Źli faceci i przypadkowi źli faceci: ludzie, przed którymi musisz się bronić.

Wiele wieków temu chiński strateg wojskowy i filozof Sun Tzu napisał, że jeśli znasz wroga i znasz siebie, nie musisz obawiać się wyniku stu bitew. Jeśli znasz siebie, ale nie wroga, za każde odniesione zwycięstwo poniesiesz porażkę. Jeśli nie znasz ani wroga, ani siebie, poddasz się w każdej bitwie.

Jak to było od czasów starożytnych, znajomość wroga ma kluczowe znaczenie dla własnej obrony. Taka mądrość pozostaje prawdziwa w erze bezpieczeństwa cyfrowego. Podczas gdy rozdział 2 omawia wiele zagrożeń stwarzanych przez cyber-wrogów, ten rozdział omawia samych wrogów:

*Kim oni są?

* Dlaczego przeprowadzają ataki?

* W jaki sposób zyskują na atakach?

Dowiesz się również o nieszkodliwych napastnikach - zarówno ludzi, jak istrony nieożywione, które mogą wyrządzić poważne szkody nawet bez zamiaru wyrządzenia szkody.

Źli i dobrzy faceci to określenia względne

Albert Einstein powiedział, że „wszystko jest względne" i ta koncepcja z pewnością jest prawdziwa, jeśli chodzi o zrozumienie, kim są „dobrzy" i „źli" faceci w sieci. Na przykład jako ktoś, kto chce się bronić przed cyberatakami, możesz postrzegać rosyjskich hakerów próbujących włamać się do Twojego komputera w celu włamania się do witryn rządowych USA, jako złoczyńców, ale dla patriotycznych obywateli Rosji mogą być bohaterami. Podobnie, jeśli mieszkasz na Zachodzie, możesz postrzegać twórców Stuxneta - złośliwego oprogramowania, które zniszczyło irańskie wirówki używane do wzbogacania uranu w celu potencjalnego użycia w broni jądrowej - jako bohaterów. Jeśli jednak jesteś członkiem irańskiego zespołu wojskowego ds. Cyberobrony, Twoje odczucia są prawdopodobnie zupełnie inne.

STUXNET

Stuxnet to robak komputerowy, który po raz pierwszy został odkryty w 2010 roku i uważa się, że spowodował, przynajmniej tymczasowo, poważne szkody w programie nuklearnym Iranu. Do tej pory nikt nie wziął na siebie odpowiedzialności za stworzenie Stuxneta, ale ogólny konsensus w branży bezpieczeństwa informacji jest taki, że został on zbudowany jako wspólny wysiłek amerykańskich i izraelskich cyberwojowników. Stuxnet jest ukierunkowany na programowalne sterowniki logiczne (PLC), które zarządzają automatycznym sterowaniem maszynami przemysłowymi, w tym wirówkami używanymi do oddzielania cięższych i lżejszych atomów pierwiastków radioaktywnych. Uważa się, że Stuxnet włamał się do sterowników PLC w irańskim zakładzie wzbogacania uranu, programując wirówki tak, aby wymykały się spod kontroli i skutecznie ulegały samozniszczeniu, a wszystko to jednocześnie informowało, że wszystko działa prawidłowo. Stuxnet wykorzystał cztery luki typu „zero-day", które nie były znane opinii publicznej i producentom w momencie wykrycia Stuxneta. Robak został zaprojektowany do rozprzestrzeniania się w sieciach - i rozprzestrzeniania się jak pożar - ale pozostawał w stanie uśpienia, jeśli nie wykrył odpowiedniego oprogramowania PLC i Siemensa używanego w irańskim obiekcie. Jeśli jesteś Amerykaninem i korzystasz z wolności słowa w Internecie i publikujesz posty dla promowania ateizmu, chrześcijaństwa, buddyzmu lub judaizmu i Irańczyka haker włamuje się do Twojego komputera, prawdopodobnie uznasz go za złego faceta, ale różni członkowie irańskiego rządu i innych fundamentalistycznych grup islamskich mogą uważać działania hakera za heroiczną próbę powstrzymania szerzenia się bluźnierczej herezji. W wielu przypadkach określenie, kto jest dobry, a kto zły, może być jeszcze bardziej skomplikowane i prowadzić do głębokich podziałów między

członkami jednej kultury. Na przykład, jak byś ocenił kogoś, kto łamie prawo i narusza wolność słowa neonazistów, przeprowadzając paraliżujący cyberatak na neonazistowską stronę internetową, która głosi nienawiść do Afroamerykanów, Żydów i gejów? Albo ktoś spoza organów ścigania, który nielegalnie przeprowadza ataki na strony rozpowszechniające pornografię dziecięcą, złośliwe oprogramowanie lub materiały o dżihadystach, które zachęcają ludzi do zabijania Amerykanów? Czy myślisz, że wszyscy, których znasz, zgodzą się z tobą? Czy sądy amerykańskie się zgodzą? Przed udzieleniem odpowiedzi proszę wziąć pod uwagę, że w sprawie z 1977 r. Narodowo-Socjalistyczna Partia Ameryki przeciwko wiosce Skokie, Sąd Najwyższy Stanów Zjednoczonych orzekł, że wolność słowa idzie tak daleko, że pozwala nazistom wymachującym swastykami swobodnie maszerować w sąsiedztwie, w którym żyło wielu ocalałych z nazistowskiego Holokaustu. Oczywiście w świecie cyberprzestrzeni tylko oko patrzącego może mierzyć dobro i zło. Dlatego musisz zdefiniować, kim są dobrzy i źli faceci, i jako taki powinieneś założyć, że język w książce działa z Twojej perspektywy, gdy starasz się bronić cyfrowo. Każdy, kto chce zaszkodzić twoim interesom, z jakiegokolwiek powodu i bez względu na to, jakie postrzegasz swoje interesy, jest dla celów tej książki zły.

