirler ve genellikle virüsleri ve solucanları vahşi doğaya bırakan sınıftırlar. Bu profilin bir örneği, solucan Sasser'ın genç yazarı Sven Jaschan. Jaschan, script-kiddy profiline çok iyi uyuyor. Sasser solucanını yazdığında 17 yaşındaydı. Ayrıca, başka bir solucan olan Dabber'ın Sasser'daki bir güvenlik açığından yararlanmak ve aynı ana bilgisayarlara bulaşmak için oluşturulduğu gerçeğine göre nispeten deneyimsiz bir kodlayıcıdır.

Model daha sonra, aynı zamanda şöhret arzusuyla hareket eden, ancak becerilerinde uzmanlığa kadar uzanan 'İzinsizciler'i tanımlar. Solucanları serbest bırakmak yerine, izinsiz girenler bildiklerini veya daha deneyimli bilgisayar korsanlarından yararlanabileceklerini kullanmamaları gereken yerlere gitmek için kullanırlar. Önceki profilde olduğu gibi, finansal kazanç onlar için bir faktör bile değil. Sebepsiz olarak "aşmak" mantıksız gelse de, bu profilin "Hacker Crackdown"dan Bruce Sterling'in tanımladığı zihniyeti göz önüne alındığında daha anlaşılır hale geliyor. Ona göre izinsiz giriş yapan bilgisayar korsanları, tüm kuralların ötesinde bu elit olma duygusuna sahiptir. Onlara göre kurallar, özel ihtiyaçları olanların koyduğu yapay sınırlardır. Hackerlar kendi kurallarını koyarlar. Bu hacker kategorisi ayrıca dünyaya ne kadar harika olduklarını söyleyerek övünerek hacker yakıtıyla beslenir. Diğer bir motivasyon ise, 13 yıl boyunca FBI'ın en çok arananlar listesinde yer aldıktan sonra 1995 yılında tutuklanan Kevin Mitnick'in anlattığı yolculuk keyfi. Mitnick'in 60 dakikalık röportajına göre, yüksek savunmalı kurumsal BT sistemlerine izinsiz girdiğinde kendisini "James Bond" gibi hissetti. Mitnick, evliliği de dahil olmak üzere kişisel hayatını da mahveden sistemlere günde 10 ila 12 saat harcadığı için bilgisayar korsanlığına olan sevgisini bir bağımlılık olarak

sınıflandırdı. Bağımlılık, izinsiz girme uğruna bu kadar yoğun bir izinsiz girme arzusunu haklı çıkarmanın başka bir yolu olabilir.

Üçüncü tip 'Hırsız' hacker'dır. Hırsız, adından da anlaşılacağı gibi, esas olarak bir tür yasadışı kazançla ilgilenir. Bazıları, yine daha deneyimli bilgisayar korsanları tarafından yazılmış araçlara güvenen ara bilgisayar korsanlarıdır veya kendi araçlarını yazan uzman bilgisayar korsanları olabilirler. Suçların kapsamı sınırsızdır ve FBI Siber Süpürme girişimi aracılığıyla bahsedilen tartışmamızla ilgili olanlar: "siber şantaj, ekonomik casusluk (Ticari Sırların Hırsızlığı), Kimlik Hırsızlığı ve kredi kartı hırsızlığı". Para faktörü nedeniyle, bu, Aucsmith'e göre siber suçun en yaygın biçimi ve ekonomiye en maliyetlisi gibi görünüyor. Aucsmith'in analizine göre bu, hacker popülasyonunun en hızlı büyüyen bölümü gibi görünüyor. Bu, FBI Bilgisayar Güvenliği Enstitüsü'nün 2003 yılında yaptığı yıllık anket tarafından onaylanmıştır. Anket, rastgele ankete katılan şirketlerde farklı hacker gruplarının (profillerinin) neden olduğu nispi yıllık kaybın, tescilli verilerin çalınması nedeniyle 70.1 milyon dolar ve hizmet reddi, virüslerden 27,3 milyon dolar. Gizli kimlik varlık gaspçısı "Zilterio", bir MSNBC e-posta röportajında şirketlerin kendisine 150.000 dolarlık "sessiz para" ödediğini gururla itiraf etti. Dışarıda muhtemelen binlerce "Zilterios" olduğu gerçeği göz önüne alındığında, bu rapor edilmemiş çok fazla para. Bu kategorideki hackerlar için norma aykırı olan "Zilterio", muhabirlere taahhüt ettiği zorla girme olayları hakkında e-posta gönderen ve çevrimiçi röportajları kabul eden vokal tipi gibi görünüyor. Ona göre tanıtım, kişisel şöhret için değil, bir pazarlama aracıdır. Bu kategorideki bazı bilgisayar korsanları, kâr elde etmenin yanı sıra dünyaya günümüz güvenliğinin ne kadar kötü olduğunu gösterme misyonunu da üstlendiklerini iddia ediyor [22] .

Son olarak, en yüksek beceri düzeyine ve ulusal güvenlik üzerinde en büyük etkiye sahip olan 'Casus' profiline geliyoruz. Siber casuslar, yabancı hükümetler tarafından korunan ve genellikle kapsamlı eğitime sahip olan bilgi çalma hedeflerine ulaşmak için daha kararlıdır. Alabilecekleri bilgilerin değeri ve birlikte çalıştıkları hükümetin kontrolü altındaki kaynakların bolluğu göz önüne alındığında, casus için ekonomik faktör de mevcut olabilir. Tarih bölümü, ABD'de KGB için çalışan bir Batı Alman casusu olan Markus Hess'i içeren en eski kovuşturma casus hack vakasından bahseder. Hess 1986'da tespit edildi ve 1990'da yargılandı. Casus bilgisayar korsanları genellikle çok karmaşıktır ve saldırının yerel olarak kaynaklandığı izlenimini vermek ve onları izlemeyi zorlaştırmak için röle bilgisayarları gibi iz gizleme teknikleri kullanırlar [18] . Yukarıdaki örnekte olduğu gibi, yetkililerin (bu durumda ABD'nin) bilgisayar korsanlarını başarılı bir şekilde izlemesi, yakalaması ve kovuşturması yıllar sürmesi normaldir. İstihbarat işindeki operasyonun doğası gereği, bu profil en gizli ve bilgi edinilmesi en zor olanıdır. Aynı zamanda, soğuk savaş sonrası istihbarat üzerine bir CNN analiz raporundan toplanan gerçeklere göre gelişmesi için nedeni ve yeri olan bir profil. Rapor, potansiyel acemilerin alışkanlıklarını takip etmeyi, köstebekleri işe almayı, bir dağıtım kanalını güvenceye almayı ve onların izini takip etmeyi zorlaştırarak internetin yabancı istihbarat topluluklarına nasıl katkıda bulunduğunu açıklıyor. Gelişmiş ülkelerdeki sivil özgürlükler, çok önemli olmasına rağmen, karşı istihbarat yapmayı zorlaştırmaktadır [23] .

Genel olarak bilgisayar korsanlığı farklı biçim ve şekillerde gelir. Merak, meydan okuma sevgisi, ego, ekonomik faktörler ve ulusal çıkar faktörleri gibi farklı faktörler arasında değişir. Farklılıklarına rağmen, farklı hacker grupları arasında, açık bir şekilde işbirliği yapma niyeti olmasa bile, bazı gayri resmi işbirliği var gibi görünüyor. Bu, çevrimiçi

forumlar ve güvenlik açıklarını ayrıntılandıran ve istismarları gösteren web siteleri aracılığıyla hacker yeraltı dünyasında bilgi paylaşımı yoluyla gerçekleşir. Farklı işbirliği yolları, 2600 gibi hacker dergileri ve bu bölümün kapsamı dışında kalan hacker konferanslarıdır. Diğer bir topluluk, ekonomik kaybın ve bu tür yıkıcı faaliyetleri ortadan kaldırma ihtiyacının ötesine geçen toplum üzerindeki etkidir.

