Ocena aktualnej postawy w zakresie cyberbezpieczeństwa

Pierwszym krokiem do poprawy ochrony przed cyberzagrożeniami jest zrozumieć dokładnie, co musisz chronić. Dopiero po dokładnym zrozumieniu tych informacji możesz ocenić, co jest faktycznie potrzebne do zapewnienia odpowiedniego zabezpieczenia i określić, czy masz jakieś luki do usunięcia. Musisz wziąć pod uwagę, jakie masz dane, przed kim musisz je chronić i jak wrażliwe są one dla Ciebie. Co by się stało, gdyby na przykład została opublikowana w Internecie, aby świat mógł ją zobaczyć? Następnie możesz ocenić, ile jesteś gotów wydać - czasowo i finansowo - na jej ochronę.

Identyfikowanie sposobów, w jakie możesz być mniej niż bezpieczny

Musisz zrozumieć różne obszary, w których może ucierpieć Twoja obecna sytuacja w zakresie cyberbezpieczeństwa, aby dowiedzieć się, jak rozwiązać problemy i zapewnić sobie odpowiednią ochronę. Musisz spisać wszystkie przedmioty, które mogą zawierać poufne dane, stać się wyrzutniami do ataków i tak dalej.

Twój domowy komputer (y)

Twoje domowe komputery mogą cierpieć z powodu jednego lub głównych rodzajów potencjalnych problemów związanych z cyberbezpieczeństwem:

* Naruszenie: haker mógł przeniknąć do twojego domowego komputera i móc z niego korzystać tak często, jak tylko możesz - przeglądaj jego zawartość, używaj go do kontaktowania się z innymi maszynami, wykorzystuj go jako bazę wypadową do ataku na inne maszyny i penetruj je, wydobywaj kryptowaluty, przeglądaj dane w Twojej sieci i tak dalej.

* Złośliwe oprogramowanie: podobnie jak niebezpieczeństwa stwarzane przez ludzi, atakujący komputerowy - czyli złośliwe oprogramowanie - może znajdować się na Twoim komputerze domowym, umożliwiając przestępcy korzystanie z komputera tak samo jak Ty może - przeglądać zawartość komputera, kontaktować się z innymi maszynami, wydobywać kryptowaluty itp. - a także czytać dane z ruchu sieciowego i infekować inne komputery w sieci i poza nią.

* Współdzielone komputery: gdy dzielisz komputer z innymi osobami - w tym ze swoją bliską osobą i dziećmi - narażasz swoje urządzenie na ryzyko, że inne osoby, które go używają, nie będą ćwiczyć odpowiedniej higieny cybernetycznej na tym samym poziomie, co Ty i w rezultacie narazić urządzenie na infekcję złośliwym oprogramowaniem lub włamanie ze strony hakera lub nieumyślnie zadają sobie obrażenia.

* Połączenia z innymi sieciami i aplikacjami do przechowywania danych: jeśli łączysz swój komputer za pośrednictwem wirtualnej sieci prywatnej (VPN) z innymi sieciami, takie jak sieć w miejscu pracy, złośliwe oprogramowanie przenoszone przez sieć w tych zdalnych sieciach lub hakerzy czający się na urządzeniach podłączonych do tych sieci mogą potencjalnie zaatakować również Twoją sieć i urządzenia lokalne. W niektórych przypadkach podobne zagrożenia mogą występować w przypadku uruchamiania aplikacji, które łączą komputer z usługami zdalnymi, takimi jak zdalne systemy magazynowania.

* Fizyczne zagrożenia bezpieczeństwa: jak omówiono szczegółowo w rozdziale 5, fizyczna lokalizacja komputera może stanowić zagrożenie dla niego i jego zawartości.

Twoje urządzenia mobilne

Z punktu widzenia bezpieczeństwa informacji urządzenia mobilne są z natury ryzykowne, ponieważ one same :

* Są stale połączeni z niezabezpieczonym Internetem

* Często przechowują na nich poufne informacje

* Są używane do komunikowania się z wieloma osobami i systemami, z których oba są grupami obejmującymi strony, które nie zawsze są godne zaufania, przez Internet (który również z natury nie jest godny zaufania)

* Może odbierać wiadomości przychodzące od stron, z którymi nigdy nie kontaktowałeś się przed otrzymaniem wiadomości, o których mowa

* Często nie uruchamiaj pełnego oprogramowania zabezpieczającego ze względu na ograniczenia zasobów

* Można go łatwo zgubić, ukraść lub przypadkowo uszkodzić lub zniszczyć

* Połącz się z niezabezpieczonymi i niezaufanymi sieciami Wi-Fi

Twoje systemy do gier

Systemy gier to komputery, które, podobnie jak komputery, mogą być czasami wykorzystywane do różnych nikczemnych celów, a nie tylko do psot związanych z grą. Jeśli na przykład urządzenia zawierają luki w oprogramowaniu, mogą zostać zhakowane i przejęte, a oprogramowanie inne niż system gier może być na nich potencjalnie uruchomione.

Twoje urządzenia Internetu rzeczy (IoT)

Jak szczegółowo omówimy później, świat połączonych komputerów zmienił się dramatycznie w ostatnich latach. Jeszcze nie tak dawno jedynymi urządzeniami podłączonymi do internetu były klasyczne komputery - komputery stacjonarne, laptopy i serwery, które można było wykorzystać do wielu różnych celów obliczeniowych, ale dziś żyjemy w innym świecie. Od smartfonów po kamery bezpieczeństwa, lodówki po samochody i ekspresy do kawy po sprzęt do ćwiczeń - urządzenia elektroniczne wszelkiego typu mają teraz wbudowane komputery, a wiele z tych komputerów jest na stałe podłączonych do Internetu. Internet rzeczy (IoT), jako powszechnie znany ekosystem podłączonych urządzeń, rozwijał się wykładniczo w ciągu ostatnich kilku lat, jednak bezpieczeństwo takich urządzeń jest często niewystarczające. Wiele urządzeń IoT nie zawiera odpowiedniej technologii zabezpieczającej, która chroniłaby się przed naruszeniami. Nawet te, które to robią, często nie są odpowiednio skonfigurowane pod kątem bezpieczeństwa. Hakerzy mogą wykorzystywać urządzenia IoT do szpiegowania Cię, kradzieży danych, hakowania lub przeprowadzania ataków typu „odmowa usługi” na inne urządzenia oraz wyrządzania różnych innych szkód.