Źli faceci nie są dobrzy

Grupa potencjalnych napastników, która jest prawdopodobnie dobrze znana większości ludzi, to źli ludzie, którzy nie planują nic dobrego. Ta grupa składa się z wielu typów napastników o zróżnicowanym zestawie motywacji i możliwości ataku, których łączy jeden wspólny cel: wszyscy starają się czerpać korzyści kosztem innych, w tym potencjalnie Ciebie. Źli faceci do niczego dobrego obejmują

* Script kiddies

* Dzieci, które nie są dziećmi

* Narody i państwa

* Szpiedzy korporacyjni

* Przestępcy

* Haktywiści

Script kiddies

Termin script kiddies (czasami skracany do skidów lub po prostu kiddies) odnosi się do ludzi - często młodych - którzy włamują się, ale są w stanie to zrobić tylko dlatego, że wiedzą, jak wykorzystać skrypty i / lub programy opracowane przez innych do atakowania systemów komputerowych. Tym ludziom brakuje zaawansowania technologicznego potrzebnego do tworzenia własnych narzędzi lub hakowania bez pomocy innych.

Dzieci, które nie są dzieciakami

Podczas gdy dzieciaki od scenariuszy są nieskomplikowane technologicznie (patrz poprzednia sekcja), wiele innych nie jest. Przez wiele lat karykaturą hakera był młody, nerdowaty mężczyzna, zainteresowany komputerami, który włamuje się z domu swoich rodziców lub z akademika na uczelni. W rzeczywistości pierwsza grupa hakerów atakujących systemy cywilne obejmowała wiele zaawansowanych technologicznie dzieciaków zainteresowanych badaniem lub wykonywaniem różnych złośliwych zadań w celu przechwalenia się lub z powodu ciekawości. Chociaż tacy napastnicy nadal istnieją, odsetek ataków pochodzących od tych napastników spadł dramatycznie z ogromnej części do niewielkiego ułamka procentu wszystkich ataków. Mówiąc najprościej, nastoletni hakerzy, podobni do tych przedstawionych w filmach z lat 80. i 90., mogli być znaczącą siłą w erze

przedkomercyjnej Internetu, ale kiedy hakowanie mogło dostarczyć prawdziwe pieniądze, drogie towary i cenne dane, na które można zarobić, przestępcy chcą zysk włączył się do walki masowo. Ponadto, w miarę jak świat stawał się coraz bardziej zależny od danych i coraz więcej systemów rządowych i przemysłowych było podłączonych do Internetu, narody i państwa zaczęły dramatycznie zwiększać zasoby, które przeznaczały na operacje cybernetyczne, zarówno ze szpiegowskiego, jak i wojskowego punktu widzenia, co jeszcze bardziej osłabiło klasyczne nastoletnie hakera do niewielkiej części dzisiejszych cyberataków.

Narody i państwa

Hakowanie dokonywane przez narody i stany było w ostatnich latach bardzo głośne w prasie. Rzekome włamania do systemów poczty elektronicznej Partii Demokratycznej przez rosyjskich agentów podczas kampanii wyborczej prezydenckiej w 2016 r. Oraz systemu poczty elektronicznej Partii Republikańskiej podczas wyborów w połowie kadencji w 2018 r. To głośne przykłady hakowania przez państwa narodowe. Podobnie szkodliwe oprogramowanie Stuxnet jest przykładem złośliwego oprogramowania sponsorowanego przez państwo lub państwo. To powiedziawszy, większość narodowych i stanowych ataków cybernetycznych nie jest tak głośna, jak te przykłady, nie dociera do mediów i nie jest wymierzona w znane cele. Często nie są one nawet odkrywane ani znane nikomu poza napastnikami! Ponadto w niektórych krajach odróżnienie hakowania narodowego lub państwowego od szpiegostwa handlowego jest trudne, jeśli nie niemożliwe. Weźmy na przykład kraje, w których duże firmy są własnością rządu i są przez niego obsługiwane. Czy takie firmy są uzasadnionymi celami rządowymi, czy hakowanie ich jest przykładem szpiegostwa korporacyjnego? Oczywiście naród i stany, które hakują, mogą również próbować wpłynąć na nastroje opinii publicznej, decyzje polityczne i wybory w innych krajach. Dyskusje na ten temat są regularnie emitowane w głównych mediach od wyborów prezydenckich w 2016 roku.

Szpiedzy korporacyjni

Firmy pozbawione skrupułów czasami wykorzystują hakowanie jako sposób na zdobycie przewagi konkurencyjnej lub kradzież cennej własności intelektualnej. Na przykład rząd Stanów Zjednoczonych wielokrotnie oskarżał chińskie korporacje o kradzież własności intelektualnej amerykańskich przedsiębiorstw, co kosztuje Amerykanów miliardy dolarów rocznie. Czasami proces kradzieży własności intelektualnej wiąże się z włamywaniem się do domowych komputerów pracowników atakowanych firm z nadzieją, że pracownicy ci będą używać swoich urządzeń osobistych do łączenia się z sieciami pracodawców.

Przestępcy

Przestępcy mają wiele powodów do uruchamiania różnych form ataków komputerowych:

* Bezpośrednia kradzież pieniędzy: atakowanie w celu uzyskania dostępu do czyjegoś konta bankowego online i wysłania pieniędzy do siebie.

* Kradzież numerów kart kredytowych, oprogramowania, wideo, plików muzycznych i innych towarów: atakowanie zakupu towarów lub dodawanie fałszywych instrukcji wysyłki do systemu korporacyjnego, co prowadzi do wysyłania produktów bez otrzymania płatności przez nadawcę itd.

* Kradzież danych firmowych i indywidualnych: atakowanie w celu uzyskania informacji, na których przestępcy mogą zarabiać na wiele sposobów. . Z biegiem lat rodzaj przestępców popełniających przestępstwa online ewoluował od aktorów wyłącznie solowych do amatorów i zorganizowanych przestępców.

Haktywiści

Haktywiści to aktywiści, którzy używają hakowania, aby rozpowszechniać przesłanie swojej „sprawy" i wymierzać sprawiedliwość stronom, które ich zdaniem nie są w inny sposób karane za wykroczenia, które aktywiści uważają za przestępstwa. Haktywiści obejmują terrorystów i nieuczciwych insiderów.

Terroryści

Terroryści mogą hakować w różnych celach, w tym

* Bezpośrednio wyrządzaj szkody (na przykład hakując narzędzie i wyłączając zasilanie).