Bunu yapmak zordur, çünkü siber suç çok çeşitli aktörleri ve yöntemleri kapsar. Fiziksel olmayan, soyut, kalıcı olmayan doğası, hukuk, politika ve uygulama için kafa karıştırıcı sorular ve sorunlar doğurur. Ancak bunlardan önce siber suçluların yakalanması gerekiyor ve burada da siber suçun dijital doğası, oyunun oynanma şeklini değiştiriyor. Adli Bilişim bölümleri, siber suçluları belirleme tekniklerinden bazılarını gösterir ve yasalar bölümü, böyle tehlikeli ve maliyetli bir faaliyete karşı koymak için toplum tarafından türetilen yasaları tartışır.

III. Siber-Adli Bilişim ve Hukuki Prosedürler

Bilgisayarların ve diğer elektronik cihazların her yerde ve her yerde kullanımı, hızla yükselen yeni ve depolanmış dijital bilgi dalgası yaratıyor. Kurumsal bilgilerin yaklaşık %90'ı şu anda dijital biçimde bulunmaktadır [1] . Şirketler yılda yaklaşık 17,5 trilyon elektronik belge üretiyor. Bu patlayıcı büyümede elektronik belgelerden daha fazlası da var . Elektronik verinin ek biçimleri şunlardan kaynaklanır:

- İnternet tabanlı elektronik ticaret, çevrimiçi bankacılık ve hisse senedi ticareti
- Telefon posta mesajlarının ve elektronik günlüklerin kurumsal kullanımı ve saklanması

- Yılda yaklaşık 40 milyon cihaz satan avuç içi pilotu ve cep bilgisayarı gibi kişisel düzenleyiciler.
- Dijital kameralar
- Grafik görüntülerin, ses ve videonun kurumsal kullanımı ve depolanması.

Bu verilerle ilişkili bilgi riskleri çoktur. Şirketler için dijital bilginin serbest akışı, arka kapının potansiyel olarak her zaman kayba açık olduğu anlamına gelir. Daha önce gördüğümüz gibi, dava riskini ve gizli kurumsal verilerin kaybolmasını artıran birkaç faktör var ve bununla birlikte siber adli tıbbın önemi arttı.

Bu bilgi çağında fiziksel suçlar bir şekilde teknoloji ile de ilişkilidir. Özellikle finans ve ticaretle ilgili olan bazı geleneksel suçlar teknolojik olarak geliştirilmeye devam etmektedir. Verilerin çalınması ve manipülasyonu ile ilgili suçlar günlük olarak tespit edilir. Bir kamyon bombası yerine internetten ciddi ve maliyetli bir terör eylemi gelebilir. Bir seri katilin günlüğü, bir kağıt veya defter yerine bir diskete veya sabit diske kaydedilebilir. Gördüğümüz gibi, suç faaliyeti, bir dereceye kadar, delillerin ve soruşturmaların somut terimlerle tanımlandığı fiziksel bir boyuttan, delillerin yalnızca elektronik ortamda bulunduğu ve soruşturmaların çevrimiçi olarak yürütüldüğü siber bir boyuta dönüşmüştür.

Ağ bilgisayarları arasındaki karşılıklı bağlantıya sürekli artan güvenin yarattığı artan suç fırsatlarının ışığında, deneyimli ve sofistike bilgisayar suçlularının kolluk kuvvetleri için önemli bir meydan okuma oluşturduğuna şüphe yoktur. Bu tür suçluları yakalamanın zorluğunda da buna paralel bir artış olmuştur. Bunun böyle olmasının birkaç nedeni var. Bilgisayar iletişiminin sağladığı anonimlik, uzun zamandır bilgisayar suçlusu olabilecek kişilerin başlıca ilgi alanlarından biri olarak kabul edilmiştir. Bu zorluk, elektronik postayı yeniden paketleyen ve böylece onu izleme yeteneğini azaltan "anonimleştiriciler" olarak

adlandırılan hizmetlerin kullanımı ve mevcudiyeti ile daha da artmıştır. Ayrıca, Birleşik Devletler dışında yerleşik sunucuları olan ağlar da dahil olmak üzere, oluşturulmuş ağdan başka bir oluşturulmuş ağa atlama pratiği, iletişimi ilk özneye kadar izlemeyi çok zorlaştırabilir. Bu bölümde daha sonra göreceğimiz gibi, adli bilimin kullanışlı olduğu yer burasıdır.

Adli bilişim, siber adli bilişim veya adli bilişimin yalnızca bilgisayarlarla ilgili olmadığını anlamak da hayati önem taşımaktadır. Delil kuralları, yasal süreçler ve kanıtın bütünlüğü ve sürekliliği, olgusal bilgilerin bir mahkemeye açık ve özlü bir şekilde bildirilmesi ve bu kanıtların kaynağına ilişkin bilirkişi görüşünün sağlanması ile ilgilidir [1].

Adli soruşturmanın amaçları

Siber adli tıpta, bir soruşturmaya neden ihtiyaç duyulduğunun nedenlerini ve bu soruşturmanın planını gözden geçirmek önemlidir. Bir soruşturma yürütmenin etkisinin ve fizibilitesinin belirlenmesi önemlidir. Bazı durumlarda, araştırmaların maliyeti yararlarından fazlaysa, soruşturmayı yürütmek için hiçbir neden olmayabilir.

Bir soruşturmayı tetikleyebilecek birçok şey (özellikle kurumsal bir ortamda) vardır ve bunlardan bazıları [1] :

- İnternet kullanımı normu aşıyor
- E-postayı uygunsuz şekilde kullanmak
- İşle ilgili olmayan bir şekilde internet, e-posta veya PC kullanımı
- bilgi hırsızlığı
- Güvenlik politikalarının veya prosedürlerinin ihlali

- Fikri mülkiyet ihlalleri
- Sahtekarlık gibi elektronik kurcalama, birini veya bir şeyi taklit etme, biri gibi maskeleme veya maskeleme.
- Ağa bağlı bilgisayarların tehlikeye girmesine neden olabilecek Ağ Saldırısı.

Bir soruşturmanın başlaması için, belirli bir şikayet için bir gerekçe veya araştırmak için bir neden olmalıdır ve bu, kurallara veya şikayetin sunulduğu, daimi bir şirket politikasını veya prosedürünü ihlal etmek gibi bir temel çizgiye dayanmalıdır. Ayrıca yasal tüzükleri, zorunlu tüzükleri veya düzenleyici tüzükleri ihlal ediyor olabilir. Soruşturmacı, temel çizgi(ler)in nasıl uygulanacağını ve bu tür ihlaller için belgelenmiş herhangi bir ceza olup olmadığını belirlemek için uygun olduğu şekilde ve araştırmanın bir parçası olarak bu temel ilkelere ve kurallara başvurmalıdır. Bu ihlallerden herhangi biri için, siber adli tıpta bir soruşturma planının resmileştirilmesine yardımcı olan bilinen bir dizi soru vardır. Sorular nedene göre farklılık gösterir ve suçun ciddiyeti de değişir.

Bir soruşturmanın gerekçeleri ve temel durum belirlendikten sonra, olayın etkisi de belirlenmelidir. Etkiyi anlayarak, soruşturmaya devam etmenin mümkün olup olmadığı belirlenir. Etkilerinden bağımsız olarak (finansal veya başka türlü) bazı olayların araştırılması gerekir. Siber Adli Bilişim uzmanlarının etkiyi belirlerken akıllarında bulundurdukları bazı öğeler şunlardır [1] :

- Böyle bir soruşturmayı sürdürmenin faydaları
- Soruşturma yürütmeme sorumluluğu
- Takip etme veya takip etmeme yükümlülükleri (kamuya, ortaklara ve diğer sözleşmelere karşı iyi niyet) • Mevcut kaynaklar (zaman, insanlar, finans, araçlar, vb.)