Twój sprzęt sieciowy

Hakerzy mogą wykorzystywać urządzenia IoT do szpiegowania Cię, kradzieży danych, hakowania lub przeprowadzania ataków typu „odmowa usługi” na inne urządzenia oraz wyrządzania różnych innych szkód.

Twój sprzęt sieciowy

Sprzęt sieciowy może zostać zhakowany w celu kierowania ruchu do fałszywych witryn, przechwytywania danych, przeprowadzania ataków, blokowania dostępu do Internetu i tak dalej.

Twoje środowisko pracy

Możesz mieć wrażliwe dane w swoim środowisku pracy - i możesz być również narażony na ryzyko przez współpracowników. Na przykład, jeśli przyniesiesz jakiekolwiek urządzenia elektroniczne do pracy, podłączysz je do sieci w pracy, a następnie przyniesiesz te urządzenia do domu i połączysz je z siecią domową, złośliwe oprogramowanie i inne problemy mogą potencjalnie rozprzestrzenić się na Twoje urządzenie z urządzenia należącego do Ciebie. pracodawca lub do jednego lub więcej twoich kolegów korzystających z tej samej infrastruktury, a następnie rozprzestrzenianie się z twojego urządzenia na inne maszyny w twojej sieci domowej.

Inżynieria społeczna

Każda osoba w Twojej rodzinie i kręgu społecznym stanowi dla Ciebie zagrożenie jako źródło informacji o Tobie, które mogą być potencjalnie wykorzystane do celów inżynierii społecznej.

Identyfikacja zagrożeń

Aby cokolwiek zabezpieczyć, musisz wiedzieć, co zabezpieczasz; Zabezpieczenie środowiska jest trudne, jeśli nie niemożliwe, jeśli nie wiesz, co się w nim znajduje. Dlatego, aby się zabezpieczyć, musisz zrozumieć, jakie zasoby - zarówno te w formatach cyfrowych, jak i w powiązanych formatach fizycznych - posiadasz, i co chcesz chronić. Musisz również zrozumieć, jakie ryzyko napotykasz na te aktywa. Inwentaryzacja takich aktywów jest zwykle dość prosta dla osób fizycznych:

Zrób pisemną listę wszystkich urządzeń, które podłączasz do swojej sieci. Często możesz uzyskać listę, logując się do routera i przeglądając sekcję Połączone urządzenia. Oczywiście możesz mieć urządzenia, które łączysz się z siecią tylko sporadycznie lub które muszą być zabezpieczone, nawet jeśli nie są podłączone do Twojej sieci, więc pamiętaj, aby uwzględnić je również na swojej liście. Dodaj do tej listy w osobnej sekcji - wszystkie używane urządzenia pamięci masowej, w tym zewnętrzne dyski twarde, dyski flash i karty pamięci. Napisz lub wydrukuj listę; zapomnienie choćby jednego urządzenia może prowadzić do problemów.

Ochrona przed zagrożeniami

Po określeniu, co należy chronić (patrz poprzednia sekcja), należy opracować i wdrożyć odpowiednie zabezpieczenia dla tych elementów, aby zapewnić ich odpowiednie bezpieczeństwo i ograniczyć wpływ potencjalnego naruszenia. W kontekście użytkowników domowych ochrona obejmuje zapewnienie barier każdemu, kto chce uzyskać dostęp do zasobów cyfrowych i fizycznych bez odpowiedniego upoważnienia, ustanowienie (nawet nieformalnych) procesów i procedur w celu ochrony poufnych danych oraz tworzenie kopii zapasowych wszystkich konfiguracji i podstawowych punkty przywracania systemu. Podstawowe elementy ochrony większości osób obejmują

* Obrona obwodowa

* Firewall / router

* Oprogramowanie zabezpieczające

* Twój fizyczny komputer (y)

*Utworzyć kopię zapasową

Obrona obwodowa

Obrona cyberprzestrzeni jest zasadniczo cyfrowym odpowiednikiem budowania fosy wokół zamku - próba powstrzymania nikogo przed wejściem poza dozwolonymi ścieżkami pod czujnym okiem strażników. Możesz zbudować tę cyfrową fosę, nigdy nie podłączając żadnego komputera

bezpośrednio do modemu internetowego. Zamiast tego podłącz zaporę / router do modemu i komputery do zapory / routera. (Jeśli twój modem zawiera zaporę / router, to służy obu celom; jeśli twoje połączenie jest z częścią firewall / router, a nie z samym modemem, to jest w porządku). Zwykle połączenia między zaporą a modemami są przewodowe - to znaczy jest osiągane za pomocą fizycznego kabla sieciowego.

Firewall / router

Nowoczesne routery używane w środowiskach domowych obejmują funkcje zapory ogniowej, które blokują większość form ruchu przychodzącego, gdy taki ruch nie jest generowany, i blokują większość form ruchu przychodzącego, gdy taki ruch nie jest generowany w wyniku działań zainicjowanych przez urządzenia chronione przez zaporę. Oznacza to, że zapora sieciowa będzie blokować osobom z zewnątrz próby skontaktowania się z komputerem w Twoim domu, ale nie będzie blokować odpowiedzi serwera WWW, jeśli komputer w domu zażąda strony internetowej z serwera. Routery wykorzystują wiele technologii do osiągnięcia takiej ochrony. Jedną z ważnych technologii wartych uwagi jest translacja adresów sieciowych, która umożliwia komputerom w sieci domowej korzystanie z adresów protokołu internetowego (IP), które są nieprawidłowe do użytku w Internecie i mogą być używane tylko w sieciach prywatnych. W Internecie wydaje się, że wszystkie urządzenia używają jednego adresu, czyli adresu zapory. Poniższe zalecenia pomogą routerowi / zaporze sieciowej chronić Cię:

* Dbaj o aktualność routera. Upewnij się, że zainstalowałeś wszystkie aktualizacje przed pierwszym uruchomieniem routera i regularnie sprawdzaj, czy są dostępne nowe aktualizacje (chyba że router ma funkcję automatycznej aktualizacji, w takim przypadku powinieneś skorzystać z tej funkcji).