* Zdobądź informacje do wykorzystania podczas planowania ataków terrorystycznych (na przykład hakowanie, aby dowiedzieć się, kiedy broń jest transportowana między obiektami i może zostać skradziona)

* Finansowanie operacji terrorystycznych (zobacz wcześniejszą sekcję dotyczącą przestępców)

Rogue insiders

Niezadowoleni pracownicy, nieuczciwi kontrahenci i pracownicy, którzy zostali zachęceni finansowo przez stronę pozbawioną skrupułów, stanowią poważne zagrożenie zarówno dla firm, jak i dla ich pracowników. Osoby, które chcą ukraść dane lub wyrządzić krzywdę, są zwykle uważane za najbardziej niebezpieczną grupę cyberataków. Zazwyczaj wiedzą znacznie więcej niż osoby z zewnątrz o tym, jakie dane i systemy komputerowe posiada firma, gdzie te systemy się znajdują, w jaki sposób są chronione, a także o innych informacjach związanych z systemami docelowymi i ich potencjalnymi słabościami. Nieuczciwi pracownicy mogą kierować reklamy na firmy z jednego lub kilku powodów:

* Mogą próbować zakłócić działalność, aby odciążyć swoje osobiste obowiązki lub pomóc konkurentowi.

* Mogą szukać zemsty za nieotrzymanie promocji lub premii.

* Mogą chcieć, aby inny pracownik lub zespół pracowników wyglądał źle.

* Mogą chcieć wyrządzić pracodawcy szkodę finansową.

* Mogą planować odejście i chcieć ukraść dane, które będą cenne w ich następnej pracy lub w przyszłych przedsięwzięciach.

Cyberatakerzy i ich kolorowe kapelusze

Cyberatakcy są zazwyczaj grupowani na podstawie ich celów:

* Hakerzy w czarnych kapeluszach mają złe zamiary i włamują się, aby kraść, manipulować i / lub niszczyć. Kiedy typowa osoba myśli o hakerze, ma na myśli hakera czarnego kapelusza.

* Hakerzy w „białych kapeluszach" to etyczni hakerzy, którzy hakują w celu testowania, naprawiania i zwiększania bezpieczeństwa systemów i sieci. Ci ludzie są zazwyczaj ekspertami w dziedzinie bezpieczeństwa komputerowego, którzy specjalizują się w testach penetracyjnych i są zatrudniani przez firmy i rządy do znajdowania luk w ich systemach IT. Haker jest uznawany za hakera typu white hat tylko wtedy, gdy ma wyraźne pozwolenie na hakowanie od właściciela systemów, które hakuje. Hakerzy w szarym kapeluszu to hakerzy, którzy nie mają złośliwych zamiarów hakerów czarnych kapeluszy, ale przynajmniej czasami zachowują się nieetycznie lub w inny sposób naruszają przepisy antyhakerskie. Haker, który próbuje znaleźć luki w systemie bez zgody właściciela systemu i który zgłasza swoje ustalenia właścicielowi bez powodowania szkód w systemach, które skanuje, zachowuje

się jak haker w szarym kapeluszu. Hakerzy z szarymi kapeluszami czasami działają w ten sposób, aby zarabiać pieniądze. Na przykład, gdy zgłaszają luki w zabezpieczeniach właścicielom systemu, mogą zaoferować rozwiązanie problemów, jeśli właściciel zapłaci im opłaty za konsultacje. Niektórzy z hakerów, których wiele osób uważa za hakerów czarnych kapeluszy, są w rzeczywistości szarymi kapeluszami.

* Hakerzy w zielonych kapeluszach to nowicjusze, którzy chcą zostać ekspertami. Tam, gdzie zielony kapelusz mieści się w biało-szaro-czarnym spektrum, może z czasem ewoluować, podobnie jak jego poziom doświadczenia.

* Hakerzy w niebieskich kapeluszach otrzymują wynagrodzenie za testowanie oprogramowania pod kątem błędów, które można wykorzystać, zanim oprogramowanie zostanie wprowadzone na rynek.

Zarabianie na swoich działaniach

Wielu cyberatakujących stara się na nich czerpać korzyści finansowe, ale nie wszystko to przestępstwa. Cyberatakujący mogą zarabiać na cyberatakach na kilka sposobów:

* Bezpośrednie oszustwo finansowe

* Pośrednie oszustwo finansowe

* Oprogramowanie ransomware

* Cryptominers

* Bezpośrednie oszustwo finansowe

Bezpośrednie oszustwo finansowe

Hakerzy mogą próbować kraść pieniądze bezpośrednio poprzez ataki. Na przykład hakerzy mogą instalować złośliwe oprogramowanie na komputerach ludzi, aby przechwytywać sesje bankowości internetowej ofiar i poinstruować serwer bankowości internetowej, aby wysyłał pieniądze na konta przestępców. Oczywiście przestępcy wiedzą, że systemy bankowe są często dobrze chronione przed takimi formami oszustw, więc wielu z nich przeniosło się na słabiej chronione systemy. Na przykład niektórzy przestępcy koncentrują się teraz bardziej na przechwytywaniu danych logowania (nazw użytkowników i haseł) do systemów przechowujących kredyty - na przykład aplikacje do kawiarni, które umożliwiają użytkownikom przechowywanie wartości kart przedpłaconych - i kradzież pieniędzy skutecznie zgromadzonych na takich kontach za ich pomocą gdzie indziej w celu zakupu towarów i usług. Ponadto, jeśli przestępcy włamują się na konta użytkowników, którzy mają skonfigurowane funkcje automatycznego uzupełniania, przestępcy mogą wielokrotnie kraść wartość po każdym automatycznym przeładowaniu. Podobnie przestępcy mogą próbować naruszyć konta osób często podróżujących i przenosić punkty na inne konta, kupować towary lub uzyskiwać bilety lotnicze i pokoje hotelowe, które sprzedają innym osobom za gotówkę. Przestępcy mogą również kraść numery kart kredytowych i albo ich używać, albo szybko sprzedawać innym oszustom, którzy następnie wykorzystują je do popełnienia oszustwa. Direct nie jest koncepcją czarno-białą; istnieje wiele odcieni szarości.

