Czym dokładnie jest cyberbezpieczeństwo?

Aby poprawić swoją zdolność do cyberbezpieczeństwa dla siebie i swoich bliskich, musisz zrozumieć, co oznacza cyberbezpieczeństwo, jakie powinny być Twoje cele w stosunku do cyberbezpieczeństwa i przed czym dokładnie się zabezpieczasz. Chociaż odpowiedzi na te pytania mogą początkowo wydawać się proste i jednoznaczne, nie są. Jak zobaczysz w tej części, odpowiedzi te mogą się znacznie różnić między ludźmi, oddziałami firmy, organizacjami, a nawet w ramach tego samego podmiotu w różnych momentach. Cyberbezpieczeństwo oznacza różne rzeczy dla różnych ludzi. Podczas gdy cyberbezpieczeństwo może wydawać się dość prostym terminem do zdefiniowania, w w rzeczywistości, z praktycznego punktu widzenia, oznacza to zupełnie różne rzeczy dla różnych ludzi w różnych sytuacjach, co prowadzi do bardzo różnych odpowiednich zasad, procedur i praktyk. Na przykład osoba, która chce chronić swoje konta w mediach społecznościowych przed przejęciem przez hakerów, jest bardzo mało prawdopodobne, aby przyjęła wiele podejść i technologii wykorzystywanych przez pracowników Pentagonu do zabezpieczenia niejawnych sieci. Zazwyczaj na przykład:

* Dla osób fizycznych cyberbezpieczeństwo oznacza, że ich dane osobowe nie są dostępne dla nikogo innego niż dla nich samych i innych osób przez nich upoważnionych, a ich urządzenia komputerowe działają poprawnie i są wolne od złośliwego oprogramowania.

* W przypadku właścicieli małych firm cyberbezpieczeństwo może obejmować zapewnienie, że dane karty kredytowej są odpowiednio chronione oraz że standardy bezpieczeństwa danych są odpowiednio wdrażane w rejestrach w punktach sprzedaży.

* W przypadku firm prowadzących działalność online cyberbezpieczeństwo może obejmować ochronę serwerów, z którymi niezaufane osoby z zewnątrz regularnie wchodzą w interakcje.

* W przypadku dostawców usług wspólnych cyberbezpieczeństwo może pociągać za sobą ochronę wielu centrów danych, w których znajduje się wiele serwerów, które z kolei obsługują wiele serwerów wirtualnych należących do wielu różnych organizacji.

* Dla rządu cyberbezpieczeństwo może obejmować ustanowienie różnych klasyfikacji danych, każda z własnym zestawem powiązanych przepisów, zasad, procedur i technologii.

Najważniejsze jest to, że chociaż słowo „cyberbezpieczeństwo" jest łatwe do zdefiniowania, praktyczne oczekiwania, które pojawiają się w umysłach ludzi, gdy słyszą to słowo, różnią się nieco. Technicznie rzecz biorąc, cyberbezpieczeństwo jest podzbiorem bezpieczeństwa informacji, który dotyczy systemów informacji i informacji, które przechowują i przetwarzają dane w formie elektronicznej, podczas gdy bezpieczeństwo informacji obejmuje bezpieczeństwo wszystkich form danych (na przykład zabezpieczanie pliku papierowego i szafki na dokumenty). To powiedziawszy, dziś wiele osób potocznie wymienia terminy, często odnosząc się do aspektów bezpieczeństwa informacji, które technicznie nie są częścią cyberbezpieczeństwa jako część tych ostatnich. Takie użycie wynika również z połączenia obu w wielu sytuacjach. Technicznie rzecz biorąc, na przykład, jeśli ktoś zapisuje hasło na kawałku papieru i zostawia go na biurku, gdzie inne osoby mogą je zobaczyć, zamiast umieszczać papier w sejfie lub sejfie, naruszył zasadę bezpieczeństwo informacji, nie cyberbezpieczeństwa, nawet jeśli jego działania mogą spowodować poważne konsekwencje cyberbezpieczeństwa.

Cyberbezpieczeństwo jest stale zmieniającym się celem

Chociaż ostateczny cel cyberbezpieczeństwa może z czasem niewiele się zmienić, zasady, procedury i technologie stosowane do jego osiągnięcia zmieniają się dramatycznie w miarę upływu lat. Na przykład wiele podejść i technologii, które były więcej niż wystarczające do ochrony danych cyfrowych

konsumentów w 1980 r., są dziś faktycznie bezwartościowe, albo dlatego, że nie są już praktyczne w użyciu, albo dlatego, że postęp technologiczny sprawił, że stały się one przestarzałe lub bezsilne. Tworząc pełną listę wszystkich postępów, jakie świat widział w ostatnich dziesięcioleciach, oraz tego, jak takie zmiany wpływają na cyberbezpieczeństwo w sposób praktycznie niemożliwy, możemy zbadać kilka kluczowych obszarów rozwoju i ich wpływ na wciąż ewoluujący charakter cyberbezpieczeństwa: zmiany technologiczne, model ekonomiczny zmiany i outsourcing.