Ayrıca, bir şirkette soruşturma yürütme konusunda en fazla deneyime sahip bölümün iç denetim bölümü olduğu da unutulmamalıdır, ancak çoğu durumda Ağ Operasyonları, İnsan Kaynakları veya Hukuk gibi diğer departmanlar yardım için çağrılabilir ve bazı durumlarda durumlarda, uzmanlığa ihtiyaç duyan alanlarda harici danışmanlar yer alabilir. Bu tür soruşturmalar sırasında, herhangi bir adli kanıtın tutarlılığını ve bütünlüğünü korurken, soruşturmanın faaliyetlerini uygun şekilde yönetmek önemli bir görevdir.

Adli bilgisayar bilimi, bilgiyi çıkarır ve üretir. Bilgisayar incelemesinin amacı, vakayla ilgili bilgileri bulmaktır. Bu tür sonuçları desteklemek için, yalnızca incelenen ortamdaki bilgilerin değiştirilmeden var olmasını sağlayacak prosedürlere ihtiyaç vardır. Adli bilişim neredeyse tamamen teknoloji ve pazar odaklıdır, genellikle laboratuvar ortamlarının dışındadır ve incelemeler hemen hemen her durumda benzersiz farklılıklar gösterir.

Adımlar ve Prosedürler

Bir soruşturma sırasında, Adli Bilişim araştırmacıları, kovuşturma için kanıt toplama hedefine odaklanmalıdır. Federal kanıt kurallarının yanı sıra kanıtların kabul edilebilirliğine ilişkin yerel ve eyalet yasalarına ve gerekli olması halinde "uzman tanık" ifadesi sağlamak için gerekenler hakkında bilgi sahibi olmalıdırlar. Müfettişler genellikle ekipmanların izolasyonu, dosyaların izolasyonu, ziyaret edilen web sitelerinin takibi, oturum açma sürelerinin ve zamanlarının takibi ve yasadışı yazılım kurulum ve kullanımının takibi üzerinde çalışırlar. Daha sonra bulunan tüm kanıtları ilişkilendirmeye çalışırlar. Bu süreç aşağıda tartışılmaktadır [1] .

Ekipmanın izolasyonu - Müfettişler, ekipmana erişmek için yönetimden onay alır. Bilgisayara veya cihaza sahip olduklarında, ne kendilerinin ne de başka birinin ekipmanla yalnız bırakılmadığından emin olarak kanıt zincirini korumaları gerekir. Bu tür ekipmanların nerede olduğu ve bu tür ekipmanlar üzerinde gerçekleştirilen eylemler hakkında günlükler tutulur. Ayrıca inceleme altındaki tüm verilerin yedeklenmesi ve yedeklemeyi gerçekleştirmek için kullanılan programların bağımsız ve bütünlük içinde olması önemlidir. Böyle bir yedekleme için iyi bir program , tam bölüm yedeklemeleri yapmaya yardımcı olan bir bit akışı yedeklemesi gerçekleştiren SafeBack [1] 'dir.

Dosyaların izolasyonu - Şüphelilerin herhangi bir dosyaya müdahale etmesini önlemek için, müfettişlerin kullanıcı kimliklerini devre dışı bırakmaları ve silmemeleri gerekir. Kimlikler devre dışı bırakıldığında, erişimleri olan tüm dosyalar bir yedekleme ortamına kopyalanmalıdır.

Ziyaret edilen web sitelerinin takibi - Bu, izole edilmiş ekipmandaki aşağıdaki öğelerin gözden geçirilmesiyle (veya diğer bir deyişle, izole edilmiş ekipmandaki verilerin yedeklenmesiyle) gerçekleşir:

- Çerezler, araştırmacıyı/araştırmacıları kullanıcının ziyaret ettiği web sitelerine götüren çerezlerdir.
- Favori URL'lerin çoğunun depolandığı yer imleri
- Geçmiş Tamponu - bunlar, bireylerin web sitelerine hangi zamanlamayla eriştiği hakkında daha fazla bilgiye sahiptir ve onaylanmamış veya yetkisiz web siteleri hakkında fikir verebilir.

- Araştırmacıların önbelleğe kaydedilen son talimat veya veri setini alabileceği önbellek. Bu, özel programlar gerektirir, çünkü çoğu durumda yanıltıcı olma eğilimindedir.
- Geçici İnternet dosyaları - Bu, sitenin adresini, en son ne zaman değiştirildiğini, en son erişildiğini ve en son kontrol edildiğini içermesi bakımından diğer öğelere göre avantajlıdır ve çok fazla internet erişimi veya uygunsuz durumlarda çok yardımcı olur. internet girişi.

Yasadışı yazılım yükleme ve kullanımının izlenmesi - Bu, şu anda bilgisayarda veya cihazda bulunan (kayıt defterini veya diskteki dosyaları inceleyerek keşfedilen) programların listesi ile aşağıdaki herhangi bir bilgisayarda olabileceklerin listesi arasında bir karşılaştırmadır. şirket politikası. Bu teknikler genellikle Sistem İnceleme olarak bilinir. Bu durumda denetçi, eğer varsa, gizli dosyaları keşfetmeye de özen göstermelidir.

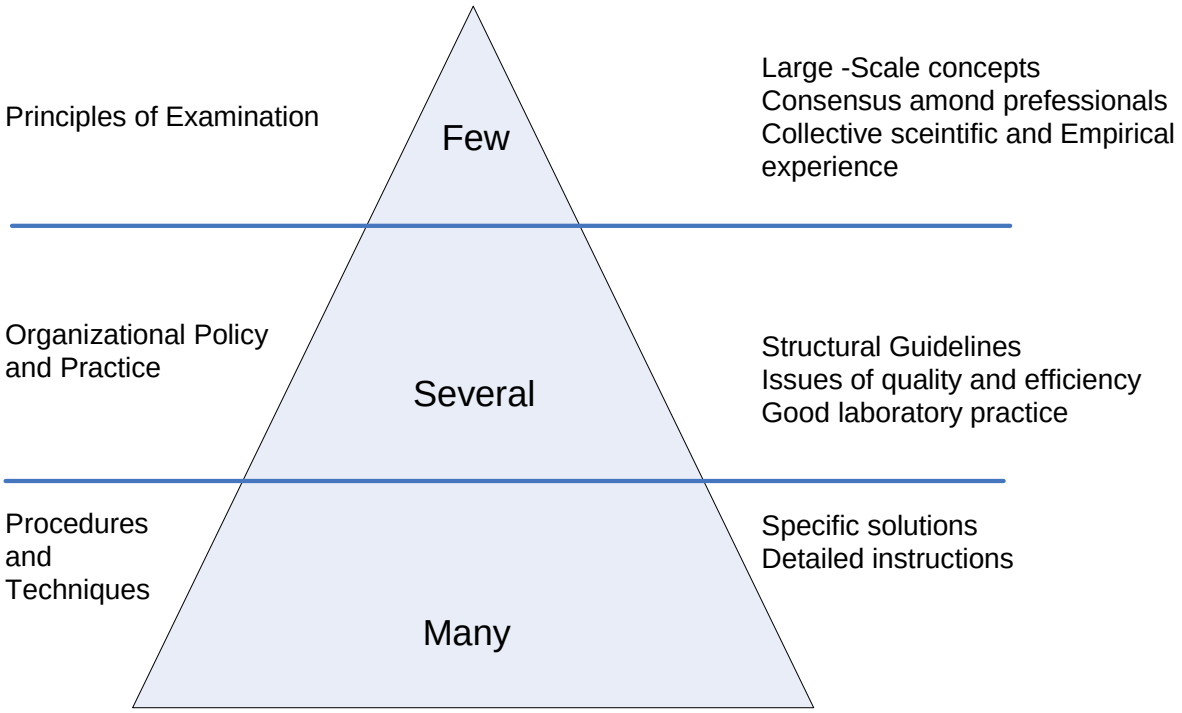
Ağa izinsiz giriş için izinsiz giriş profili oluşturma - Ağa izinsiz giriş için yukarıdakilerden biraz farklıdır. Hacker şirket dışından olabilir. Birkaç bükülme ile suç profili oluşturma kavramı, bilgisayar / ağ izinsiz girişlerinin profilini çıkarmak için de uygulanabilir. Profil oluşturma süreci, izinsiz girişi bağlam içinde görmeyi, faaliyetleri iş fonksiyonlarına yönelik tehditle ilişkilendirmeyi ve olasılık, deneyim ve ipuçlarına dayalı eğitimli tahminler yapmayı içerir. Profil, davetsiz misafirin izlenmesine, gelecekteki hedeflerin, saldırının imzalarının ve geçmişteki olası izinsiz giriş konumlarının belirlenmesine ve bilgisayar korsanının risk veya tehdidinin değerlendirilmesine yardımcı olabilir. Profil oluşturma, bilgisayar korsanının olası nedenlerini, teknik yeteneklerini ve coğrafi konumlarını da ortaya çıkarabilir.