Pośrednie oszustwo finansowe

Wyrafinowani cyberprzestępcy często unikają cyberprzestępstw, które wiążą się z bezpośrednimi oszustwami finansowymi, ponieważ schematy te często przynoszą stosunkowo niewielkie kwoty w dolarach i mogą zostać osłabione przez strony zagrożone nawet po fakcie (na przykład poprzez cofnięcie oszukańczych transakcji lub unieważnienie zamówienia na towary złożone ze skradzionych

informacji) i stwarzają stosunkowo duże ryzyko złapania. Zamiast tego mogą starać się uzyskać dane, na których mogą zarabiać za oszustwa pośrednie. Oto kilka przykładów takich przestępstw

* Zyski z nielegalnego obrotu papierami wartościowymi

* Kradzież informacji o karcie kredytowej

* Kradzież towarów

* Kradzież danych

Zyski na nielegalnym obrocie papierami wartościowymi

Cyberprzestępcy mogą zarabiać fortuny na nielegalnym handlu papierami wartościowymi, takimi jak akcje, obligacje i opcje, na kilka sposobów:

* Pump and dump: Przestępcy hakują firmę i kradną dane, skracają akcje firmy, a następnie wyciekają dane firmy do Internetu, aby spowodować spadek ceny akcji firmy, po czym kupują akcje (w celu pokrycia krótkiej sprzedaży) po niższa cena niż wcześniej ją sprzedali.

* Fałszywe komunikaty prasowe i posty w mediach społecznościowych: przestępcy kupują lub sprzedają akcje firmy, a następnie publikują fałszywe informacje prasowe lub w inny sposób rozpowszechniają fałszywe informacje o firmie, włamując się do systemów marketingowych firmy lub kont w mediach społecznościowych i publikując fałszywe złe lub dobre wiadomości za pośrednictwem oficjalnych kanałów firmy.

* Informacje poufne: przestępca może próbować ukraść wersje robocze komunikatów prasowych z działu PR spółki publicznej, aby sprawdzić, czy pojawią się jakieś zaskakujące kwartalne ogłoszenia o dochodach. Jeśli oszust stwierdzi, że firma ma zamiar ogłosić znacznie lepsze liczby, niż spodziewał się Wall Street, może kupić opcje kupna (opcje, które dają oszustowi prawo do zakupu akcji firmy za określoną cenę), których wartość może gwałtownie wzrosnąć po takim ogłoszeniu. Podobnie, jeśli firma ma zamiar ogłosić złe wieści, oszust może skrócić akcje firmy lub kupić opcje sprzedaży (opcje, które dają oszustom prawo do sprzedaży akcji firmy po określonej cenie), które z oczywistych powodów mogą gwałtownie wzrosnąć, jeśli cena rynkowa powiązanych spadków zapasów.

Dyskusje na temat pośrednich oszustw finansowych wymienionych powyżej typów nie są teoretyczne ani nie są wynikiem teorii paranoicznych lub spiskowych; przestępcy zostali już przyłapani na takich właśnie zachowaniach. Tego typu oszustwa są często również mniej ryzykowne dla przestępców niż bezpośrednia kradzież pieniędzy, ponieważ organom regulacyjnym trudno jest wykryć takie przestępstwa na bieżąco, a cofnięcie jakichkolwiek istotnych transakcji jest prawie niemożliwe. W przypadku wyrafinowanych cyberprzestępców mniejsze ryzyko złapania w połączeniu ze stosunkowo dużymi szansami na sukces przekłada się na potencjalną żyłę złota.

Kradzież informacji o karcie kredytowej

Jak często pojawia się w doniesieniach prasowych, wielu przestępców stara się kraść numery kart kredytowych. Złodzieje mogą używać tych numerów do kupowania towarów lub usług bez płacenia. Niektórzy przestępcy kupują elektroniczne karty podarunkowe, numery seryjne oprogramowania lub inne półpłynne lub płynne aktywa, które następnie odsprzedają za gotówkę niczego niepodejrzewającym osobom, podczas gdy inni kupują rzeczywiste towary i usługi, które mogli dostarczyć do miejsc takich jak puste domy , gdzie mogą łatwo odebrać przedmioty. Inni przestępcy nie używają ukradzionych kart kredytowych. Zamiast tego sprzedają numery w ciemnej sieci (to znaczy części Internetu, do których można uzyskać dostęp tylko przy użyciu technologii zapewniającej

anonimowość osobom korzystającym z niej) przestępcom, którzy mają infrastrukturę umożliwiającą maksymalne wykorzystanie kart kredytowych szybko, zanim ludzie to zgłoszą. oszustwa na kontach i kartach są zablokowane.

Kradzież towarów

Oprócz form kradzieży towarów opisanych w poprzedniej sekcji, niektórzy przestępcy poszukują informacji o zamówieniach małych, płynnych przedmiotów o dużej wartości, takich jak biżuteria. W niektórych przypadkach ich celem jest kradzież przedmiotów, gdy są one dostarczane do odbiorców, a nie tworzenie fałszywych transakcji.

Kradzież danych

Niektórzy przestępcy kradną dane, aby wykorzystać je do popełnienia różnych przestępstw finansowych. Inni przestępcy kradną dane, aby sprzedać je innym lub ujawnić publicznie. Na przykład skradzione dane firmy mogą być niezwykle cenne dla pozbawionego skrupułów konkurenta.

Oprogramowanie ransomware

Ransomware to złośliwe oprogramowanie komputerowe, które uniemożliwia użytkownikom dostęp do ich plików, dopóki nie zapłacą okupu jakimś przestępczym przedsiębiorstwom. Sam ten rodzaj cyberataku przyniósł już przestępcom miliardy dolarów (tak, to jest miliardy z b) i zagroził wielu istnieniom, ponieważ zainfekowane szpitalne systemy komputerowe stały się niedostępne dla lekarzy. Ransomware pozostaje rosnącym zagrożeniem, a przestępcy stale ulepszają możliwości techniczne i zarabiają na swoich cyberbroniach. Na przykład przestępcy tworzą oprogramowanie ransomware, które w celu uzyskania większego zwrotu z inwestycji infekuje komputer i próbuje przeszukiwać połączone sieci i urządzenia w celu znalezienia najbardziej wrażliwych systemów i danych. Następnie zamiast porywać dane, które napotkał jako pierwszy, ransomware aktywuje się i uniemożliwia dostęp do najbardziej wartościowych informacji. Przestępcy rozumieją, że im ważniejsze są informacje dla ich właściciela, tym większe prawdopodobieństwo, że ofiara będzie skłonna zapłacić okup, i tym wyższy prawdopodobnie będzie maksymalny okup, który zostanie dobrowolnie zapłacony. Oprogramowanie ransomware staje się coraz bardziej ukryte i często unika wykrycia przez oprogramowanie antywirusowe. Ponadto przestępcy korzystający z oprogramowania ransomware często przeprowadzają ukierunkowane ataki na strony, o których wiedzą, że mogą zapłacić przyzwoity okup. Przestępcy wiedzą na przykład, że przeciętny Amerykanin jest znacznie bardziej skłonny do zapłacenia 200 dolarów za okup niż przeciętny mieszkaniec Chin. Podobnie często atakują środowiska, w których wyłączenie z sieci ma poważne konsekwencje - na przykład szpital nie może sobie pozwolić na brak systemu dokumentacji pacjentów przez dłuższy czas.