* Niezałatana luka w routerze może umożliwić osobom postronnym wejście do Twojej sieci.

* Zmień domyślne hasło administracyjne swojej zapory / routera na silne hasło, które znasz tylko Ty. Zapisz go i umieść papier w sejfie lub skrytce depozytowej. Poćwicz logowanie się do routera - i rób to regularnie, aby nie zapomnieć hasła.

* Nie używaj domyślnej nazwy podanej przez router jako nazwy sieci Wi-Fi (jej identyfikatora SSID). Utwórz nową nazwę.

* Skonfiguruj swoją sieć Wi-Fi tak, aby korzystała z szyfrowania co najmniej w standardzie WPA2.

* Ustal hasło, które musi znać każde urządzenie, aby dołączyć do Twojej sieci Wi-Fi. Uczyń to hasło silnym.

* Jeśli wszystkie Twoje urządzenia bezprzewodowe wiedzą, jak korzystać z nowoczesnego standardu 802.11ac i protokoły sieci bezprzewodowej 802.11n, wyłącz starsze protokoły Wi-Fi obsługiwane przez router - na przykład 802.11b i 802.11g.

* Włącz filtrowanie adresów MAC lub upewnij się, że wszyscy domownicy wiedzą, że nikt nie może niczego podłączać do sieci przewodowej bez Twojej zgody. Przynajmniej w teorii filtrowanie adresów MAC zapobiega łączeniu się dowolnego urządzenia z siecią, jeśli wcześniej nie skonfigurowałeś routera, aby umożliwić mu połączenie - nie pozwalaj ludziom na podłączanie niezabezpieczonych urządzeń do sieci bez ich uprzedniego zabezpieczenia.

* Zlokalizuj router bezprzewodowy centralnie w swoim domu. Dzięki temu uzyskasz lepszy sygnał, a także zmniejszysz siłę sygnału, który dostarczasz osobom spoza domu, które mogą próbować połączyć się z Twoją siecią.

* Nie włączaj zdalnego dostępu do routera. Chcesz, aby routerem można było zarządzać tylko za pośrednictwem połączeń z urządzeń, które chroni, a nie ze świata zewnętrznego. Wygoda zdalnego zarządzania zaporą domową rzadko jest warta zwiększenia ryzyka związanego z bezpieczeństwem, jakie stwarza włączenie takiej funkcji.

* Utrzymuj aktualną listę urządzeń podłączonych do sieci. Uwzględnij także urządzenia, którym zezwalasz na łączenie się z siecią.

* Dla wszystkich gości, którym chcesz udzielić dostępu do sieci, włącz obsługę sieci gościa w routerze i, podobnie jak w przypadku sieci prywatnej, włącz szyfrowanie i wymagaj silnego hasła. Daj gościom dostęp do tej sieci gości, a nie do sieci podstawowej. To samo dotyczy wszystkich innych osób, którym musisz zapewnić dostęp do Internetu, ale których bezpieczeństwu nie w pełni nie ufasz, w tym członków rodziny, takich jak dzieci.

* Jeśli masz wystarczającą wiedzę techniczną, aby wyłączyć DHCP i zmienić domyślny zakres adresów IP używany przez router w sieci wewnętrznej, zrób to. Takie postępowanie koliduje z niektórymi zautomatyzowanymi narzędziami hakerskimi i zapewnia inne korzyści w zakresie bezpieczeństwa. Jeśli nie znasz takich pojęć lub nie masz pojęcia, co oznacza powyższe zdanie, po prostu zignoruj ten akapit. W takim przypadku korzyści bezpieczeństwa wynikające z zalecenia prawdopodobnie przeważą nad problemami, które możesz napotkać ze względu na dodatkową złożoność techniczną, którą może spowodować wyłączenie DHCP i zmiana domyślnego zakresu adresów IP.

Oprogramowanie zabezpieczające

Jak korzystać z oprogramowania zabezpieczającego, aby się chronić?

* Używaj oprogramowania zabezpieczającego na wszystkich komputerach i urządzeniach mobilnych. Oprogramowanie powinno zawierać co najmniej program antywirusowy i zaporę sieciową urządzeń osobistych możliwości.

* Używaj oprogramowania antyspamowego na dowolnym urządzeniu, na którym czytasz e-maile.

* Włącz zdalne czyszczenie na dowolnym urządzeniu mobilnym.

* Wymagaj silnego hasła, aby zalogować się do dowolnego komputera i urządzenia mobilnego.

* Włączaj automatyczne aktualizacje, gdy tylko jest to możliwe, i aktualizuj urządzenia.

Twój fizyczny komputer (y)

Aby fizycznie zabezpieczyć komputery:

* Kontroluj fizyczny dostęp do komputera i przechowuj go w bezpiecznym miejscu. Jeśli na przykład ktoś wchodzący do Twojego domu może dostać się do maszyny, urządzenie to może zostać stosunkowo łatwo skradzione, użyte lub uszkodzone bez twojej wiedzy.

* Jeśli to możliwe, nie udostępniaj swojego komputera członkom rodziny. Jeśli musisz udostępniać swój komputer, utwórz oddzielne konta dla każdego członka rodziny i nie nadawaj innym użytkownikom tego urządzenia uprawnień administracyjnych.

* Nie polegaj na usuwaniu danych przed wyrzuceniem, recyklingiem, przekazaniem lub sprzedażą starego urządzenia. Używaj wielościeżkowego systemu wymazywania dla wszystkich dysków twardych i dysków SSD. Najlepiej wyjąć nośnik pamięci z komputera przed pozbyciem się urządzenia - i fizycznie zniszczyć nośnik.