İyi bir profil oluşturmak için müfettişlerin izinsiz giriş zamanı, saldırının kaynağı, sızılan sistemlerin listesi, sızma yöntemi ve tüm yazılan/okunan ve oluşturulan dosyalar dahil olmak üzere erişilen tüm dosyaların listesi hakkında bilgi toplaması gerekir. Bu tür bilgilerin düzenlenmesi ve derlenmesi, bilgileri bir araya getirecek ve davetsiz misafirin kim olabileceğine dair düzenli bir resim oluşturacak uygun profilin oluşturulmasına yardımcı olur.

Kanıtları ilişkilendirme - Listelenen çeşitli prosedürlerden görüldüğü gibi bilgisayar kanıtı neredeyse hiçbir zaman tek başına mevcut değildir. Depolanan verilerin, onu oluşturmak ve depolamak için kullanılan uygulamanın ve bu faaliyetleri yöneten bilgisayar sisteminin bir ürünüdür. Daha az ölçüde, laboratuvarda onu çıkarmak için kullanılan yazılım araçlarının da ürünüdür.

Dosya kanıtlarını ve verileri yakaladıktan sonra, incelemeyi yapan kişi bir erişim modelinin grafiğini çıkarabilir veya yasa dışı yazılımı veya ne zaman yüklendiğini listeleyebilir. Ardından, soruşturma altındaki şüphelinin söz konusu ekipmanı kullanarak yetkisiz eylemlerde bulunma fırsatına sahip olduğundan emin olmak için erişim ve indirme tarihlerini ve saatlerini zaman çizelgelerine, gözetim ve diğer tanık hesaplarına göre kontrol etmeleri gerekir. Müfettişler bu tür kanıtları incelerken yalnızca gerçekleri göstermeli, başka bir şey göstermemelidir. A noktasını B noktasına bağlamak için mantıklarında herhangi bir sıçrama yapamazlar, çünkü bu sadece yeterli kanıttan yoksun olduklarını gösterir. Ayrıca, inceleme altındaki kişinin suçu, yasa dışı eylemi veya yetkisiz eylemi nasıl gerçekleştirdiğini yeterince açıklayabilmeli ve bunun nasıl yapıldığına dair kanıt ve kanıt sunabilmelidir.

Aşağıdaki şekil (1) 'de [1] , adli bilişim kanıtları için yönergeler gösterilmektedir:



Şekil, aşağıdakilerden oluşan üç seviyeli bir hiyerarşik modele işaret etmektedir:

- Kapsamlı bir sınav ilkeleri kavramı.
- Politikalar ve uygulamalar
- Prosedürler ve teknikler

Sınav ilkeleri, her zaman sınav için geçerli olan büyük ölçekli kavramlardır. Adli bilgisayar denetçilerinin toplu teknik uygulamalarını ve deneyimlerini temsil ederler. Bunun bir laboratuvardaki örnekleri, incelemelerin orijinal kanıtın kopyaları üzerinde yapılmasını gerektirebilir. Örgütsel Politika ve Uygulamalar, sınav için geçerli olan yapısal yönergelerdir. Bir örnek, gerekli kopyayı oluşturmak ve bunun doğru ve doğru olduğundan emin olmak olabilir. Prosedür ve teknikler , verilen probleme özel yazılım ve donanım çözümleridir. Örnekler, Döngüsel Artıklık Kontrolü ve Mesaj Özeti, hem orijinal veriler hem

de kopya için hesaplanabilen ve daha sonra genellikle kimlik için karşılaştırılabilen verilerin benzersiz matematiksel temsillerini üreten bilgisayar algoritmalarıdır.

Siber Adli Bilişim için araçlar

Siber Adli Bilişim araçları üç farklı kategoriye ayrılabilir: tespit araçları, koruma araçları ve analiz araçları [1] .

Tespit araçları - Bunlar riskleri belirlemek için kullanılır. Ağ tabanlı araçlarla başlarlar, en yaygın olarak kullanılanlardan biri **Nmap olarak bilinir** . Bu aracın imza özelliklerinden biri, TCP/IP parmak izi yoluyla işletim sistemi algılamasıdır. Ayrıca dinamik ttl sürelerini, paralel tarama ve ping göndermeyi, esnek hedef ve bağlantı noktası özelliklerini, sahte taramayı ve günlükleri metne veya makine tarafından okunabilir biçimlere çıkarmayı destekler. Başka bir araç, belirli bir ana bilgisayarı belirli açıklar için tarayan ana bilgisayar tabanlı bir araç olan Nessus'tur **.** Mükemmel bir GUI ön ucuna sahip bir güvenlik açığı tarayıcısıdır.

Retina başka bir mükemmel tarayıcıdır.

Gerçek araştırma senaryolarında birden fazla aracın bir kombinasyonu kullanılır. Örneğin, bir web sunucusunu güvenlik açığı açısından denetlemek için önce Nmap, ardından Nessus çalıştırılabilir ve ardından göz taraması yapılabilir. Yukarıdaki araçlar çok güçlüdür ve aslında farklı sistemlerde birçok güvenlik açığının ortaya çıkmasına yardımcı olur.

Koruma araçları - Koruma araçları, algılama araçlarının tanımladığı riski azaltır. İlk risk formülünde açıklanan ağ veya ana bilgisayar tabanlı karşı önlemleri artırarak bu riski azaltırlar. Trafiği doğru konuma ileten cihazlar olan yönlendiriciler, tipik olarak bir ağ

için ilk savunma hattını oluşturur. Güvenlik duvarları, güvenli bir ağda ikinci savunma katmanını oluşturur ve ağ için bir nöbetçi olarak hareket ederek ve yalnızca özel olarak izin verilen trafiğe izin vererek riski azaltır. İzinsiz giriş tespit sistemleri (IDS'ler), imzalara dayalı olarak kötü niyetli trafiği tanımlayarak bir ağ için hırsız alarmı işlevi görür. Snort, bu tür IDS sistemlerine iyi bir örnektir. Artan farkındalık ve bilgi yoluyla riski azaltırlar. Proxy'ler, izin verilen verilerin kötü amaçlı olmadığını doğrulayarak bir tür sigorta poliçesi görevi görür. Koruma araçları hem ana bilgisayarda hem de ağda uygulanabilir. Ağ tabanlı araçlar daha pahalı, daha karmaşık olma eğilimindedir ve uygulanması daha uzun sürer. Ancak ağın güvenliği için hayati önem taşırlar.

Analiz araçları - Bu araçlar riski ölçmek için kullanılır. Bir olayın ne yaptığını, nasıl yapıldığını ve sonuçlarının ne olduğunu ölçerler. Analiz araçlarına örnek olarak NIX altında çalışan Coroners araç takımı ve Windows altında çalışan EnCase dahildir.