Cryptominers

W kontekście złośliwego oprogramowania kryptowaluta odnosi się do oprogramowania, które przywłaszcza sobie część zasobów zainfekowanego komputera w celu wykorzystania ich do wykonywania złożonych obliczeń matematycznych potrzebnych do tworzenia nowych jednostek kryptowaluty. Utworzona waluta jest przekazywana przestępcy obsługującemu kryptowalutę. Wiele współczesnych wariantów złośliwego oprogramowania cryptominer wykorzystuje grupy zainfekowanych maszyn współpracujących w celu wydobywania. Ponieważ gracze kryptowalut generują pieniądze dla przestępców bez konieczności angażowania ich ludzkich ofiar, cyberprzestępcy, zwłaszcza ci, którym brakuje wyrafinowania w przeprowadzaniu ukierunkowanych ataków ransomware o wysokiej stawce, coraz częściej skłaniają się ku kryptowalutom jako szybkiemu sposobowi zarabiania na cyberatakach. Podczas gdy wartość kryptowalut podlega gwałtownym

wahaniom (przynajmniej w momencie pisania tego rozdziału), uważa się, że niektóre stosunkowo nieskomplikowane sieci wydobywające kryptowaluty przynoszą swoim operatorom ponad 30000 USD miesięcznie.

Radzenie sobie z niegodziwymi zagrożeniami

Podczas gdy niektórzy potencjalni napastnicy zamierzają czerpać korzyści Twoim kosztem, inni nie mają zamiaru wyrządzać szkody. Jednak partie te mogą niewinnie stwarzać niebezpieczeństwa, które mogą być nawet większe niż te stwarzane przez wrogich aktorów.

Ludzki błąd

Być może największe zagrożenie dla cyberbezpieczeństwa ze wszystkich - czy to dla domeny osoby fizycznej, biznesowa lub rządowa - to możliwość popełnienia błędu ludzkiego. Niemal wszystkie poważne naruszenia, o których informowały media w ciągu ostatniej dekady, były możliwe, przynajmniej częściowo, z powodu jakiegoś elementu ludzkiego błędu. W rzeczywistości ludzki błąd jest często niezbędny, aby wrogo nastawieni aktorzy odnieśli sukces w swoich atakach - zjawisko, o którym dobrze wiedzą.

Ludzie: pięta achillesowa cyberbezpieczeństwa

Dlaczego ludzie tak często są słabym punktem łańcucha cyberbezpieczeństwa - popełniając błędy, które umożliwiają masowe włamania? Odpowiedź jest dość prosta. Zastanów się, jak bardzo rozwinęła się technologia w ostatnich latach. Urządzenia elektroniczne, które są dziś wszechobecne, były przedmiotem książek i filmów science-fiction zaledwie jedno lub dwa pokolenia temu. W wielu przypadkach technologia przewyższyła nawet przewidywania dotyczące przyszłości - dzisiejsze telefony są znacznie wydajniejsze i wygodniejsze niż telefon do butów Maxwell Smart, a zegarek Dicka Tracy'ego nie byłby nawet postrzegany jako wystarczająco zaawansowany, aby być współczesną zabawką w porównaniu z urządzeniami które dziś kosztują poniżej 100 dolarów. Technologia bezpieczeństwa również rozwinęła się dramatycznie w czasie. Każdego roku wprowadzanych jest wiele nowych produktów, a na rynku pojawia się wiele nowych, ulepszonych wersji istniejących technologii. Dzisiejsza technologia wykrywania włamań jest na przykład o wiele lepsza niż jeszcze dziesięć lat temu, że nawet zaklasyfikowanie ich do tej samej kategorii oferty produktowej jest wątpliwe. Z drugiej strony rozważmy jednak ludzki mózg. Ludzkie mózgi wyewoluowały z mózgów wcześniejszych gatunków dziesiątki tysięcy lat - za życia człowieka, a nawet w ciągu stuleci kolejnych pokoleń, nie następuje żadna fundamentalna poprawa. W związku z tym technologia bezpieczeństwa rozwija się znacznie szybciej niż ludzki umysł. Ponadto postęp technologiczny często przekłada się na to, że ludzie muszą wchodzić w interakcje z coraz większą liczbą coraz bardziej złożonych urządzeń, systemów i oprogramowania oraz rozumieć, jak właściwie je wykorzystywać. Biorąc pod uwagę ludzkie ograniczenia, prawdopodobieństwo popełnienia przez ludzi poważnych błędów z czasem rośnie. Rosnące zapotrzebowanie na siłę umysłową, które rozwijająca się technologia nakłada na ludzi, jest widoczne nawet na najbardziej podstawowym poziomie. Ile haseł musieli znać twoi dziadkowie, kiedy byli w twoim wieku? Ilu twoi rodzice potrzebowali? Ile potrzebujesz? I jak łatwo zdalni hakerzy łamią hasła i wykorzystują je dla zysku w erze Twoich dziadków? Twoi rodzice? Siebie? Większość Twoich dziadków prawdopodobnie mi ała nie więcej niż jedno lub dwa hasła, gdy byli w Twoim wieku - jeśli nie zero. I żadne z tych haseł nie mogło zostać zhakowane przez dowolne zdalne komputery - co oznacza, że zarówno wybieranie, jak i zapamiętywanie haseł było banalne i nie narażało ich na ryzyko. Jednak obecnie prawdopodobnie będziesz mieć dziesiątki haseł, z których większość można zhakować zdalnie przy użyciu zautomatyzowanych narzędzi, co znacznie zwiększa ryzyko. Podsumowując: musisz zrozumieć, że błąd ludzki stanowi duże zagrożenie dla Twojego cyberbezpieczeństwa - i odpowiednio postępować.