Utwórz kopię zapasową

Wykonuj regularnie kopie zapasowe

Wykrywanie

Wykrywanie oznacza wdrażanie mechanizmów, dzięki którym można wykrywać zdarzenia cyberbezpieczeństwa tak szybko, jak to możliwe po ich rozpoczęciu. Chociaż większość użytkowników domowych nie ma środków na zakup wyspecjalizowanych produktów w celu wykrywania, nie oznacza to, że należy ignorować fazę wykrywania zabezpieczeń. Obecnie większość programów zabezpieczających komputery osobiste ma różnego rodzaju możliwości wykrywania. Upewnij się, że każde urządzenie, którym zarządzasz, ma oprogramowanie zabezpieczające, które wyszukuje możliwe włamania, na przykład ...

Odpowiadam

Reagowanie oznacza działanie w odpowiedzi na incydent związany z cyberbezpieczeństwem. Większość programów zabezpieczających automatycznie zachęci użytkowników do podjęcia działań, jeśli wykryją potencjalne problemy.

Odzyskiwanie

Odzyskiwanie oznacza przywrócenie dotkniętego problemem komputera, sieci lub urządzenia - i wszystkich jego odpowiednich możliwości - do pełnego funkcjonowania, właściwego stanu po wystąpieniu zdarzenia związanego z cyberbezpieczeństwem. Idealnie byłoby, gdyby formalny plan z ustalonymi priorytetami dotyczący naprawy powinien zostać udokumentowany, zanim będzie potrzebny. Większość użytkowników domowych w rzeczywistości tego nie robi aby je utworzyć, ale może to być niezwykle korzystne. W większości domu taki plan będzie krótszy niż jedna strona.

Poprawa

Wstyd dla każdego, kto nie uczy się na własnych błędach. Każdy incydent cybernetyczny oferuje wyciągnięte wnioski, które można wykorzystać w celu zmniejszenia ryzyka w przyszłości. Przykłady uczenia się na błędach.

Ocena obecnych środków bezpieczeństwa

Gdy już wiesz, co musisz chronić i jak chronić takie przedmioty, możesz określić różnicę między tym, czego potrzebujesz, a tym, co aktualnie masz. W poniższych sekcjach omówiono kilka kwestii, które należy wziąć pod uwagę. Nie wszystkie ,w każdym przypadku obowiązują następujące zasady:

Oprogramowanie

Jeśli chodzi o oprogramowanie i cyberbezpieczeństwo, rozważ następujące pytania dla każdego urządzenia:

* Czy wszystkie pakiety oprogramowania (w tym sam system operacyjny) na komputerze zostały legalnie pozyskane i znane jako legalne wersje?

* Czy wszystkie pakiety oprogramowania (w tym sam system operacyjny) obecnie obsługiwane przez odpowiednich dostawców?

* Czy wszystkie pakiety oprogramowania (w tym sam system operacyjny) aktualny?

* Czy wszystkie pakiety oprogramowania (w tym sam system operacyjny) są ustawione na automatyczne aktualizowanie?

* Czy na urządzeniu jest oprogramowanie zabezpieczające?

* Czy oprogramowanie zabezpieczające jest skonfigurowane do automatycznej aktualizacji?

* Czy oprogramowanie zabezpieczające jest aktualne?

* Czy oprogramowanie zabezpieczające obejmuje technologię ochrony przed złośliwym oprogramowaniem i czy ta funkcja jest w pełni włączona?

* Czy skanowanie w poszukiwaniu wirusów jest skonfigurowane do uruchamiania po zastosowaniu każdej aktualizacji?

* Czy oprogramowanie zawiera technologię zapory - i czy to jest funkcja w pełni włączony?

* Czy oprogramowanie zawiera technologię antyspamową - i czy ta funkcja jest w pełni włączona? Jeśli nie, czy jest obecne inne oprogramowanie antyspamowe i czy jest ono uruchomione?

* Czy oprogramowanie obejmuje technologię zdalnego blokowania i / lub zdalnego czyszczenia - i czy ta funkcja jest w pełni włączona? Jeśli nie, to inny pilot oprogramowania blokującego / zdalne czyszczenie jest obecne i czy jest uruchomione?

* Czy wszystkie inne aspekty oprogramowania są włączone? Jeśli nie, co nie jest?

* Czy jest uruchomione oprogramowanie do tworzenia kopii zapasowych, które utworzy kopię zapasową urządzenia w ramach strategii tworzenia kopii zapasowych?

* Czy szyfrowanie jest włączone przynajmniej dla wszystkich poufnych danych przechowywanych na urządzeniu?

* Czy uprawnienia są odpowiednio ustawione dla oprogramowania - blokowanie osób, które mogą mieć dostęp do urządzenia, ale nie powinny mieć dostępu do oprogramowania?

* Czy ustawiono uprawnienia, aby uniemożliwić oprogramowaniu wprowadzanie zmian na komputerze, których nie chcesz robić (na przykład jest to oprogramowanie działające z uprawnieniami administratora, gdy nie powinno)

Oczywiście wszystkie te pytania dotyczą oprogramowania na urządzeniu, z którego korzystasz, ale którego nie udostępniasz do użytku niezaufanym, zdalnym osobom z zewnątrz. Jeśli masz urządzenia, które są używane tak jak w drugim przypadku - na przykład serwer WWW - musisz rozwiązać wiele innych problemów związanych z bezpieczeństwem

Sprzęt komputerowy

W przypadku wszystkich urządzeń sprzętowych rozważ następujące pytania:

* Czy sprzęt został uzyskany od zaufanej strony? (Jeśli kupiłeś kamerę internetową bezpośrednio z Chin w jakimś sklepie internetowym, o którym nigdy nie słyszałeś przed dokonaniem zakupu, na przykład odpowiedź na to pytanie może nie brzmieć tak.)