Bu araç takımlarını kullanmak için çok güçlü bir teknik yeteneğin önemi fazla vurgulanamaz. Siber adli tıpla uğraşırken bazı gereksinimlerin karşılanması gerekir. Bunlar, eylemlerin teknik sonuçları hakkında bilgi yoluyla teknik bir farkındalık, verilerin nasıl değiştirilebileceğine dair bir anlayış, akıllılık, açık fikirlilik, dolambaçlılık, yüksek bir etik standardı, sürekli eğitim ve gereksiz veri kaynaklarının kullanımını içerir. Yukarıdaki gereksinimlerin tam olarak anlaşılmaması veya karşılanmaması durumunda sistem, adli açıdan ilk başta tehlikeye atıldığından çok daha kötü durumda kalabilir. Bir cinayet mahallini araştıran bir trafik polisi gibidir (ve resmi alırsınız).

"EcCase" araçlarından birine bir örnek verirdim. Tanıdık bir Windows Gezgini stili görünümü sağlar. Görünüm, silinen dosyaları içeren boş alan da dahil olmak üzere dosyaları hiçbir şekilde değiştirmeden görüntüler. Önizleme bölmesi, birçok dosya

arasında sıralama yaparken de çok yararlıdır. Müfettişlerin ilerledikçe bir vaka oluşturmalarına yardımcı olan güçlü bir Rapor görünümüne sahiptir. Ayrıca işaretle ve tıkla dosya karma işlemine izin verir; dosyaları daha sonra doğrulamak için paha biçilmez bir araç.

Siber Adli Bilişim bugün nerede duruyor?

Siber Adli Bilişim analizi ve soruşturmalarına dahil olan farklı yönleri inceledikten sonra, bu aşamada konunun dışına çıkmak ve siber adli tıpın kullanıldığı gerçek yaşam örneklerine ve yukarıda bahsedilen teknik ve prosedürlerin bazılarının neden kanıtlandığına bakmak faydalı olabilir. bazı suçluları mahkum etmede güvenilir ve uygulanabilir olması.

Aşağıdaki bağlantılarda atıfta bulunulan makalelerden [2] :

- http://www.krollontrack.com/publications/rosenthal.pdf
- http://www.krollontrack.com/publications/kish.pdf
- http://www.boston.com/business/articles/2005/05/11/gillette_workers_may_have_deleted

  _e_mail/

Verilerin, kullanıcıların beklediğinin ötesinde olduğunun farkına varırdık. Örneğin bir dosyayı silmek, mevcut işletim sistemlerinin çoğunda gerçekten silindiği anlamına gelmez. Bu sadece, o dosyaya yapılan referansın, onu kullanıcı için görünmez kılacak şekilde karıştırıldığı anlamına gelir. Bir uzman, belirli bir süre içinde bu dosyayı kolayca alabilir. Bir e-postanın silinmesi, silindiği anlamına gelmez. E-posta sunucularında veriler her gün (ve bazı durumlarda birkaç saatte bir) yedeklenir ve sistemde feci bir arıza olması durumunda bilgileri kurtarmak için birkaç ay boyunca korunur ve bu, uygun izinle

araştırmacıların aşağıdakileri alabileceği anlamına gelir. bu yedekleme ortamına erişebilir ve uygun e-postaları alabilir. Ayrıca web sitelerinde, son kullanıcılar için tarayıcı tarafından etkinlikleri için kaç tane referans tutulduğunun kolay olduğu ortaya çıkıyor. Siber suçlara karışan kişiler ile izlerini ne kadar iyi gizleyebilecekleri arasında da bir ayrım yapmalıyız. Kanımızca siber-adli tıp, http://www.krollontrack.com/publications/SPPP.pdf ve http://www.krollontrack.com adresinde bulunan diğer bağlantılarda bulunan bilgilerle tanık olunan delillerin bulunmasında ve suçluların mahkum edilmesinde faydalı olmuştur. /yasal kaynaklar .

Ancak diğer yandan, siber-adli tıbbı engelleyebilecek engellerin bir kısmı bu tür soruşturmalarda ortaya çıkan masraflar olacaktır. Bazen bu tür harcamaların, birini mahkum ederek elde edilen faydalardan daha ağır olduğu algılanır. Gelecekte bu alanda daha fazla uzmana sahip olunarak ve daha fazla otomatikleştirilmiş araca sahip olunarak bunun üstesinden gelinebilir. Diğer engeller, bazı gizlilik yasalarının ihlali olabilir, ancak bu, mevcut yasaların bazılarında bazı güncellemeler yapılarak da çözülebilir ve bu, gelecekte daha büyük bir kitle siber-adli tıbbın faydalarını fark etmeye başladığında potansiyel olarak gerçekleşebilir.

IV. Mevcut Kanun ve Politika

Siber suçluları yakalayacak teknolojinin mevcut olması ve başarıyla uygulanması şartıyla, hukuk sistemimiz kovuşturmaya hazır mı? Çeşitli siber suçlar hangi yasaların yargı

yetkisine giriyor? Politikanın neredeyse her zaman teknolojinin yıllarca gerisinde kaldığını bilerek, şu anda durum nedir ve yetişmek için ne tür adımlar atılmalıdır?

Siber faaliyetin dijital doğası, geleneksel yargı yetkilerini geçersiz kılıyor. Coğrafi sınırlar internette hiçbir şey ifade etmez ve neredeyse tüm siber suçlar eyalet sınırlarında gerçekleşir. Bu, Kaliforniya'nınki gibi eyalet ceza kanunlarının siber suçla ilgili bölümleri olmasına rağmen, çoğu vakanın özellikle Bilgisayar Dolandırıcılığı ve Kötüye Kullanımı Yasası (18 USC § 1030'da kodlanmış) kapsamında federal yargı yetkisine girdiği anlamına gelir. [26] 1986'da Kongre tarafından kabul edilen, genellikle Başlık 18 olarak anılan Kanun, siber hukukun temel kaynak noktasıdır ve yeni mevzuatın üzerine inşa edildiği temel olarak çalışır.

Yeni teknolojiler, yetenekler ve eğilimler ortaya çıktıkça, yasada ince ayar yapılmalıdır. Yeni teknolojilerden etkilenebilecek her tüzüğü değiştirmek için Birleşik Devletler Yasasının tamamını taramak yerine, yasa koyucular Başlık 18'de dikkatli, önemli değişikliklere odaklanmalı ve özellikle yeni sorunları ele almalıdır. Örneğin , ilk ortaya çıkışında yasa, şimdi bildiğimiz gibi siber suçluların büyük bir yüzdesini oluşturan çocuklar için bile geçerli değildi. [10] Başlık 18, 1996 yılında Ulusal Bilgi Altyapısını Koruma Yasası ile en önemli şekilde değiştirilmiştir ve şu anda olduğu gibi, "sistemlerin ve bilgilerin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin" korunmasını hedeflemektedir. [27] Adalet Bakanlığı'ndan temel bir kılavuz aşağıdadır:

	izinsiz girenler	**Yetkili Kullanıcılar**
Kasıtlı Hasar	*Suç*	*Suç*

Pervasız Hasar	*Suç*	*suç yok*
İhmal Edilen Hasar	*kabahat*	*suç yok*

18 USC § 1030(a)(5)

Görüldüğü gibi, kanun hem sanığın bilgisayara erişim yetkisine hem de zarar verme niyetine dayanmaktadır. Bu, örneğin, bir çalışanın ofis bilgisayarının sabit diskinden aptalca bir şekilde dosyaları silerse (yetkili bir kullanıcı tarafından ihmal edilen hasar), bir çalışanı ve yetkili kullanıcısı *olmadığında* olacağı gibi, kanunen cezalandırılmayacağı anlamına gelir . makine. İkinci bir örnek olarak, çalışanın genç kızı bir şaka olarak ofis bilgisayarına girerse ve *yanlışlıkla* dosyaları silerse, kadın bir kabahat işlemiş olur (bir izinsiz giriş yapan kişinin ihmal sonucu verdiği zarar).