Inżynieria społeczna

W kontekście bezpieczeństwa informacji inżynieria społeczna odnosi się do psychologicznej manipulacji istotami ludzkimi w celu wykonywania działań, których w innym przypadku nie wykonaliby i które są zwykle szkodliwe dla ich interesów.

Przykłady inżynierii społecznej obejmują.

* Dzwonienie do kogoś przez telefon i nakłanianie tej osoby do przekonania, że dzwoniący jest członkiem działu IT i proszenie osoby o zresetowanie hasła e-mail

* Wysyłanie wiadomości phishingowych

* Wysyłanie e-maili dotyczących oszustw CEO

Podczas gdy przestępcy przeprowadzający ataki socjotechniczne mogą mieć złośliwy zamiar, strony, które tworzą lukę lub wyrządzają szkody, zwykle robią to bez zamiaru wyrządzenia szkody osobie docelowej. W pierwszym przykładzie użytkownik, który resetuje swoje hasło, uważa, że robi to, aby pomóc działowi IT w naprawie problemów z pocztą e-mail, a nie że pozwala hakerom na dostęp do systemu pocztowego. Podobnie osoba, która padła ofiarą phishingu lub oszustwa CEO, oczywiście nie stara się pomóc hakerowi, który go atakuje. Inne formy błędu ludzkiego, które zagrażają cyberbezpieczeństwu, obejmują przypadkowe usunięcie informacji, przypadkową błędną konfigurację systemów, nieumyślne zainfekowanie komputera złośliwym oprogramowaniem, omyłkowe wyłączenie technologii bezpieczeństwa i inne niewinne błędy, które umożliwiają przestępcom popełnienie wszelkiego rodzaju złośliwych czynów.

Najważniejsze jest to, aby nigdy nie lekceważyć zarówno nieuchronności, jak i siły ludzkich błędów - w tym własnych. Będziesz popełniać błędy, ja też - wszyscy. Dlatego w ważnych sprawach zawsze dokładnie sprawdzaj, czy wszystko jest tak, jak powinno być.

Katastrofy zewnętrzne

Jak opisano w Części 2, cyberbezpieczeństwo obejmuje zachowanie poufności, integralności i dostępności danych. Jednym z największych zagrożeń dla dostępności - które stwarza również ryzyko z drugiej ręki dla jego poufności i integralności - są katastrofy zewnętrzne. Te katastrofy można podzielić na dwie kategorie: naturalne i spowodowane przez człowieka.

Klęski żywiołowe

Duża liczba ludzi żyje na obszarach w pewnym stopniu narażonych na różne formy klęsk żywiołowych. Od huraganów po tornada, powodzie i pożary, przyroda może być brutalna - i może uszkodzić, a nawet zniszczyć komputery i dane przechowywane w maszynach. Dlatego planowanie ciągłości i odzyskiwanie po awarii są nauczane w ramach procesu certyfikacji dla specjalistów ds. Cyberbezpieczeństwa. Rzeczywistość jest taka, że statystycznie rzecz biorąc, większość ludzi napotka i doświadczy przynajmniej jednej formy klęski żywiołowej w pewnym momencie swojego życia. W związku z tym, jeśli chcesz chronić swoje systemy i dane, musisz odpowiednio zaplanować taką ewentualność. Strategia przechowywania kopii zapasowych na dyskach twardych w dwóch różnych lokalizacjach może być złą strategią, na przykład, jeśli obie lokalizacje składają się z piwnic znajdujących się w domach znajdujących się w strefach powodzi.

Problemy środowiskowe spowodowane przez człowieka

Oczywiście natura nie jest jedyną stroną stwarzającą problemy zewnętrzne. Ludzie mogą powodować powodzie i pożary, a katastrofy spowodowane przez człowieka mogą czasami być gorsze niż te, które

występują naturalnie. Ponadto przerwy w dostawie prądu i skoki napięcia, protesty i zamieszki, strajki, ataki terrorystyczne oraz awarie Internetu i zakłócenia telekomunikacyjne mogą również wpływać na dostępność danych i systemów. Firmy, które tworzyły kopie zapasowe swoich danych z systemów znajdujących się w nowojorskim World Trade Center do systemów w pobliskim World Financial Center, po 11 września przekonały się, jak ważne jest przechowywanie kopii zapasowych poza sąsiedztwem odpowiednich systemów, ponieważ World Financial Center pozostało niedostępny przez jakiś czas po ataku na World Trade Center.

Ryzyko stwarzane przez rządy i przedsiębiorstwa

Niektóre zagrożenia dla cyberbezpieczeństwa - w tym, można rozsądnie argumentować, te najbardziej niebezpieczne dla prywatności osób - nie są tworzone przez przestępców, ale raczej przez przedsiębiorstwa i podmioty rządowe, nawet w zachodnich demokracjach.

Cyberwarriors i cyberspies

Współczesne rządy często dysponują ogromnymi armiami cyberwojowników. Takie zespoły często próbują wykryć luki w oprogramowaniu i systemach, aby wykorzystać je do atakowania i szpiegowania adwersarzy, a także jako narzędzie do egzekwowania prawa. Takie postępowanie stwarza jednak ryzyko dla osób fizycznych i firm. Zamiast zgłaszać luki w zabezpieczeniach odpowiednim dostawcom, różne agencje rządowe często starają się utrzymać luki w tajemnicy, co oznacza, że pozostawiają swoich obywateli, przedsiębiorstwa i inne podmioty rządowe podatne na ataki ze strony przeciwników, którzy mogą odkryć tę samą lukę. Ponadto rządy mogą wykorzystywać swoje zespoły hakerów do walki z przestępczością - lub, w niektórych przypadkach, nadużywać zasobów cybernetycznych, aby zachować kontrolę nad swoimi obywatelami i utrzymać władzę partii rządzącej. Nawet w Stanach Zjednoczonych, po 11 września, rząd wdrożył różne programy masowego gromadzenia danych, które miały wpływ na przestrzegających prawa obywateli USA. Gdyby którakolwiek z zebranych baz danych została okradziona przez obce mocarstwa, obywatele USA mogliby być narażeni na wszelkiego rodzaju cyberproblemy. Niebezpieczeństwa związane z tworzeniem przez rządy skarbów wykorzystywania danych nie są teoretyczne. W ostatnich latach kilka potężnych cyberbroni, które przypuszczalnie zostały stworzone przez agencję wywiadowczą rządu USA, pojawiło się w Internecie i najwyraźniej zostały skradzione przez osobę, której interesy nie były zgodne z interesami agencji. Do dziś nie jest jasne, czy ta broń została użyta przeciwko amerykańskim interesom przez tego, kto ją ukradł.