* Czy cały Twój sprzęt jest odpowiednio chroniony przed kradzieżą i uszkodzeniem (deszcz, wyładowania elektryczne itp.), Ponieważ znajduje się w miejscu zamieszkania?

* Co chroni Twój sprzęt podczas podróży?

* Czy masz zasilacz awaryjny lub wbudowaną baterię chroniącą urządzenie przed gwałtownym, nagłym wyłączeniem w przypadku awarii zasilania, nawet chwilowo?

* Czy cały Twój sprzęt ma najnowsze oprogramowanie sprzętowe - i czy pobrałeś je z wiarygodnego źródła, takiego jak dostawca witryny internetowej czy aktualizacja zainicjowana w narzędziu konfiguracyjnym urządzenia?

* W przypadku routerów (i zapór ogniowych), czy Twoje urządzenie spełnia kryteria wymienione jako zalecenia w sekcji „Zapora / router" ?

* Czy masz hasło BIOS, blokujące urządzenie przed użyciem bez wprowadzenia hasła?

* Czy wyłączyłeś wszystkie protokoły bezprzewodowe, których nie potrzebujesz? Jeśli na przykład nie używasz Bluetootha na laptopie, wyłącz radio Bluetooth, co nie tylko poprawia bezpieczeństwo, ale także wydłuża żywotność baterii.

Ubezpieczenie

Chociaż ubezpieczenie cyberbezpieczeństwa jest często pomijane, zwłaszcza przez mniejsze firmy i osoby prywatne, jest to realny sposób na złagodzenie niektórych zagrożeń cybernetycznych. W zależności od konkretnej sytuacji, zakup polisy chroniącej przed określonymi zagrożeniami może mieć sens.

Jeśli jesteś właścicielem małej firmy, która może zbankrutować, jeśli dojdzie do naruszenia, będziesz oczywiście chciał wdrożyć silne zabezpieczenia. Ale ponieważ żadne zabezpieczenia nie są w 100% doskonałe i niezawodne, zakup polisy obejmującej katastrofalne sytuacje może być rozsądny.

Edukacja

Odrobina edukacji może w dużym stopniu pomóc zapobiec staniu się piętami achillesowymi twojego gospodarstwa domowego przez ludzi w twoim gospodarstwie domowym. Poniższa lista zawiera kilka spraw do przemyślenia i omówienia:

* Czy wszyscy członkowie rodziny wiedzą, jakie są ich prawa i obowiązki związane z technologią w domu, z podłączaniem urządzeń do sieci domowej oraz z umożliwieniem gościom łączenia się z siecią domową (lub sieć gości)?

* Czy poinformowałeś członków swojej rodziny o zagrożeniach, o których muszą wiedzieć - na przykład wiadomościach phishingowych. Czy masz pewność, że „rozumieją"?

* Czy upewniłeś się, że wszyscy w rodzinie, którzy używają urządzeń, wiedzą o higienie cyberbezpieczeństwa (np. Nie klikają linków w e-mailach)?

* Czy upewniłeś się, że wszyscy członkowie rodziny korzystający z urządzeń wiedzą o wyborze hasła i ochronie?

* Czy upewniłeś się, że wszyscy w rodzinie korzystają z mediów społecznościowych , i każdy wie, co można, a czego nie można bezpiecznie udostępniać?

* Czy upewniłeś się, że wszyscy w rodzinie rozumieją koncepcję myślenia przed podjęciem działania?

Prywatność 101

Technologia zagraża prywatności na wiele sposobów: wszechobecne kamery regularnie Cię obserwują, firmy technologiczne śledzą Twoje zachowania online za pomocą różnego rodzaju metod technicznych, a urządzenia mobilne śledzą Twoją lokalizację. Chociaż technologia z pewnością znacznie utrudniła utrzymanie prywatności niż kilka lat temu, prywatność nie umarła. Możesz zrobić wiele rzeczy, aby poprawić swój poziom prywatności, nawet we współczesnej, połączonej erze.

Pomyśl, zanim udostępnisz

Ludzie często chętnie przekraczają udostępnianie informacji, gdy są o to proszeni. Weź pod uwagę dokumenty typowe dla gabinetu lekarskiego, o wypełnienie których prawdopodobnie zostałeś poproszony w więcej niż jednej placówce podczas pierwszej wizyty u danego lekarza. Chociaż odpowiedzi na wiele pytań są istotne i mogą zawierać informacje, które lekarz powinien znać, aby odpowiednio ocenić i leczyć, inne części prawdopodobnie nie są. Wiele (jeśli nie większość) takich formularzy wymaga podania numerów ubezpieczenia społecznego. Takie informacje były potrzebne dziesiątki lat temu, kiedy firmy ubezpieczeniowe zwykle używały numerów ubezpieczenia społecznego jako numerów identyfikacyjnych ubezpieczenia, ale praktyka ta już dawno się skończyła. Być może niektóre placówki używają numeru ubezpieczenia społecznego do zgłaszania konta do biur kredytowych, jeśli nie płacisz rachunków, ale w większości przypadków rzeczywistość jest taka, że pytanie to pozostałość po przeszłości i możesz pozostawić to pole puste . Nawet jeśli nie sądzisz, że strona prosząca Cię o dane osobowe kiedykolwiek nadużyłaby informacji, które zebrała na Twój temat, w miarę wzrostu liczby stron, które posiadają prywatne informacje o Tobie, oraz w miarę wzrostu ilości i jakości tych danych, zwiększa się prawdopodobieństwo, że naruszysz prywatność z powodu naruszenia bezpieczeństwa danych. Jeśli chcesz poprawić swoją prywatność, pierwszą rzeczą do zrobienia jest rozważenie, jakie informacje o sobie i swoich bliskich możesz ujawniać, zanim je ujawnisz. Dzieje się tak podczas interakcji z agencjami rządowymi, korporacjami, placówkami medycznymi i innymi osobami. Jeśli nie musisz podawać prywatnych informacji, nie rób tego.