Bununla birlikte, siber suçların önlenmesinde ceza kanunundan daha fazlası vardır. Çeşitli kurumlar ve diğer politika kuruluşları, son yirmi yılda siber hukuku tasarlama ve uygulama mücadelesine farklı şekillerde katılmıştır. 2002 yılında, yeni İç Güvenlik Departmanı, Kritik Altyapı Güvence Ofisi, Ulusal Altyapı Koruma Merkezi, Federal Bilgisayar Olayı Müdahale Merkezi ve Ulusal İletişim Sisteminden Ulusal Siber Güvenlik Birimi'ni (NCSD) konsolide etme ihtiyacını fark etti ve oluşturdu. NCSD, Robert Liscouski'nin gözetiminde 2003 yılının Haziran ayında açıldı ve DHS'ye göre "siber tehditleri ve güvenlik açıklarını belirlemek, analiz etmek ve azaltmak; tehdit uyarı bilgilerini yaymak; olay yanıtını koordine etmek; ve operasyonların sürekliliği ve kurtarma planlamasında teknik yardım sağlamak." [28]

Kolluk kuvvetleri için ön saflar "CHIP" birimleri veya Bilgisayar Hackleme ve Fikri Mülkiyet birimleri tarafından tutulur. Bu tür uzmanlık birimlerinin etkinliği her zaman söz konusu olsa da, Adalet Bakanlığı, mevcut tüm CHIP birimlerinin ilk yılı olan 2003 yılında, bu birimlere sahip ofislerin "dört mali yılda ortalamadan yüzde 46 daha fazla sanık aleyhine dava açtığını" iddia ediyor. birimlerin oluşumundan yıllar önce." [29]

Tabii ki mevcut yasalar ve politika mükemmel olmaktan uzak. Şüpheli olsa da, özellikle yeni teknolojiler ortaya çıktıkça, yasal boşluklar olasılığı hala mevcuttur. Politika her *zaman* yavaştır, çünkü teknoloji, Kongre'nin onu yönetmek için yasaları geçirmesinden daha hızlı gelişir. Bu nedenle, genellemelere varmak ve saçma sapan boşlukları önlemek için mevzuat dikkatli bir şekilde oluşturulmalıdır.

Ayrıca, yasa ve politika tamamen güncel olsa bile, yasanın uygulanması, politikanın uygulanması ve siber suçluların başarılı bir şekilde kovuşturulması konusundaki fiili uygulama çok zordur. Siber suç oranlarına ilişkin henüz kesin ve kesin veriler bulunmamakla birlikte , diğer suç türlerinde olduğu gibi bu alanda da yaptırım kapasitelerinin kaçınılmaz olarak suç kapasitelerinin gerisinde kaldığını büyük bir güvenle söyleyebiliriz.

Bu, siber suçluların her zaman suçlarından kurtuldukları anlamına gelmez. Federal mahkemeler artık siber suç davalarını kovuşturuyor ve bu tür kovuşturmalar şu anda giderek daha yaygın hale geliyor. Örneğin, 80 milyon dolarlık zarara neden olan Melissa virüsünün faili David Smith, 2002'de mahkûm edilmiş ve yirmi ay federal hapis cezasına ve ardından üç yıl denetimli salıvermeye mahkum edilmiş ve 5.000 dolar para cezasına çarptırılmıştır. [30] *ABD v. Jeansonne davasında* Louisiana'lı David Jeansonne altı ay hapis

cezasına çarptırıldı ve 9-1-1 aramalarına müdahale ederek saldırıyı Adalet Bakanlığı'nın dediği gibi bir Truva atı için Microsoft'a 27.000 $'dan fazla ödemek zorunda kaldı. "kamu sağlığı ve güvenliğine tehdit" [31] Yine de gidilecek çok yol var. İlk botnet kovuşturması, *US v. Ancheta* , ancak şimdi, yani 2005 yılının Kasım ayında gerçekleşiyor. [25]

Elbette, yetkin siber Adli Bilişim yöntemleri olmadan, herhangi bir kovuşturma tartışmasının esasen tartışmalı bir nokta olduğunu hatırlamak önemlidir. Yani kolluk kuvvetlerinin *yakalayamadığını* mahkeme mahkûm edemez . Adli Bilişim sorusu aynı zamanda maliyet etkinliği ve teşviklerle ilgili soruları da beraberinde getiriyor. Siber suçluları yakalamanın maliyeti yüksek mi, yoksa bunu yapmak için yeterli teşvikler var mı? Mevcut siber Adli Bilişim yöntemleri, suçluları caydırmak için yeterince etkili mi?

Siber hukuk ve siber güvenlik politikasının geleceği henüz görülmedi, ancak bazı unsurlar tahmin edilebilir. Birincisi, CHIP birimleri gibi daha uzmanlaşmış kolluk kuvvetleri bekleyebiliriz (veya en azından umut edebiliriz). Bomba ekiplerinin patlayıcı uzmanları çalıştırması gibi, siber suç birimlerinin de beyaz şapkalı bilgisayar korsanlarından ve bilgisayar bilimi uzmanlarından oluşması gerekecek. Ayrıca, kolluk kuvvetleri ve endüstri arasında daha fazla koordinasyona ihtiyaç vardır. Son Sony skandalı, suç taktikleri uygulayan bir teknoloji endüstrisi devinin sadece bir örneğidir. Sektörün ayrıca gri şapka korsanlığı açısından nelere izin verilmesi gerektiğiyle ilgili soruları tartışmak için masada olması gerekiyor. Politika dünyası, yalnızca endüstri ve akademik çevrelerin işbirliğiyle siber suçluları yakalamayı umabilir.

V. Siber Suçun Etkileri ve Gelecek Eğilimler

Rhodes Üniversitesi'nde dijital adli hukuk alanında uzman bir hukuk araştırmacısı olan Lunda Wright, Ekim 2005'te yayınlanan bir blogda ilginç bir araştırma bulgusuna sahiptir. Siber suçluların kovuşturma oranlarının arttığını belirtiyor. Film ve müzik çalışmalarıyla ilgili siber korsanlığa karşı artan bir baskı var. Dava için yeni davalar ve stratejiler var. Şirketlerde ve devlette adli bilişim uzmanlarının becerilerine daha fazla bağımlılık vardır. Son olarak, hükümetler arası işbirliği çabalarında bir artış var.

Organize suç grupları, büyük dolandırıcılık ve hırsızlık faaliyetleri için interneti kullanıyor. Beyaz yakalı suçlarda organize suça karıştığını gösteren eğilimler var. Suçlular geleneksel yöntemlerden uzaklaştıkça internet tabanlı suçlar daha yaygın hale geliyor. İnternet tabanlı hisse senedi dolandırıcılığı, suçlulara her yıl milyonlarca dolar kazandırarak yatırımcıların zarar görmesine neden oldu ve bu da onu bu tür suçlar için kazançlı bir alan haline getirdi.

Ülke çapındaki polis departmanları, son yıllarda rapor edilen bu tür suçlardan artan sayıda aldıklarını doğrulamaktadır. Bu, artan bilgisayar kullanımı, çevrimiçi ticaret ve geeky sofistike suçlulardan kaynaklanan ulusal eğilim ile uyumludur. 2004 yılında, siber suçlar uyuşturucu kaçakçılığından daha yüksek bir geri ödeme sağladı ve gelişmekte olan ülkelerde teknolojinin kullanımı genişledikçe daha da büyüyecek.

ABD İç Güvenlik Bakanlığı tarafından desteklenen bir kurum olan ABD Siber Sonuçlar Birimi'nin yöneticisi Scott Borg, kısa süre önce hizmet reddi saldırılarının geleceğin yeni dalgası olmayacağını belirtti. Solucanlar, virüsler, gelecekteki saldırı potansiyeline kıyasla 'oldukça olgunlaşmamış' olarak kabul edilir.