Zmiany technologiczne

Zmiany technologiczne mają ogromny wpływ na cyberbezpieczeństwo. Pojawiają się nowe zagrożenia wraz z nowymi możliwościami i udogodnieniami zapewnianymi przez nowe oferty. W związku z tym, że pakt postępu technologicznego wciąż rośnie, rośnie również tempo nowych zagrożeń cyberbezpieczeństwa. Chociaż liczba takich zagrożeń stworzonych w ciągu ostatnich kilku dekad w wyniku nowych ofert jest zdumiewająca, obszary opisane w poniższych sekcjach mają nieproporcjonalny wpływ na cyberbezpieczeństwo.

Cyfrowe dane

W ciągu ostatnich kilku dziesięcioleci nastąpiły dramatyczne zmiany w istniejących technologiach, a także w stosunku do tych, którzy korzystają z takich technologii, jak to robią i do jakich celów. Wszystkie te czynniki wpływają na cyberbezpieczeństwo.

Rozważmy na przykład, że kiedy wielu dzisiejszych ludzi było dziećmi, kontrolowanie dostępu do danych w środowisku biznesowym oznaczało po prostu, że właściciel danych umieścił plik fizyczny zawierający informacje w zamkniętej szafce i przekazał klucz tylko osobom, które uznał za upoważniony personel i tylko wtedy, gdy poprosiły o klucz w godzinach pracy . Dla dodatkowego bezpieczeństwa mógł zlokalizować szafkę w biurze, które było zamknięte po godzinach pracy i które samo było w budynku, który był również zamknięty i zaniepokojony. Dzisiaj, przy cyfrowym przechowywaniu informacji, proste schematy archiwizacji i ochrony zostały zastąpione złożonymi technologiami, które muszą automatycznie uwierzytelniać użytkowników, którzy szukają danych z potencjalnie dowolnego miejsca w potencjalnie dowolnym czasie, określają, czy użytkownicy są upoważnieni do dostępu do określonej element lub zestaw danych i bezpiecznie dostarczaj odpowiednie dane - wszystko to jednocześnie zapobiegając wszelkim atakom na system obsługujący żądania danych, atakom na przesyłane dane oraz wszelkim kontrolom bezpieczeństwa chroniącym oba z nich. Ponadto przejście z komunikacji pisemnej na e-mail i czat przeniosło ogromne ilości poufnych informacji na serwery podłączone do Internetu. Podobnie przejście społeczeństwa z filmu na fotografię cyfrową i wideografię zwiększyło ryzyko cyberbezpieczeństwa. Niemal każde zrobione dziś zdjęcie i nagranie wideo jest przechowywane elektronicznie, a nie na filmie i negatywach - sytuacja, która umożliwiła przestępcom znajdującym się w dowolnym miejscu kradzież zdjęć ludzi i wyciek ich lub zatrzymanie cennego zdjęcia ludzi za pomocą oprogramowania ransomware. Fakt, że filmy i programy telewizyjne są teraz przechowywane i przesyłane elektronicznie, umożliwił również piratom ich kopiowanie i oferowanie masom - czasem za pośrednictwem stron internetowych zainfekowanych złośliwym oprogramowaniem.

Internet

Najbardziej znaczącym postępem technologicznym w zakresie wpływu cyberbezpieczeństwa było nadejście ery Internetu. Jeszcze kilkadziesiąt lat temu było niezrozumiałe, że hakerzy z całego świata mogą zakłócać działalność gospodarczą, manipulować wyborami lub ukraść miliard dolarów. Dzisiaj żadna znająca się na rzeczy osoba nie odrzuciłaby takich możliwości. Przed erą Internetu przeciętny haker miał niezwykle trudny do osiągnięcia zysków finansowych przez hakowanie. Pojawienie się

bankowości internetowej i handlu w latach 90. oznaczało jednak, że hakerzy mogli bezpośrednio ukraść pieniądze, towary i usługi - co oznaczało, że nie tylko hakerzy mogli szybko i łatwo zarabiać na swoich wysiłkach, ale także nieetyczni ludzie mieli silną motywację, aby wejść do świata cyberprzestępczość.