Pomyśl, zanim wyślesz

Rozważ konsekwencje każdego posta w mediach społecznościowych, zanim go opublikujesz - mogłoby to mieć wiele negatywnych konsekwencji, w tym skutecznie naruszyć prywatność informacji. Na przykład przestępcy mogą wykorzystywać wspólne informacje o relacjach rodzinnych, miejscu pracy i zainteresowaniach danej osoby w ramach kradzieży tożsamości i w celu inżynierii społecznej dostać się na Twoje konta. Jeśli z własnego wyboru lub z powodu niedbałych zasad dostawcy używasz nazwiska panieńskiego swojej matki jako hasła de facto, upewnij się, że nie ułatwiasz przestępcom znalezienia tego nazwiska, podając swoją matkę jako swoją matkę na Facebook lub poprzez przyjaźń na Facebooku z wieloma kuzynami, których nazwisko jest takie samo jak nazwisko panieńskie Twojej matki. Często można uzyskać nazwisko panieńskie matki po prostu wybierając z listy znajomych innej osoby na Facebooku najczęściej używane nazwisko, które nie jest takie samo jak nazwisko właściciela konta. Udostępnianie informacji o dzieciach danej osoby i jej harmonogramach może pomóc w rozwiązaniu różnego rodzaju problemów - w tym potencjalnego porwania, włamań do domu osoby, gdy jedzie do pracy, lub innych szkodliwych działań. Udostępnianie informacji związanych z działalnością medyczną może prowadzić do ujawnienia wrażliwych i prywatnych informacji. Na przykład zdjęcia lub dane dotyczące lokalizacji osoby w określonej placówce medycznej mogą ujawniać, że dana osoba cierpi na schorzenie, w leczeniu którego dana placówka specjalizuje się. Udostępnianie różnego rodzaju informacji lub obrazów może wpłynąć na osobiste relacje użytkownika i spowodować ujawnienie prywatnych informacji na ich temat. Udostępnianie informacji lub obrazów może powodować wyciek prywatnych informacji o potencjalnie kontrowersyjnych działaniach, w które dana osoba była zaangażowana - na przykład spożywanie alkoholu lub zażywanie narkotyków rekreacyjnych, używanie różnych broni, uczestnictwo w niektórych kontrowersyjnych organizacjach itp. Nawet ujawnienie, że ktoś był w określonej lokalizacji w określonym czasie, może nieumyślnie naruszyć prywatność poufnych informacji. Pamiętaj też, że problem nadmiernego udostępniania nie ogranicza się do sieci społecznościowych. Nadmierne udostępnianie informacji za pośrednictwem czatu, poczty e-mail, czatów grupowych itp. Jest również poważnym problemem współczesności. Czasami ludzie nie zdają

sobie sprawy, że nadmiernie udostępniają, a czasami przypadkowo wklejają niewłaściwe dane do wiadomości e-mail lub dołączają niewłaściwe pliki do wiadomości e-mail.

Ogólne wskazówki dotyczące prywatności

Oprócz przemyślenia przed udostępnieniem, możesz zrobić kilka innych rzeczy, aby zmniejszyć ryzyko nadmiernego udostępniania:

* Użyj ustawień prywatności mediów społecznościowych. Oprócz nieudostępniania informacji prywatnych, upewnij się, że ustawienia prywatności w mediach społecznościowych chronią Twoje dane przed przeglądaniem przez członków ogółu społeczeństwa - chyba że dane stanowisko jest przeznaczone do użytku publicznego.

* Ale nie polegaj na nich. Niemniej jednak nigdy nie polegaj na ustawieniach zabezpieczeń mediów społecznościowych, aby zapewnić prywatność informacji. Wielokrotnie odkrywano znaczące luki w zabezpieczeniach, które osłabiają skuteczność mechanizmów kontroli bezpieczeństwa różnych platform.

* Chroń prywatne dane przed chmurą, chyba że je zaszyfrujesz. Nigdy nie przechowuj prywatnych informacji w chmurze, chyba że je zaszyfrujesz. Nie polegaj na szyfrowaniu dostarczonym przez dostawcę chmury, aby zapewnić sobie prywatność. Jeśli dostawca zostanie naruszony, w niektórych przypadkach szyfrowanie może również zostać naruszone.

* Nie przechowuj prywatnych informacji w aplikacjach w chmurze przeznaczonych do udostępniania i współpracy. Na przykład nie przechowuj listy swoich haseł, zdjęć prawa jazdy lub paszportu ani poufnych informacji medycznych w dokumencie Google. Może się to wydawać oczywiste, ale wiele osób i tak to robi.

* Wykorzystaj ustawienia prywatności przeglądarki - lub jeszcze lepiej, użyj Tora. Jeśli używasz przeglądarki internetowej do uzyskiwania dostępu do materiałów, których nie chcesz z Tobą kojarzyć, włącz przynajmniej tryb prywatny / incognito (który zapewnia tylko częściową ochronę) lub, jeśli to możliwe, użyj przeglądarki internetowej, takiej jak Paczka Tora z przeglądarką (która zawiera zaciemniony routing, domyślne silne ustawienia prywatności i różne, wstępnie skonfigurowane dodatki do prywatności).

Jeśli nie podejmiesz środków ostrożności podczas korzystania z przeglądarki, możesz zostać śledzony. Jeśli szukasz szczegółowych informacji o stanie zdrowia w normalnym oknie przeglądarki różne strony prawdopodobnie wykorzystają te dane. Prawdopodobnie widziałeś efekty takiego śledzenia - na przykład, gdy na jednej stronie internetowej pojawiają się reklamy związane z czymś, czego szukałeś na innej.

* Nie publikuj swojego prawdziwego numeru telefonu komórkowego. Uzyskaj numer przekierowania z usługi takiej jak Google Voice i ogólnie podawaj ten numer zamiast faktycznego numeru telefonu komórkowego. Takie postępowanie pomaga chronić się przed wieloma zagrożeniami - wymianą karty SIM, spamem itp. Przechowuj materiały prywatne w trybie offline. Najlepiej przechowywać bardzo wrażliwe materiały w trybie offline, na przykład w ognioodpornym sejfie lub w banku. Jeśli musisz przechowywać je w formie elektronicznej, przechowuj je na komputerze bez połączenia sieciowego.