Potansiyel Ekonomik Etki

Günümüz tüketicisi bilgisayarlara, ağlara ve bunların depolamak ve korumak için kullanılan bilgilere giderek daha fazla bağımlı hale geldiğinden, siber suçlara maruz kalma riski yüksektir. Geçmişte yapılan anketlerden bazıları, ankete katılan şirketlerin %80'inin bilgisayar ihlallerinden kaynaklanan mali kayıpları kabul ettiğini göstermiştir. Etkilenen yaklaşık sayı 450 milyon dolardı. Neredeyse %10'u mali dolandırıcılık bildirdi [3] . Her hafta bilgisayar sistemlerinin gizliliğine, bütünlüğüne ve kullanılabilirliğine yönelik yeni saldırılar duyuyoruz. Bu, kişisel olarak tanımlanabilir bilgilerin çalınmasından hizmet reddi saldırılarına kadar değişebilir.

Ekonomi internete olan bağımlılığını artırdıkça, siber suçluların oluşturduğu tüm tehditlere maruz kalıyor. Hisse senetleri internet üzerinden işlem görmekte, banka işlemleri internet üzerinden yapılmakta, internet üzerinden kredi kartı ile alışveriş yapılmaktadır. Bu tür işlemlerdeki tüm dolandırıcılık örnekleri, etkilenen şirketin mali durumunu ve dolayısıyla ekonomiyi etkiler.

Uluslararası finans piyasalarının bozulması, büyük etkilerden biri olabilir ve ciddi bir endişe kaynağı olmaya devam etmektedir. Modern ekonomi birden fazla ülkeyi ve zaman dilimini kapsar. Dünyanın ekonomik sisteminin böyle bir karşılıklı bağımlılığı, dünyanın bir bölgesindeki bir bozulmanın diğer bölgelerde dalgalanma etkileri olacağı anlamına gelir. Bu nedenle, bu sistemlerin herhangi bir kesintisi, sorunun kaynağı olan piyasanın dışına şok dalgaları gönderecektir.

Verimlilik de risk altındadır. Solucanlardan, virüslerden vb. gelen saldırılar, kullanıcıdan verimli zaman alır. Makineler daha yavaş çalışabilir; sunucular erişilebilir

durumda olabilir, ağlar sıkışmış olabilir vb. Bu tür saldırı örnekleri, kullanıcının ve kuruluşun genel üretkenliğini etkiler. Dış müşterinin onu organizasyonun olumsuz bir yönü olarak gördüğü müşteri hizmetleri etkileri de vardır .

Buna ek olarak, kullanıcıların potansiyel dolandırıcılık konusundaki endişeleri, çevrimiçi alışveriş yapanların önemli bir bölümünün iş yapmasını engeller. E-ticaret gelirlerinin önemli bir kısmının alışveriş yapanların tereddüt, şüphe ve endişelerinden dolayı kaybedildiği açıktır. Bu tür tüketici güveni sorunlarının ciddi sonuçları olabilir ve daha fazla ayrıntıya girmeyi gerektirebilir.

Tüketici güveni

Siber saldırganlar başkalarının alanına girip sayfanın mantığını bozmaya çalıştıkları için, ilgili sayfayı ziyaret eden son müşteri hüsrana uğrayacak ve söz konusu siteyi uzun vadede kullanmaktan vazgeçecektir. Söz konusu site dolandırıcı olarak adlandırılırken, gizli saldırıyı yöneten suçlu, temel neden olarak kabul edilmiyor. Bu, müşterinin söz konusu siteye ve internete ve güçlü yönlerine olan güvenini kaybetmesine neden olur.

Better Business Bureau Online tarafından desteklenen raporlara göre, çevrimiçi alışveriş yapanların %80'inden fazlası, İnternet üzerinden iş yaparken güvenliği birincil endişe olarak belirtti. Çevrimiçi alışveriş yapanların yaklaşık %75'i, kredi kartı bilgileri istendiğinde çevrimiçi bir işlemi sonlandırıyor. İnternetin kredi kartı dolandırıcılığı ve güvenlik tehlikeleriyle dolu olduğu *algısı büyüyor.* Bu, e-ticaret için ciddi bir sorun olmuştur.

Konuyu karmaşıklaştıran, tüketicinin dolandırıcılık algıları, durumu gerçekte olduğundan *daha kötü olarak değerlendiriyor.* Tüketici algısı, gerçek kadar güçlü veya zarar verici olabilir. Bu nedenle, kullanıcıların dolandırıcılık konusundaki endişeleri, birçok çevrimiçi alışveriş yapanın iş yapmasını engeller. Bir e-işin güvensiz veya dağınık olması açısından güvenilirliğine ilişkin endişe, alışveriş yapanları iş yapmak konusunda isteksiz kılar. En ufak bir güvenlik riski veya amatörce ticaret algısı bile potansiyel işi ciddi şekilde tehlikeye atıyor.

Sömürü için Olgun Alanlar

Çoğu ülkenin modern ordusu, büyük ölçüde gelişmiş bilgisayarlara bağlıdır. Ağ saldırısı, istismar ve savunma dahil olmak üzere Bilgi Savaşı veya IW, yeni bir ulusal güvenlik sorunu değildir, ancak 9/11'den beri ek bir önem kazanmıştır. IW, düşük maliyetli, son derece etkili olabileceği ve saldırgana inkar edilebilirlik sağlayabileceği için çekicidir. Kötü amaçlı yazılımları kolayca yayarak ağların çökmesine ve yanlış bilgilerin yayılmasına neden olabilir. Vurgu daha çok bilgi dışı savaş üzerine olduğu için, bilgi savaşı kesinlikle keşif için olgunlaşmıştır.

Çoğu spam gönderici satmayı düşünmez. Tek istedikleri kredi kartı numarasını almak. Geçenlerde eşimin başına geldi. eBay'den iki farklı e-posta aldı. Bu e-postalar, hesabı doğrulamasını istedi. Son kullanma tarihi ve üç haneli şifre ile birlikte kredi kartı numarasını girmesini beklediler. Hatta ondan ATM kartı için PIN numarasını girmesini istedi. Uygun eBay markasına sahip gerçek bir eBay web sitesine benzeyen bir web sitesine götürüldü. Ancak bu tür web siteleri aslında dolandırıcılık halkaları tarafından

yönetilmektedir. Kredi kartı ve banka kartı bilgilerinin doğrudan kaybının yanı sıra, bu tür dolandırıcılıklar, yukarıda tartışıldığı gibi, internete ve güvenliğine olan popüler güveni zedeler. Bu, yakın gelecekte yeni sınırlar görecek yeni bir saldırı yöntemidir. Geçmişte, bilgisayar korsanları esas olarak övünme haklarının peşindeydi, ancak profesyonel bilgisayar korsanları kar elde etmeyi hedefliyor. Dolayısıyla kararlılıkları ve sahip oldukları kaynaklar çok daha fazladır.

Gittikçe daha fazla güvenlik duvarı hack'i rapor edildikçe, her modemde iki yönlü bir güvenlik duvarına sahip olmak vurgulanacaktır. Bu, gelen saldırıları ve giden saldırıları da güvence altına alacaktır. Bu kesinlikle profesyonel bir bilgisayar korsanının yararlanacağı ve şu anda iki yönlü güvenlik duvarının oluşturduğu bariz bir güvenliği aşmanın yollarını bulacağı yeni bir yol olacaktır.

Ulusal Güvenlik

İnternetin yüzde 90'ı önemsiz ve yüzde 10'u iyi güvenlik sistemlerine sahiptir. Davetsiz misafirler, kolayca girilebilecek sistemler bulduğunda, sisteme sızarlar. Teröristler ve suçlular, suç faaliyetlerini planlamak ve yürütmek için bilgi teknolojisini kullanır. Uluslararası etkileşimin artması ve bilişimin yaygınlaşması suç ve terörizmin büyümesini kolaylaştırmıştır. Gelişmiş iletişim teknolojisi nedeniyle, insanların bu tür suçları organize etmek için tek bir ülkede olmalarına gerek yoktur. Böylece teröristler ve suçlular sistemde güvenlik açıkları bulabilir ve ikamet ettikleri ülke yerine olağandışı yerlerden çalışabilirler. Bu tür suçların çoğu gelişmekte olan ülkelerden kaynaklanmaktadır. Bu ülkelerdeki yaygın yolsuzluk, bu güvenlik saldırılarını körüklüyor. İnternet, dolandırıcılık amaçlı banka

işlemleri, para transferi vb. yoluyla bu tür suçların finanse edilmesine yardımcı olmuştur. Daha fazla şifreleme teknolojisi bu suç faaliyetlerine yardımcı olmaktadır.