Bezsilna ustawa o rzetelnej sprawozdawczości kredytowej

Wielu Amerykanów zna ustawę Fair Credit Reporting Act (FCRA), zbiór przepisów wprowadzonych początkowo prawie pół wieku temu i wielokrotnie aktualizowanych. FCRA reguluje gromadzenie raportów kredytowych i wykorzystywanych w nich danych oraz zarządzanie nimi. FCRA została ustanowiona, aby zapewnić sprawiedliwe traktowanie ludzi, a informacje dotyczące kredytów pozostają dokładne i poufne. Zgodnie z ustawą o rzetelnej sprawozdawczości kredytowej biura informacji kredytowej muszą usuwać różne formy negatywnych informacji z raportów kredytowych osób po upływie określonych ram czasowych. Jeśli na przykład nie zapłacisz rachunku karty kredytowej w terminie, gdy jesteś na studiach, jest to niezgodne z prawem, aby opóźniona płatność była umieszczana w Twoim raporcie i uwzględniana w Twojej ocenie kredytowej podczas ubiegania się o kredyt hipoteczny dwie dekady później. Prawo zezwala nawet osobom, które ogłaszają upadłość, aby zacząć od nowa, na usunięcie zapisów dotyczących ich upadłości. W końcu po co by zacząć od nowa, gdyby upadłość na zawsze uniemożliwiła komuś uzyskanie czystej karty? Dziś jednak różne firmy technologiczne podważają ochronę FCRA. Jak trudno jest urzędnikowi kredytowemu banku znaleźć internetowe bazy danych pozwów sądowych związanych z upadłością, wykonując proste wyszukiwanie w Google, a następnie przeszukując takie bazy danych w poszukiwaniu informacji istotnych dla

potencjalnego pożyczkobiorcy? Albo po to, by sprawdzić, czy jakiekolwiek zapisy dotyczące egzekucji z dowolnego czasu są powiązane z nazwiskiem osoby ubiegającej się o pożyczkę? Wykonanie jednego lub drugiego zajmuje tylko kilka sekund, a żadne przepisy nie zabraniają takim bazom danych. Wykonanie zajmuje tylko kilka sekund i żadne przepisy nie zabraniają takim bazom danych uwzględniania rekordów wystarczająco starych, aby usunąć je z raportów kredytowych, a przynajmniej w Stanach Zjednoczonych żadne nie zabrania Google pokazywanie linków do takich baz danych, gdy ktoś wyszukuje nazwisko osoby zaangażowanej w takie działania dziesiątki lat wcześniej.

Usunięte rekordy nie są już tak naprawdę usuwane

Wymiar sprawiedliwości ma różne prawa, które w wielu przypadkach pozwalają młodym osobom, które dopuszczają się drobnych przestępstw do ich trwałych rejestrów karnych i dają sędziom możliwość pieczętowania niektórych akt i usuwania innych form informacji z rejestrów osób. Te prawa pomagają ludziom zaczynać od nowa, a wielu wspaniałych, produktywnych członków społeczeństwa mogło się nie udać bez tych zabezpieczeń. Ale po co takie prawa, jeśli potencjalny pracodawca może znaleźć rzekomo usunięte informacje w ciągu kilku sekund, wyszukując w Google nazwisko kandydata? Google zwraca wyniki z notatek lokalnej policji i dzienników sądowych opublikowanych w lokalnych gazetach, które są teraz archiwizowane online. Ktoś, kto został przywołany za drobne przestępstwo, a następnie pozbawiono go wszystkich zarzutów, może nadal ponosić konsekwencje zawodowe i osobiste dziesiątki lat później - nawet jeśli nigdy nie został oskarżony, osądzony ani uznany za winnego jakiegokolwiek przestępstwa.

Numery ubezpieczenia społecznego

Jeszcze pokolenie temu powszechnie używano numerów ubezpieczenia społecznego jako numerów identyfikacyjnych uczelni. Świat był wtedy tak inny, że ze względu na ochronę prywatności wiele szkół publikowało nawet oceny uczniów przy użyciu numerów ubezpieczenia społecznego, a nie nazwisk uczniów! Tak poważnie. Czy wszyscy studenci, którzy poszli do college'u w latach 70., 80. lub na początku lat 90., naprawdę powinni ujawniać publicznie swoje numery ubezpieczenia społecznego, ponieważ materiały uniwersyteckie, które powstały w świecie przedinternetowym, są teraz archiwizowane online i indeksowane w niektórych wyszukiwarkach ? Co gorsza, niektóre strony uwierzytelniają użytkowników, prosząc o podanie ostatnich czterech cyfr ich numerów telefonów, które często można znaleźć w ułamku sekundy za pomocą sprytnie spreparowanego wyszukiwania Google lub Bing. Jeśli powszechnie wiadomo, że takie informacje stały się niepewne w wyniku wcześniej akceptowanych zachowań, dlaczego rząd nadal wykorzystuje numery ubezpieczenia społecznego i traktuje je tak, jakby nadal były prywatne? Podobnie internetowe archiwa kościoła, synagogi i inne biuletyny społecznościowe często zawierają ogłoszenia o urodzeniu zawierające nie tylko imię dziecka i jego rodziców, ale także szpital, w którym urodziło się dziecko, datę urodzenia i nazwisko dziadków. nazwy. Ile pytań bezpieczeństwa dla konkretnego użytkownika systemu komputerowego może zostać podważonych przez oszusta, który znajdzie tylko jedno takie ogłoszenie? Wszystkie te przykłady pokazują, jak postęp technologiczny może osłabić naszą prywatność i cyberbezpieczeństwo - nawet podważając przepisy prawne, które zostały ustanowione, aby nas chronić.