Kryptowaluta

Jednym z elementów tych zachęt było pojawienie się i rozpowszechnianie kryptowaluty w ciągu ostatniej dekady, a także innowacje, które dramatycznie zwiększyły potencjalny zwrot z inwestycji dla przestępców uczestniczących w cyberprzestępczości, jednocześnie zwiększając ich zdolność do zarabiania pieniędzy dzięki cyberprzestępczości i zwiększając ich możliwości aby to ukryć. Przestępcy w przeszłości mieli trudności z otrzymywaniem płatności, ponieważ konto, z którego ostatecznie wycofali pieniądze, często mogło być z nimi związane. Kryptowaluta skutecznie eliminowała takie ryzyko.

Mobilna siła robocza i powszechny dostęp

Nie tak wiele lat temu, w erze przed Internetem, było to niemożliwe aby hakerzy zdalnie uzyskiwali dostęp do systemów korporacyjnych, ponieważ sieci korporacyjne nie są połączone z żadnymi sieciami publicznymi i często nie mają możliwości telefonowania. Kierownicy w drodze często dzwonili do swoich asystentów, aby sprawdzali wiadomości i uzyskiwali niezbędne dane, gdy byli zdalnie. Łączność z Internetem stwarzała pewne ryzyko, ale początkowo zapory ogniowe nie pozwalały osobom spoza organizacji inicjować komunikację - więc z powodu błędnych konfiguracji i / lub błędów zapory większość systemów wewnętrznych pozostała stosunkowo odizolowana. Początek e-handlu i bankowości elektronicznej oznaczał oczywiście, że niektóre systemy produkcyjne musiały być osiągalne i możliwe do adresowania ze świata zewnętrznego, ale na przykład sieci pracowników zwykle pozostawały zazwyczaj odizolowane. Pojawienie się technologii zdalnego dostępu - zaczynając od usług takich jak Outlook Web Access i pcAnywhere, a kończąc na pełnej VPN i dostępie zbliżonym do VPN - całkowicie zmieniło grę.

Inteligentne urządzenia

Podobnie pojawienie się inteligentnych urządzeń i Internetu przedmiotów (wszechświat urządzeń, które nie są tradycyjnymi komputerami, ale które są podłączone do Internetu) - których rozprzestrzenianie się i ekspansja występują obecnie w zaskakującym tempie - oznacza niemożliwy do zhakowania półprzewodnikowy maszyny są szybko zastępowane urządzeniami, które mogą być potencjalnie kontrolowane przez hakerów w połowie świata.

Big Data

Chociaż duże zbiory danych pomagają w tworzeniu wielu technologii cyberbezpieczeństwa, stwarzają również możliwości dla atakujących. Na przykład poprzez powiązanie dużej ilości informacji o osobach pracujących dla organizacji przestępca może łatwiej niż wcześniej zidentyfikować idealne metody inżynierii społecznej w swojej organizacji lub zlokalizować i wykorzystać ewentualne luki w infrastrukturze organizacji. W rezultacie różne organizacje zostały skutecznie zmuszone do wprowadzenia wszelkiego rodzaju kontroli, aby zapobiec wyciekaniu informacji. Całe książki zostały napisane na temat wpływu postępu technologicznego. Należy przede wszystkim zrozumieć, że postęp technologiczny miał znaczący wpływ na bezpieczeństwo cybernetyczne, utrudniając zapewnienie bezpieczeństwa i podnosząc stawkę, gdy strony nie będą odpowiednio chronić swoich aktywów.