* Szyfruj wszystkie prywatne informacje, takie jak dokumenty, obrazy, filmy i tak dalej. Jeśli nie masz pewności, czy coś powinno być zaszyfrowane, prawdopodobnie powinno.

* Jeśli korzystasz z czatu online, używaj szyfrowania od końca do końca. Załóżmy, że wszystkie wiadomości tekstowe wysyłane za pośrednictwem zwykłej usługi telefonii komórkowej mogą

potencjalnie zostać odczytane przez osoby z zewnątrz. Najlepiej nie podawać poufnych informacji na piśmie. Jeśli musisz udostępnić jakiś poufny element na piśmie, zaszyfruj dane.

Najprostszym sposobem szyfrowania danych jest użycie aplikacji do czatu, która oferuje szyfrowanie typu end-to-end. Kompleksowe oznacza, że wiadomości są szyfrowane na Twoim urządzeniu i odszyfrowywane na urządzeniu odbiorcy i odwrotnie - przy czym dostawca nie jest w stanie odszyfrować wiadomości; w związku z tym hakerzy, którzy włamują się do serwerów dostawcy, wymagają znacznie więcej wysiłku, aby odczytać Twoje wiadomości, jeśli stosowane jest szyfrowanie typu end-to-end. (Czasami dostawcy twierdzą, że hakerzy nie mogą w ogóle odczytać takich wiadomości, co nie jest poprawne. Z dwóch powodów: 1. Hakerzy mogą być w stanie zobaczyć metadane - na przykład, z kim rozmawiałeś i kiedy to zrobiłeś, oraz 2. Jeśli hakerzy włamują się do wystarczającej liczby serwerów wewnętrznych, mogą przesłać do sklepu z aplikacjami zatrutą wersję aplikacji zawierającą pewnego rodzaju backdoor). WhatsApp jest prawdopodobnie najpopularniejszą aplikacją do czatu, która wykorzystuje szyfrowanie od końca do końca.

* Praktykuj odpowiednią cyberhigienę. Ponieważ tak dużo informacji które chcesz zachować jako prywatne, są przechowywane w formie elektronicznej, dlatego przestrzeganie właściwej higieny w sieci ma kluczowe znaczenie dla zachowania prywatności.

WŁĄCZANIE TRYBU PRYWATNOŚCI

Aby włączyć tryb prywatności:

Google Chrome: Control + Shift-N lub wybierz z menu Nowe okno incognito

Firefox: Control + Shift + P lub wybierz z menu Nowe okno prywatne

Opera: Control + Shift + N lub wybierz z menu Nowe okno prywatne

Microsoft Edge: Control + Shift + P lub wybierz z menu Nowe okno prywatne

Vivaldi: Control + Shift + N lub wybierz z menu Nowe okno prywatne

Safari: Command + Shift + N lub wybierz Nowe okno prywatne z menu Plik

Bezpieczna bankowość online

Unikanie bankowości internetowej ze względu na obawy związane z bezpieczeństwem, które stwarza, jest po prostu niepraktyczne dla większości ludzi żyjących w dzisiejszych czasach. Na szczęście nie musisz rezygnować z odpowiednich udogodnień, aby zachować bezpieczeństwo. W rzeczywistości doskonale zdaję sobie sprawę z związanego z tym ryzyka, ponieważ bankowałem online od czasu, gdy bankowość internetowa została po raz pierwszy oferowana przez kilka dużych instytucji finansowych w połowie lat 90. jako zamiennik bezpośrednich usług bankowych dial-up. Oto kilka sugestii, co możesz zrobić, aby zwiększyć swoje bezpieczeństwo podczas korzystania z bankowości internetowej:

* Twoje hasło do bankowości internetowej powinno być silne, niepowtarzalne i zapisane w pamięci - nie może być przechowywane w bazie danych, menedżerze haseł ani w żadnym innym miejscu elektronicznym. (Jeśli chcesz to zapisać i przechowywać papier w skrytce depozytowej, to w porządku - ale rzadko konieczne).

* Wybierz losowy osobisty numer identyfikacyjny (PIN) do karty bankomatowej i / lub numeru identyfikacyjnego telefonu. Kod PIN nie powinien być powiązany z żadnymi znanymi Ci informacjami. Nie używaj kodu PIN, którego użyłeś do innych celów i nie ustalaj żadnych kodów PIN ani haseł na podstawie tego, który wybrałeś dla swojej karty bankomatowej. Nigdy nie zapisuj swojego kodu PIN.

Nigdy nie dodawaj go do żadnego pliku komputerowego. Nigdy nie podawaj swojego kodu PIN nikomu, w tym pracownikom banku.

* Rozważ zwrócenie się do swojego banku o kartę bankomatową, której nie można używać jako karty debetowej. Chociaż takie karty mogą nie mieć możliwości zakupu towarów i usług, jeśli dokonujesz zakupów za pomocą kart kredytowych, nie potrzebujesz funkcji zakupu na karcie bankomatowej. Zapobiegając używaniu karty jako karty debetowej, zwiększasz prawdopodobieństwo, że tylko ktoś, kto zna Twój numer PIN, może pobrać pieniądze z Twojego konta. Być może równie ważne jest to, że „okaleczone" karty bankomatowe nie mogą być również wykorzystywane przez oszustów do dokonywania oszukańczych zakupów.

Jeśli Twoja karta debetowa została użyta w nieuczciwy sposób, stracisz pieniądze i musisz je odzyskać. Jeśli Twoja karta kredytowa jest wykorzystywana w nieuczciwy sposób, nie tracisz żadnych pieniędzy, chyba że dochodzenie wykaże, że to Ty dokonałeś oszustwa.

* Loguj się do bankowości internetowej tylko z zaufanych urządzeń, które kontrolujesz, na których jest zainstalowane oprogramowanie zabezpieczające i które są aktualizowane.