Gelecek trendleri

En büyük endişelerden biri, hükümet, şirketler, finans kurumları vb. kritik sistemlere bir saldırı olursa ne olur? Bu, kritik sistemlerde kötü amaçlı yazılımlara yol açarak veri kaybına, yanlış kullanıma ve hatta kritik sistemlerin ölümüne neden olabilir. İnternet üzerinden iletişim akışı kolay olduğu için suç örgütleri şu anda olduğundan daha fazla birleşip işbirliği yapabilmektedir.

Artan hareketlilik nedeniyle fonların ve insanların kolayca transfer olabileceğinden korkulmaktadır. İnternetin kara para aklama için kullanılması giderek daha olasıdır. İnternet, giderek daha fazla uluslararası ticaretin gerçekleştiği ortam haline geldikçe, fazla faturalama ve eksik faturalama yoluyla kara para aklama fırsatları da artacaktır. Çevrimiçi açık artırmalar, görünüşte meşru satın alımlar yoluyla parayı taşımak için benzer fırsatlar sunar, ancak malların değerinden çok daha fazlasını ödemek. Çevrimiçi kumar, özellikle denizaşırı finans merkezlerine para taşımayı da mümkün kılar .

İnternet üzerinden suç teşkilatlarına işe alım eskisinden daha kolay olacak. Gizli mesajlar internet üzerinden çok büyük bir kitleye dikkat çekmeden çok kolay bir şekilde aktarılabilmektedir.

Bilgi teknolojisi şirketlerinin çoğu özel sektöre ait olduğundan, odak noktası, ulusötesi suç hakkında endişelenmek yerine müşteriyi mutlu etmek olacaktır. Ayrıca, bilgi teknolojisinin

izlenmemesi lehinde meşru medeni özgürlükler tartışılabilir. Tüm bunlar siber suçlarla mücadeleyi daha da zorlaştırıyor.

Çözüm

İnternetin son yirmi yılda hayatımızı, kültürümüzü ve toplumumuzu sayısız şekilde değiştirdiğini kimse inkar edemez. Tüm fenomen hala o kadar yeni ki, bundan tam olarak nasıl etkilendiğimizi ve gelecekte bizi hangi yeni yollarla etkilemeye devam edeceğini henüz keşfetmedik. İnternetin bize hangi yeni gelişmeleri sağlayacağını, hangi yeni sanat formlarını, sosyal sınıfları veya alt kültürleri doğuracağını kesin olarak söyleyemeyiz. Getirdiği tüm tehlikeleri de tahmin edemeyiz.

Siber suç da mutlaka çok yenidir. Belli ki internetin kendisinden daha eski değil. Bununla birlikte, daha genç de değil - bir internet olduğu anda, onu sömürmek için çalışan suçlular vardı. Tüm yeni teknolojilerde böyledir. Kendimizi en iyi şekilde korumak için siber suçların bir adım önünde olmak için elimizden gelenin en iyisini yapmalıyız. En azından, çok geride kalmayı göze alamayız.

Referanslar

[1] Siber Adli Tıp
Bilgisayar suçlarının kanıtlarını toplamak, incelemek ve korumak için bir dosya kılavuzu
Yazan: Albert J. Marcella ve Robert S. Greenfield
ISBN: 0-8493-0955-7

[2] Hacking Exposed – Adli Bilişim – Sırlar ve Çözümler

Yazan: Chris Davis, Aaron Philipp ve David Cowen
ISBN: 0 – 07- 225675-
3

[3] http://usinfo.state.gov/journals/itgic/0801/ijge/gj07.htm

[4] http://www.cwalsh.org/isnd/archives/001270.html

[5] http://www.ci.san-luis-obispo.ca.us/police/cybercrime.asp

[6]

http://computerworld.com/securitytopics/security/cybercrime/story/0,10801,106574,00.html?SK

C=siber suç-106574
[7] Hacker'ın biyografisi http://www.rotten.com/library/bio/hackers

[8] Siber Suç Mahalli: Debra Littlejohn Shinder Tarafından Yazan Adli

Bilgisayar El Kitabı http://www.syngress.com/catalog/?pid=2250

[9] Hükümet Teknolojisi: 21. Yüzyılda Siber-terörizm

http://www.governmenttechnologyuk.com/default.asp?id=261

[10] Hacking'in Tarihi

http://pcworld.about.com/news/Apr102001id45764.htm

[11] Hacker'lar: Bir St. Petersburg Times dizisi.

http://www.sptimes.com/Hackerlar

[12] 'Aşk' virüsünün dersleri hala batıyor

(http://news.com.com/Lessons+of+Love+virus+still+sinking+in/2100-1001_3-257095.html)

[13] TheWHIR'in Web Sunucusu Haberleri http://www.thewhir.com/marketwatch/ [14] Phreaking'in Kısa Tarihi http://emmaf.isuisse.com/anarcook/frekhist.htm

[15] Hacking ve Hackerlar http://www.thocp.net/reference/hacking/hacking.htm

[16] Wahingtonpost.com: Federal İnternet Rehberi http://www.washingtonpost.com/wp-srv/national/longterm/fedguide/stories/fig010998.htm

[17] Güvenilir Bilgi İşlem http://www.microsoft.com/mscorp/execmail/2002/07-18twc.asp

[18] I-Way Robbery: Crime on the Internet (ciltsiz) William C. Boni, Gerald L. Kovacich

[19] http://stuff.mit.edu/hacker/hacker.html

[20] http://www.cbsnews.com/stories/2004/10/20/60II/main650428.shtml

[21]http://www.microsoft.com/smallbusiness/resources/technology/security/hacking_into_the_m ind_of_a_hacker.mspx

[22]http://msnbc.msn.com/id/3078571/

[23]http://www.cnn.com/SPECIALS/cold.war/experience/spies/melton.essay/

[24] Chawki, Mohamed. "Siber Suçlar Yönetmeliğine Eleştirel Bir Bakış." *Bilgisayar Suçu Araştırma Merkezi* . <http://www.crime-research.org/articles/Critical/>

[25] "Bilgisayar Saldırı Vakaları İndeksi" *Adalet Bakanlığı, Ceza Dairesi, Bilgisayar Suçları ve Fikri Mülkiyet Bölümü.*

< http://www.usdoj.gov/criminal/cybercrime/cccases.html>

[26] Bilgisayar Dolandırıcılığı ve Kötüye Kullanımı Yasası , 18 USC § 1030 (1986)

[27] "1996 Ulusal Bilgi Altyapısını Koruma Yasası: Mevzuat Analizi."

Adalet Bakanlığı, Ceza Bölümü, Bilgisayar Suçları ve Fikri Mülkiyet Bölümü.

<http://www.usdoj.gov/criminal/cybercrime/1030_anal.html>

[28] "Ridge, Siber Tehditlerle Mücadele İçin Yeni Birim Oluşturuyor." *Vatan Departmanı Güvenlik, Basın Odası. <* http://www.dhs.gov/dhspublic/display?content=916>

[29] "Bilgisayar Hackleme ve Fikri Mülkiyet Birimi Oluşturulacak Sacramento'daki ABD Savcılığı." *Adalet Bakanlığı, Ceza Dairesi.*

<http://www.usdoj.gov/criminal/cybercrime/chips101904.htm>

[30] Leydon, John. "Melissa Virüs Yazarı 20 Ay Hapsedildi" *The Register,* Mayıs 2002

<http://www.theregister.co.uk/2002/05/01/melissa_virus_author_jailed/>

[31] "Adam 911 Truva Atı İçin Mahkûm Edildi." *Virüs Bülteni* , Mart 2005. **http://www.virusbtn.com/news/virus_news/2005/03_15.xml**