Zmiany społeczne

Różne zmiany w sposobie, w jaki ludzie zachowują się i wchodzą w interakcje, również miały duży wpływ na cyberbezpieczeństwo. Na przykład Internet pozwala ludziom z całego świata na interakcję w czasie rzeczywistym. Oczywiście ta interakcja w czasie rzeczywistym umożliwia także przestępcom na całym świecie zdalne popełnianie przestępstw. Ale pozwala także obywatelom krajów represyjnych i wolnych krajów komunikować się, stwarzając możliwości rozproszenia ciągłej propagandy wykorzystywanej jako usprawiedliwienie dla porażki totalitaryzmu w zapewnianiu jakości życia na równi ze światem demokratycznym. Jednocześnie zapewnia cyberwojennym rządom sprzecznych ze sobą możliwość przeprowadzania ataków za pośrednictwem tej samej sieci. Konwersja różnych systemów zarządzania informacjami z wersji papierowej na komputerową, z izolowanej na podłączoną do Internetu oraz z dostępnej tylko w biurze na dostęp z dowolnego smartfona lub komputera zmieniła dramatycznie równanie, jeśli chodzi o to, co hakerzy informacji mogą ukraść. Co więcej, w wielu przypadkach, w których takie konwersje ze względów bezpieczeństwa nie były początkowo wykonywane, presja wynikająca z oczekiwań współczesnych ludzi, że każdy kawałek danych będzie dla nich dostępny przez cały czas z dowolnego miejsca, zmusiła do wystąpienia takich konwersji, tworząc dodatkowe możliwości dla przestępców. Ku uciesze hakerów wiele organizacji, które w przeszłości mądrze chroniły poufne informacje pozostawiając offline, po prostu stracili możliwość korzystania z takich zabezpieczeń, jeśli chcą kontynuować działalność. Media społecznościowe również zmieniły świat informacji - ludzie przyzwyczaili się do dzielenia się o sobie znacznie bardziej niż kiedykolwiek wcześniej - często także z widownią znacznie większą niż wcześniej. Dzisiaj, ze względu na zmianę zachowań w tym zakresie, złoczyńcy z dowolnego miejsca zbierają listy przyjaciół, współpracowników i krewnych celu oraz ustalają mechanizmy komunikacji z tymi wszystkimi ludźmi. Podobnie, łatwiej niż kiedykolwiek wcześniej dowiedzieć się, z jakich technologii korzysta dana firma i do jakich celów, poznać harmonogramy podróży ludzi i poznać ich opinie na różne tematy lub upodobania w muzyce i filmach. Tendencja do zwiększonego udostępniania nadal trwa. Większość osób pozostaje ślepo nieświadoma, jak wiele informacji na ich temat żyje na komputerach podłączonych do Internetu i ile innych informacji na ich temat można ekstrapolować z wyżej wymienionych danych. Wszystkie te zmiany przełożyły się na przerażającą rzeczywistość: z powodu zmian społecznych złoczyńca może z łatwością przeprowadzić dziś znacznie większy, bardziej wyrafinowany atak inżynierii społecznej niż dziesięć lat temu.

Zmiany modelu ekonomicznego

Połączenie niemal całego świata pozwoliło Internetowi na ułatwienie innych trendów z ogromnymi konsekwencjami cyberbezpieczeństwa. Modele operacyjne, które kiedyś były nie do pomyślenia, takie jak amerykańska firma korzystająca z call center w Indiach i sklepu programistycznego na Filipinach, stały się podstawą wielu korporacji. Zmiany te jednak powodują wszelkiego rodzaju zagrożenia cyberbezpieczeństwa. W ciągu ostatnich 20 lat nastąpił ogromny wzrost outsourcingu różnych zadań, od lokalizacji, w których ich realizacja jest droższa, do regionów, w których można je wykonać przy znacznie niższych kosztach. Pomysł, że firma w Stanach Zjednoczonych może polegać przede wszystkim na programistach komputerowych w Indiach lub na Filipinach, lub że ktoś w Nowym Jorku, który chce uzyskać logo dla swojej firmy, może krótko przed pójściem spać zapłacić komuś w połowie świata 5,50 USD, aby je utworzyć i mieć logo w skrzynce odbiorczej e-maila natychmiast po przebudzeniu następnego ranka, brzmiałoby jak science-fiction przed pokoleniem. Dzisiaj jest nie tylko powszechny, ale także w wielu przypadkach, jest bardziej powszechny niż jakakolwiek inna metoda uzyskiwania podobnych wyników. Oczywiście skutkuje to wieloma konsekwencjami cyberbezpieczeństwa.

Przesyłane dane muszą być chronione przed zniszczeniem, modyfikacją i kradzieżą oraz potrzebna jest większa pewność, że tylne drzwi nie są celowo lub przypadkowo wstawiane do kodu. Potrzebne są większe zabezpieczenia, aby zapobiec kradzieży własności intelektualnej i innym formom szpiegostwa

korporacyjnego. Hakerzy niekoniecznie muszą już bezpośrednio naruszać organizacje, które chcą włamać; muszą jedynie narazić na szwank jednego lub więcej dostawców, którzy mogą być znacznie mniej ostrożni w zakresie bezpieczeństwa informacji i praktyk personelu niż ostateczny cel.

Zmiany polityczne

Podobnie jak w przypadku postępu technologicznego, zmiany polityczne miały ogromne reperkusje dla cyberbezpieczeństwa, z których niektóre wydają się być stałym elementem nagłówków wiadomości. Połączenie siły rządowej i potężnej technologii często okazało się kosztowne dla obywateli. Jeżeli utrzymają się obecne trendy, wpływ różnych zmian politycznych na bezpieczeństwo cybernetyczne będzie się zwiększał tylko w dającej się przewidzieć przyszłości.