* Loguj się do bankowości internetowej tylko z bezpiecznych sieci, którym ufasz. Jeśli jesteś w drodze, korzystaj z połączenia z siecią komórkową, a nie z publicznej sieci Wi-Fi.

* Zaloguj się do bankowości internetowej za pomocą przeglądarki internetowej lub oficjalnej aplikacji banku. Nigdy nie loguj się z aplikacji innej firmy lub aplikacji uzyskanej z innego miejsca niż oficjalny sklep z aplikacjami na platformę Twojego urządzenia.

* Zarejestruj się, aby otrzymywać alerty ze swojego banku. Powinieneś skonfigurować, aby otrzymywać powiadomienia SMS-em i / lub e-mailem za każdym razem, gdy zostanie dodany nowy odbiorca płatności, nastąpi wypłata i tak dalej.

* Używaj uwierzytelniania wieloskładnikowego i chroń dowolne urządzenie używane do takiego uwierzytelniania. Jeśli na przykład wygenerujesz jednorazowe hasła w telefonie, a Twój telefon zostanie skradziony, Twój drugi czynnik stanie się (przynajmniej tymczasowo) użyteczny dla oszusta, a nie dla Ciebie.

* Nie zezwalaj przeglądarce na przechowywanie hasła do bankowości internetowej. Twoje hasło do bankowości internetowej nie powinno być nigdzie zapisywane - na pewno nie w systemie, który będzie go wprowadzał w imieniu kogoś korzystającego z przeglądarki internetowej.

* Wprowadź adres URL swojego banku za każdym razem, gdy odwiedzasz bank w sieci. Nigdy nie klikaj linków do niego.

* Najlepiej używać innego komputera do bankowości internetowej niż do zakupów online, dostępu do poczty e-mail i mediów społecznościowych. Jeśli nie jest to możliwe lub praktyczne, użyj innej przeglądarki internetowej i pamiętaj o jej aktualizowaniu.

* Jako dodatkowe zabezpieczenie możesz skonfigurować przeglądarkę tak, aby zapamiętywała nieprawidłowe hasło do witryny, aby jeśli ktoś kiedykolwiek dostał się do Twojego laptopa lub telefonu, miał mniejsze szanse na pomyślne zalogowanie się do tej witryny przy użyciu Twoich danych logowania.

* Upewnij się, że zabezpieczasz wszystkie urządzenia, z których korzystasz z bankowości internetowej. Obejmuje to fizyczne ich zabezpieczenie (nie zostawiaj ich na stole w restauracji, gdy idziesz do toalety), wymaganie hasła do ich odblokowania i włączenie zdalnego czyszczenia.

* Monitoruj swoje konto pod kątem nieautoryzowanych działań.

Bezpieczne korzystanie z urządzeń inteligentnych

Inteligentne urządzenia i tak zwany Internet przedmiotów stwarzają różnego rodzaju zagrożenia dla cyberbezpieczeństwa. Oto kilka zaleceń, jak poprawić swoje bezpieczeństwo podczas korzystania z takich urządzeń:

* Upewnij się, że żadne z urządzeń IoT nie stwarza zagrożeń bezpieczeństwa w przypadku awarii. Nigdy nie twórz sytuacji, w której inteligentny zamek uniemożliwia np. Wyjście z pomieszczenia w trakcie pożaru lub pozwala rabusiom na wejście do Twojego domu podczas przerwy w dostawie prądu lub awarii sieci.

* Jeśli to możliwe, uruchamiaj urządzenia IoT w innej sieci niż Twoje komputery. Sieć IoT powinna być chroniona przez zaporę ogniową.

* Aktualizuj wszystkie urządzenia IoT. Hakerzy wykorzystali luki w zabezpieczeniach urządzeń IoT, aby przejąć te urządzenia i wykorzystać je do przeprowadzenia poważnych ataków. Jeśli urządzenie ma funkcję automatycznej aktualizacji oprogramowania układowego, rozważ jej włączenie.

* Zachowaj pełną, aktualną listę wszystkich urządzeń podłączonych do sieci. Zachowaj również listę wszystkich urządzeń, które nie są aktualnie podłączone, ale które mają autoryzację do połączenia, a czasami się łączą.

* Jeśli to możliwe, odłączaj urządzenia, gdy ich nie używasz. Jeśli urządzenie jest w trybie offline, z pewnością nie może zostać zhakowane przez nikogo nie fizycznie przez obecność na urządzeniu.

* Zabezpiecz hasłem wszystkie urządzenia. Nigdy nie zachowuj domyślnych haseł dostarczonych z urządzeniami. Każde urządzenie powinno mieć unikalny login i hasło.

* Sprawdź ustawienia swoich urządzeń. Wiele urządzeń ma domyślne wartości ustawień, które są straszne z punktu widzenia bezpieczeństwa.

* Zabezpiecz swój smartfon fizycznie i cyfrowo. Prawdopodobnie uruchamia aplikacje z dostępem do niektórych lub wszystkich Twoich urządzeń,

* Jeśli to możliwe, wyłącz funkcje urządzenia, których nie potrzebujesz. Takie postępowanie zmniejsza odpowiednią powierzchnię ataku - to znaczy zmniejsza liczbę potencjalnych punktów, w których nieautoryzowany użytkownik może próbować włamać się do urządzenia - i jednocześnie zmniejsza prawdopodobieństwo, że urządzenie ujawni lukę w oprogramowaniu, którą można wykorzystać. Universal Plug and Play upraszcza konfigurację urządzeń, ale także ułatwia hakerom wykrywanie urządzeń i atakowanie ich z wielu powodów, w tym ze względu na to, że wiele implementacji UPnP zawiera luki w zabezpieczeniach, UPnP może czasami pozwolić złośliwemu oprogramowaniu na ominięcie procedur zabezpieczeń zapory ogniowej, a UPnP może czasami być wykorzystywane przez hakerów do uruchamiania poleceń na routerach.

* Nie podłączaj urządzeń IoT do niezaufanych sieci.