Platformy mediów społecznościowych

Jedną z grup firm technologicznych, które generują poważne zagrożenia dla cyberbezpieczeństwa, są platformy mediów społecznościowych. Cyberprzestępcy coraz częściej skanują media społecznościowe - czasami za pomocą zautomatyzowanych narzędzi - w celu znalezienia informacji, które mogą wykorzystać przeciwko firmom i ich pracownikom. Atakujący następnie wykorzystują znalezione informacje do przeprowadzania różnego rodzaju ataków, takich jak atak obejmujący dostarczanie

oprogramowania ransomware. Na przykład mogą tworzyć wysoce skuteczne wiadomości e-mail typu spear phishing, które są wystarczająco wiarygodne, aby nakłonić pracowników do kliknięcia adresów URL witryn dostarczających oprogramowanie ransomware lub do otwarcia witryn internetowych dostarczających oprogramowanie ransomware lub do otwarcia załączników zainfekowanych oprogramowaniem ransomware. Liczba oszustw związanych z wirtualnym porwaniem - w których przestępcy kontaktują się z rodziną osoby, która jest poza zasięgiem sieci z powodu lotu lub podobnego zdarzenia i żądają okupu w zamian za uwolnienie osoby, którą rzekomo porwali - gwałtownie wzrosła. era mediów społecznościowych, ponieważ przestępcy często potrafią określić, patrząc na posty użytkowników w mediach społecznościowych, zarówno kiedy podjąć działania, jak iz kim się skontaktować.

Wszechwiedzące komputery Google

Jednym ze sposobów, w jaki systemy komputerowe weryfikują, czy dana osoba jest tym, za kogo się podaje, jest zadawanie pytań, na które niewiele osób poza stroną uprawnioną znałoby poprawne odpowiedzi. W wielu przypadkach osoba, która może z powodzeniem odpowiedzieć „Ile wynosi Twoja obecna spłata kredytu hipotecznego?" i „Kto był Twoim nauczycielem przedmiotów ścisłych w siódmej klasie?" jest bardziej prawdopodobne, że będzie stroną autentyczną niż podszywającą się. Ale wszechwiedzący silnik Google podważa takie uwierzytelnianie. Wiele informacji, które były trudne do szybkiego uzyskania jeszcze kilka lat temu, można teraz uzyskać niemal natychmiastowo za pomocą wyszukiwarki Google. W wielu przypadkach odpowiedzi na pytania zabezpieczające używane przez różne witryny internetowe w celu pomocy w uwierzytelnianiu użytkowników są dla przestępców „za jednym kliknięciem". Podczas gdy bardziej zaawansowane witryny mogą uznać, że odpowiedź na pytania bezpieczeństwa jest błędna, jeśli zostanie wprowadzona później niż kilka sekund po zadaniu pytania, większość witryn nie nakłada takich ograniczeń - co oznacza, że każdy, kto wie w jaki sposób korzystania z Google może osłabić wiele nowoczesnych systemów uwierzytelniania.

Śledzenie lokalizacji urządzeń mobilnych

Podobnie samo Google może korelować wszelkiego rodzaju dane, które uzyskuje z telefonów z systemem Android lub aplikacji Mapy i Waze - co prawdopodobnie oznacza od większości ludzi w zachodnim świecie. Oczywiście dostawcy innych aplikacji, które działają na milionach telefonów i którzy mają dostawców innych aplikacji działających na milionach telefonów i które mają uprawnienia dostępu do danych o lokalizacji, również mogą zrobić to samo. Każda strona, która śledzi, gdzie dana osoba się znajduje i jak długo się tam znajduje, mogła stworzyć bazę danych, którą można wykorzystać do różnych niecnych celów - w tym do podważania uwierzytelniania opartego na wiedzy, ułatwiania ataków socjotechnicznych, podważania poufności projekty i tak dalej. Nawet jeśli firma tworząca bazę danych nie ma złośliwych zamiarów, nieuczciwi pracownicy lub hakerzy, którzy uzyskują dostęp do bazy danych lub ją kradną, stanowią poważne zagrożenie. Takie śledzenie podważa również prywatność. Google wie na przykład, kto regularnie chodzi do placówki chemioterapii, gdzie ludzie śpią (dla większości osób czas snu to jedyny czas, w którym ich telefony w ogóle się nie ruszają przez wiele godzin) i różne inne informacje na podstawie których można dokonać wszelkiego rodzaju wrażliwych ekstrapolacji.

Obrona przed tymi napastnikami

Ważne jest, aby zrozumieć, że nie ma czegoś takiego jak 100-procentowe cyberbezpieczeństwo. Raczej adekwatne cyberbezpieczeństwo definiuje się poprzez zrozumienie, jakie zagrożenia istnieją, które z nich są odpowiednio ograniczane, a które trwają. Zabezpieczenia, które są wystarczające, aby chronić przed niektórymi zagrożeniami i napastnikami, są niewystarczające, aby chronić się przed innymi. To, co może wystarczyć na przykład do rozsądnej ochrony komputera domowego, może okazać się

zdecydowanie niewystarczające do ochrony serwera bankowości internetowej. To samo dotyczy zagrożeń opartych na tym, kto korzysta z systemu: Telefon komórkowy używany przez Prezydenta Stanów Zjednoczonych, na przykład do rozmów z doradcami, wymaga oczywiście lepszego zabezpieczenia niż telefon komórkowy używany przez przeciętnego szóstoklasistę.

Przeciwdziałanie zagrożeniom za pomocą różnych metod

Nie wszystkie zagrożenia wymagają uwagi, a nie wszystkie rodzaje ryzyka, które wymagają uwagi, wymagają rozwiązania w ten sam sposób. Możesz na przykład zdecydować, że zakup ubezpieczenia jest wystarczającą ochroną przed określonym ryzykiem lub że ryzyko jest tak mało prawdopodobne i / lub de minimis, że nie jest warte prawdopodobnego kosztu jego rozwiązania.

Z drugiej strony, czasami ryzyko jest tak duże, że osoba lub firma może całkowicie zrezygnować z określonego wysiłku, aby uniknąć związanego z nim ryzyka. Na przykład, jeśli koszt odpowiedniego zabezpieczenia małej firmy byłby konsekwentnie wyższy niż zysk, jaki firma osiągnęłaby bez zabezpieczenia, otwarcie sklepu może być w pierwszej kolejności nierozsądne.