Zbieranie danych

Rozpowszechnianie informacji w Internecie i możliwość atakowania maszyn na całym świecie sprawiły, że rządy mogą szpiegować obywateli swoich krajów i mieszkańców innych narodów w stopniu, w jakim nigdy wcześniej nie było to możliwe. Co więcej, ponieważ coraz więcej działalności biznesowych, osobistych i społecznych pozostawia po sobie cyfrowy ślad, rządy mają łatwy dostęp do znacznie większej ilości informacji o swoich potencjalnych celach wywiadowczych, niż mogliby uzyskać nawet znacznie wyższymi kosztami zaledwie kilka lat temu. W połączeniu ze stosunkowo niskim kosztem cyfrowej pamięci masowej, rozwojem technologii dużych zbiorów danych i oczekiwaną ostateczną impotencją wielu dzisiejszych technologii szyfrowania, rządy mają silną motywację do gromadzenia i przechowywania jak największej liczby danych o jak największej liczbie osób , na wypadek, gdyby był używany w późniejszym terminie. Nie ma wątpliwości, że niektóre rządy już to robią. Długookresowe konsekwencje tego zjawiska są, jak dotąd, nieznane, ale jedno jest jasne: jeśli firmy nie będą odpowiednio chronić danych, narody mało przyjazne są skłonne je uzyskać i przechowywać w celu wykorzystania krótkookresowo, długoterminowo lub jedno i drugie.

Zakłócenia wyborcze

Pokolenie temu jeden naród ingerujący w wybory innego nie był banalną sprawą. Oczywiście taka ingerencja istniała - zdarzała się tak długo, jak były wybory - ale przeprowadzanie znaczących kampanii ingerujących było kosztowne, wymagające dużych zasobów i ryzykowne. Aby rozpowszechniać dezinformację i inną propagandę, materiały musiały być drukowane i fizycznie dystrybuowane lub rejestrowane i przesyłane drogą radiową, co oznacza, że pojedyncze kampanie mogły dotrzeć do niewielkiej grupy odbiorców. Jako takie, efekty skuteczności takich wysiłków były często dość niskie, a ryzyko narażenia partii prowadzącej kampanię było stosunkowo wysokie. Manipulowanie bazami danych rejestrujących wyborców, aby uniemożliwić głosowanie uprawnionym wyborcom i / lub umożliwić fałszywym wyborcom głosowanie, było niezwykle trudne i wiązało się z ogromnym ryzykiem; ktoś „pracujący od wewnątrz" musiałby być zdrajcą. W kraju takim jak Stany Zjednoczone, w którym bazy danych rejestrujących wyborców są zdecentralizowane i zarządzane na poziomie hrabstwa, rekrutacja wystarczającej liczby sabotażystów, aby naprawdę wpłynąć na wielkie wybory, byłaby prawdopodobnie niemożliwa, a szanse na złapanie podczas próby byłyby niemożliwe. prawdopodobnie bardzo wysoki. Podobnie w erze papierowych kart do głosowania i ręcznego liczenia, obce mocarstwo manipulujące faktyczną liczbą głosów na dowolną dużą skalę było praktycznie niemożliwe. Dziś jednak gra się zmieniła. Rząd może łatwo rozpowszechniać dezinformacje za pośrednictwem mediów społecznościowych przy wyjątkowo niskich kosztach. Jeśli opracuje przemyślaną kampanię, może polegać na innych ludziach w rozpowszechnianiu dezinformacji - czegoś, czego ludzie nie mogliby masowo robić w erze nagrań radiowych i broszur drukowanych. Zdolność dotarcia do znacznie większej liczby osób, przy znacznie niższych kosztach niż kiedykolwiek wcześniej, oznacza, że więcej partii może ingerować w kampanie polityczne i może to robić z większą

skutecznością niż w przeszłości. Podobnie rządy mogą rozpowszechniać dezinformacje, aby wzbudzić niezadowolenie społeczne u swoich przeciwników i szerzyć wrogość między grupami etnicznymi i religijnymi zamieszkującymi obce ziemie. Dzięki bazom danych rejestrujących wyborców przechowywanym elektronicznie, a czasem na serwerach, które są przynajmniej pośrednio podłączone do Internetu, zapisy mogą być dodawane, modyfikowane lub usuwane z połowy świata bez wykrycia. Nawet jeśli takie hakowanie jest w rzeczywistości niemożliwe, fakt, że wielu obywateli uważa, że jest to możliwe, doprowadził do podważenia wiary w wybory, zjawiska, którego byliśmy świadkami w ostatnich latach i które przeniknęło wszystkie poziomy społeczeństwo.

Nawet Jimmy Carter, były prezydent Stanów Zjednoczonych, wyraził przekonanie, że pełne śledztwo w wyborach prezydenckich w 2016 r. wykazałoby, że Donald Trump przegrał wybory - mimo że nie ma absolutnie żadnych dowodów na poparcie takiego wniosku, nawet po dokładne dochodzenie FBI w tej sprawie. Nietrudno też wyobrazić sobie, że gdyby kiedykolwiek odbyło się głosowanie online, potencjał manipulacji głosami przez zagraniczne rządy, przestępców, a nawet partie polityczne w głosowaniu narodowym - oraz usunięcie istniejącej dziś kontroli głosowania - wzrosłoby astronomicznie. Niespełna dziesięć lat temu Stany Zjednoczone nie uznały systemów komputerowych związanych z wyborami za infrastrukturę krytyczną i nie zapewniły federalnych funduszy bezpośrednio na zabezpieczenie takich systemów. Dzisiaj większość ludzi rozumie, że potrzeba bezpieczeństwa cybernetycznego w takich obszarach ma ogromne znaczenie, a polityka i zachowanie sprzed kilku lat wydaje się niczym szalonym.

Hacktavism

Podobnie rozprzestrzenianie się demokracji od czasu rozpadu Związku Radzieckiego przed pokoleniem, w połączeniu z interakcjami internetowymi między ludźmi na całym świecie, zapoczątkowało erę haktywizmu. Ludzie są świadomi tego, co dzieje się w większej liczbie miejsc niż w przeszłości. Hakerzy wściekli na niektóre polityki lub działania rządu w niektórych lokalizacjach mogą atakować ten rząd lub obywateli kraju, nad którym rządzi z odległych miejsc.

Większa wolność

Jednocześnie represjonowani ludzie są teraz bardziej świadomi stylu życia ludzi w bardziej wolnych i zamożnych krajach, zjawisko to zmusiło niektóre rządy do liberalizacji, a inne zmotywowały do wprowadzenia kontroli typu cyberbezpieczeństwa, aby zapobiec korzystaniu z różnych internetowych usługi.

Sankcje

Innym politycznym następstwem cyberbezpieczeństwa są sankcje międzynarodowe: zbuntowane państwa podlegające takim sankcjom były w stanie wykorzystać cyberprzestępczość różnych form w celu obejścia sankcji. Na przykład uważa się, że Korea Północna rozpowszechnia złośliwe oprogramowanie, które wydobywa kryptowalutę dla państwa totalitarnego na komputery na całym świecie, umożliwiając w ten sposób obejście sankcji poprzez uzyskanie płynnych pieniędzy, które można łatwo wydać w dowolnym miejscu. W 2019 r. Brak odpowiedniego zabezpieczenia komputerów osobistych przez osoby fizyczne może bezpośrednio wpłynąć na negocjacje polityczne.

Tworzenie nowej równowagi sił

Podczas gdy siły zbrojne niektórych narodów już dawno stały się potężniejsze niż siły ich przeciwników - zarówno jakość, jak i ilość broni różnią się znacznie między narodami - jeśli chodzi o cyberbezpieczeństwo, równowaga sił jest zupełnie inna. Chociaż jakość cyberbroni może się różnić w poszczególnych krajach, fakt, że uruchomienie cyberataków kosztuje niewiele, oznacza, że wszystkie wojska mają skutecznie nieograniczoną podaż używanej przez siebie broni. W rzeczywistości w

większości przypadków uruchomienie milionów cyberataków kosztuje niewiele więcej niż uruchomienie tylko jednego. Ponadto, w przeciwieństwie do świata fizycznego, w którym każdy naród, który bombardował domy cywilne na terytorium swojego przeciwnika, może spotkać się z surowymi represjami, nieuczciwe rządy regularnie hakują bezkarnie ludzi w innych krajach. Ofiary często nie zdają sobie sprawy, że zostały narażone na szwank, rzadko zgłaszają takie incydenty organom ścigania, a na pewno nie wiedzą, kogo winić. Nawet gdy ofiara zda sobie sprawę, że doszło do naruszenia, a nawet gdy eksperci techniczni wskażą napastników jako winowajców, państwa stojące za takimi atakami często cieszą się prawdopodobną zaprzeczeniem, uniemożliwiając jakiemukolwiek rządowi publiczny odwet. W rzeczywistości trudność w ustaleniu źródła cyberataków w połączeniu z elementem prawdopodobnej zaprzeczenia stanowi silną zachętę dla rządów do wykorzystywania cyberataków jako mechanizmu proaktywnego atakowania przeciwnika, siejącego różne formy spustoszenia bez obawy o znaczne represje. Co więcej, świat cyberbezpieczeństwa stworzył ogromną nierównowagę między atakującymi i obrońcami, co działa na korzyść słabszych narodów. Rządy, które nigdy nie mogłyby sobie pozwolić na uruchomienie ogromnych zapór przeciw przeciwnikowi w świecie fizycznym, mogą to łatwo zrobić w świecie cybernetycznym, gdzie uruchomienie każdego ataku kosztuje prawie nic. W rezultacie atakujący mogą sobie pozwolić na kontynuowanie ataku, dopóki nie odniesie sukcesu - i tylko raz muszą złamać systemy, aby „odnieść sukces" - tworząc ogromny problem dla obrońców, którzy muszą chronić swoje aktywa przed każdym atakiem. Ta nierównowaga przełożyła się na dużą przewagę atakujących nad obrońcami i oznaczała, że nawet niewielkie potęgi mogą skutecznie naruszać systemy należące do supermocarstw. W rzeczywistości ta nierównowaga przyczynia się do tego, że naruszenia bezpieczeństwa cybernetycznego zdają się występować tak często, ponieważ wielu hakerów po prostu atakuje, dopóki im się nie uda. Jeśli organizacja skutecznie obroni się przed 10 milionami ataków, ale nie zdoła powstrzymać 10 000 0001, może ponieść poważne naruszenie i przekazać wiadomości.

Raporty o naruszeniu prawdopodobnie nawet nie wspominają o tym, że ma 99,999999 procent skuteczności w zakresie ochrony swoich danych i że skutecznie powstrzymał atakujących milion razy z rzędu. Podobnie, jeśli firma zainstalowała 99,999 procent łatek, które powinna była zaniedbać, aby naprawić jedną znaną lukę, prawdopodobnie ucierpi z powodu liczby exploitów dostępnych przestępcom. Media informują o tym, że organizacja nie dokonała prawidłowej łatki, pomijając jej prawie doskonały wynik w tym obszarze. W związku z tym era cyberprzestrzeni zmieniła także równowagę sił między przestępcami a organami ścigania. Przestępcy wiedzą, że szanse na złapanie i udane ściganie za cyberprzestępczość są znacznie mniejsze niż w przypadku większości innych przestępstw, a powtarzające się nieudane próby przeprowadzenia cyberprzestępczości nie są receptą na pewne aresztowania, jak w przypadku większości innych przestępstw. Są również świadomi, że organy ścigania nie mają środków na ściganie zdecydowanej większości cyberprzestępców. Wyśledzenie, aresztowanie i skuteczne ściganie osoby kradnącej dane z połowy świata za pośrednictwem licznych przeskoków w wielu krajach i sieci komputerów na przykład dowodzona przez osoby przestrzegające prawa, wymaga zebrania i przeznaczenia znacznie większej ilości zasobów niż złapanie złodzieja, który został nagrany kamerą podczas trzymania w sklepie w lokalnej komisariacie policji. Dzięki niskim kosztom przeprowadzania powtarzających się ataków, szansom na ostateczny sukces na ich korzyść, szansom na złapanie i ukaranie maleńkim, a także potencjalnym korzyściom rosnącym wraz ze zwiększoną cyfryzacją, przestępcy wiedzą, że cyberprzestępczość się opłaca, podkreślając powód, dla którego należy chronić siebie.

Patrząc na ryzyko, które łagodzi cyberbezpieczeństwo

Ludzie czasami tłumaczą powód, dla którego cyberbezpieczeństwo jest ważne jako „ponieważ zapobiega hakerom włamywania się do systemów i kradzieży danych i pieniędzy". Ale taki opis

dramatycznie nie docenia roli, jaką cyberbezpieczeństwo odgrywa w utrzymaniu nowoczesnego domu, biznesu, a nawet świata. W rzeczywistości na rolę cyberbezpieczeństwa można spojrzeć z różnych punktów widzenia, z których każdy przedstawia inny zestaw celów. Oczywiście poniższe listy nie są kompletne, ale powinny dostarczać do myślenia i podkreślać znaczenie zrozumienia, w jaki sposób zabezpieczyć siebie i swoich bliskich przed cyberbezpieczeństwem.

Cel cyberbezpieczeństwa: triada CIA

Specjaliści ds. Cyberbezpieczeństwa często wyjaśniają, że celem cyberbezpieczeństwa jest zapewnienie poufności, integralności i dostępności (CIA) danych, czasami nazywanych triadą CIA, z grą z miłością:

* Poufność oznacza, że informacje nie zostaną ujawnione ani w żaden inny sposób udostępnione nieupoważnionym podmiotom (w tym osobom, organizacjom lub procesom komputerowym). Nie myl poufności z prywatnością: Poufność to podzbiór sfery prywatności. Dotyczy to w szczególności ochrony danych przed nieuprawnionymi przeglądającymi, podczas gdy prywatność ogólnie obejmuje znacznie więcej. Hakerzy kradnący dane podważają poufność.

* Integralność odnosi się do zapewnienia, że dane są zarówno dokładne, jak i kompletne. Dokładność oznacza na przykład, że dane nigdy nie są modyfikowane w jakikolwiek sposób przez osobę nieupoważnioną lub przez usterkę techniczną. Kompletne odnosi się na przykład do danych, które nie zostały usunięte przez żadną nieupoważnioną osobę lub usterkę techniczną. Uczciwość obejmuje również zapewnienie niezaprzeczalności, co oznacza, że dane są tworzone i przetwarzane w taki sposób, że nikt nie może racjonalnie twierdzić, że dane nie są autentyczne lub niedokładne. Cyberataki, które przechwytują dane i modyfikują je przed przekazaniem ich do miejsca docelowego - czasami znanego jako ataki typu man-in-the-middle - podważają integralność.

* Dostępność odnosi się do zapewnienia, że informacje, systemy używane do ich przechowywania i przetwarzania, mechanizmy komunikacyjne używane do uzyskania dostępu i przekazywania, a wszystkie związane z tym środki kontroli bezpieczeństwa działają poprawnie, aby spełnić określone kryteria (na przykład 99,99 procent czasu sprawności). Ludzie spoza obszaru bezpieczeństwa cybernetycznego czasami uważają dostępność za drugi aspekt bezpieczeństwa informacji po poufności i integralności. W rzeczywistości zapewnienie dostępności jest integralną częścią cyberbezpieczeństwa. Takie postępowanie jest jednak czasami trudniejsze niż zapewnienie poufności lub integralności. Jednym z powodów tego jest prawda ,że utrzymywanie dostępności często wymaga zaangażowania o wiele większej liczby specjalistów niezwiązanych z bezpieczeństwem, co prowadzi do wyzwania typu „zbyt wielu kucharzy w kuchni", szczególnie w większych organizacjach. Rozpowszechniane ataki typu „odmowa usługi" mają na celu podważenie dostępności. Weź również pod uwagę, że ataki często wykorzystują dużą liczbę skradzionej mocy komputera i przepustowości, aby przeprowadzić ataki DDoS, ale osoby odpowiadające, które chcą zapewnić dostępność, mogą wykorzystać jedynie stosunkowo niewielką ilość zasobów, na które mogą sobie pozwolić.

Z ludzkiej perspektywy

Ryzyko, które rozwiązuje cyberbezpieczeństwo, można również rozpatrywać w kategoriach lepiej odzwierciedlających ludzkie doświadczenia:

* Ryzyko związane z prywatnością: ryzyko wynikające z potencjalnej utraty odpowiedniej kontroli lub niewłaściwego wykorzystania danych osobowych lub innych poufnych informacji.

* Ryzyko finansowe: ryzyko strat finansowych spowodowanych włamaniem. Straty finansowe mogą obejmować zarówno te, które są bezpośrednie - na przykład kradzież pieniędzy z czyjegoś konta

bankowego przez hakera, który włamał się na konto - oraz straty pośrednie, takie jak utrata klientów, którzy nie ufają już małej firmie po ten drugi doznał naruszenia bezpieczeństwa.

* Ryzyko zawodowe: Ryzyko związane z karierą zawodową wynikające z naruszeń. Oczywiście specjaliści ds. bezpieczeństwa cybernetycznego są narażeni na ryzyko utraty kariery, jeśli dojdzie do naruszenia pod ich nadzorem i zostanie ustalone, że nastąpiło z powodu zaniedbania, ale inne typy specjalistów mogą również ponieść szkodę zawodową z powodu naruszenia. Dyrektorzy na poziomie C mogą być zwolnieni, członkowie zarządu mogą być pozwani, i tak dalej. Szkody zawodowe mogą również wystąpić, jeśli hakerzy udostępnią prywatną komunikację lub dane, które pokazują kogoś w złym świetle - na przykład dowodzą, że dana osoba została ukarana za niewłaściwe działanie, wysłała wiadomość e-mail zawierającą nieodpowiednie materiały i tak dalej.

* Ryzyko biznesowe: Ryzyko dla firmy podobne do ryzyka zawodowego dla osoby fizycznej. Dokumenty wewnętrzne wyciekły po naruszeniu Sony Pictures, które odmalowały różne firmy w negatywnym świetle w stosunku do niektórych praktyk kompensacyjnych.

* Ryzyko osobiste: wiele osób przechowuje prywatne informacje na swoich urządzeniach elektronicznych, od wyraźnych zdjęć po zapisy uczestnictwa w działaniach, które nie mogą być uznane przez członków ich kręgów społecznych za godne szacunku. Takie dane mogą czasem wyrządzić znaczną szkodę osobistym relacjom, jeśli zostaną ujawnione. Podobnie, skradzione dane osobowe mogą pomóc przestępcom w kradzieży tożsamości ludzi, co może powodować różnego rodzaju problemy osobiste.