W PROSTOCIE TKWI SIŁA

wydanie II

Cyber bezpieczeństwo

dla bystrzaków

Przewiduj potencjalne zagrożenia

Unikaj włamań i odpieraj ataki

Zadbaj o swoje cyberbezpieczeństwo

Joseph Steinberg

Tytuł oryginału: Cybersecurity For Dummies, 2nd Edition

Tłumaczenie: Grzegorz Werner

ISBN: 978-83-8322-286-8

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
https://dlabystrzakow.pl/user/opinie/cybeb2
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *dlabystrzakow@dlabystrzakow.pl*
WWW: *https://dlabystrzakow.pl*

Printed in Poland.

Spis treści

W TYM ROZDZIALE:

- Dlaczego nie jesteś tak bezpieczny, jak Ci się wydaje
- Jak się chronić przed zagrożeniami cyfrowymi
- Ocena bieżących środków bezpieczeństwa
- Kwestie prywatności
- Stosowanie zalecanych praktyk

Rozdział 4

Ocena bieżącej postawy w zakresie cyberbezpieczeństwa

Pierwszym krokiem w kierunku skuteczniejszej obrony przed zagrożeniami cyfrowymi jest zrozumienie, co właściwie musisz chronić. Kiedy już to ustalisz, będziesz mógł ocenić, co jest potrzebne, aby zapewnić wystarczający stopień bezpieczeństwa, i czy masz jakieś luki w zabezpieczeniach, którymi trzeba się zająć.

Musisz się zastanowić, jakie masz dane, przed kim musisz je chronić i czy są wrażliwe. Co by się na przykład stało, gdyby zostały opublikowane w internecie i każdy mógł je zobaczyć? Następnie będziesz mógł określić, ile czasu i pieniędzy jesteś gotów przeznaczyć na ich zabezpieczenie.

Nie bądź Achillesem: identyfikowanie obszarów, które nie są w pełni zabezpieczone

Historia greckiego herosa Achillesa uczy nas, że jeśli masz słaby punkt, napastnicy prędzej czy później znajdą sposób, aby zadziałał on na Twoją szkodę. W związku z tym powinieneś zidentyfikować obszary, w których Twoja obecna postawa w zakresie cyberbezpieczeństwa odbiega od ideału, i rozwiązać ewentualne problemy, a tym samym zapewnić sobie odpowiednią ochronę. Powinieneś na przykład zinwentaryzować wszystkie urządzenia, które mogą zawierać wrażliwe dane, stać się odskocznią do ataku itd.

Komputery domowe

W komputerach domowych może występować jeden lub wiele spośród poniższych problemów związanych z cyberbezpieczeństwem:

- **Włamanie**. Napastnik mógł spenetrować Twój komputer domowy i obecnie ma nad nim pełną kontrolę. Może przeglądać jego zawartość, używać go do łączenia się z innymi maszynami, wykorzystywać do ataków na inne komputery, telefony i urządzenia inteligentne, wydobywać kryptowaluty, czytać dane przesyłane w Twojej sieci itd.
- **Złośliwe oprogramowanie**. W Twoim komputerze domowym może znajdować się *złośliwe oprogramowanie*, które stwarza zagrożenia podobne do tych wynikających z obecności włamywacza, dając przestępcom pełną kontrolę nad komputerem. Mogą oni przeglądać zawartość komputera, kontaktować się z innymi urządzeniami elektronicznymi, wydobywać kryptowaluty itd. — a także czytać dane w Twojej sieci oraz infekować inne komputery.
- **Współdzielone komputery**. Kiedy dzielisz komputer z innymi osobami — w tym z małżonkiem i (lub) dziećmi — ryzykujesz, że nie będą one przestrzegać zasad cyberhigieny równie rygorystycznie jak Ty, w rezultacie narażając urządzenie na infekcję złośliwym oprogramowaniem lub atak hakera. Mogą też nieumyślnie same wyrządzić sobie krzywdę.
- **Połączenia z innymi sieciami i aplikacjami do przechowywania danych**. Jeśli Twój komputer łączy się za pośrednictwem wirtualnej sieci prywatnej (*virtual private network*, VPN) z innymi sieciami, na przykład w Twoim miejscu zatrudnienia, złośliwe oprogramowanie obecne tych sieciach albo hakerzy czający się w podłączonych do nich urządzeniach mogą zaatakować również Twoją sieć i inne lokalne urządzenia. W niektórych przypadkach podobne zagrożenia występują wtedy, kiedy używasz aplikacji, które łączą Twój komputer z usługami sieciowymi, takimi jak zdalne systemy przechowywania danych.

- **Zagrożenia fizyczne**. Jak opisano szczegółowo w rozdziale 5., fizyczna lokalizacja może zmniejszać lub zwiększać stopień zagrożenia komputera i jego zawartości.

Urządzenia mobilne

Z perspektywy bezpieczeństwa informacji urządzenia mobilne są ryzykowne z natury, ponieważ:

- są stale połączone z internetem, czyli niezabezpieczoną, publiczną siecią, w której czai się wielu hakerów i za pośrednictwem której przeprowadzane są niemal wszystkie cyberataki;
- często zawierają dużo poufnych informacji;
- służą do komunikacji z wieloma osobami i systemami, czasem niegodnymi zaufania, za pośrednictwem internetu (któremu również nie można ufać);
- mogą odbierać wiadomości od osób, z którymi użytkownik nigdy wcześniej się nie kontaktował, a część takich osób może mieć złe zamiary;
- często nie korzystają z oprogramowania zabezpieczającego ze względu na ograniczenia zasobów albo używają wstępnie zainstalowanego oprogramowania, którego nie można ręcznie zaktualizować lub zmienić, jeśli użytkownik uzna, że nie spełnia ono jego potrzeb;
- łatwo je zgubić lub ukraść;
- łatwo je przypadkowo uszkodzić lub zniszczyć;
- często łączą się z niezabezpieczonymi i niezaufanymi sieciami Wi-Fi;
- są regularnie wymieniane i wyrzucane bez usuwania z nich wrażliwych danych;
- są często oddawane w rozliczeniu za nowsze urządzenia — również bez usunięcia wrażliwych danych.

Urządzenia internetu rzeczy (IoT)

Jak wyjaśniono szczegółowo w rozdziale 18., świat przetwarzania danych w sieci radykalnie zmienił się w ostatnich latach. Jeszcze niedawno jedynymi urządzeniami podłączonymi do internetu były klasyczne komputery — desktopy, laptopy i serwery, których można było używać do wielu różnych celów. Dziś jednak żyjemy w zupełnie innym świecie, w którym komputery stanowią niewielką część urządzeń podłączonych do sieci.

Od smartfonów do kamer bezpieczeństwa, lodówek, samochodów, ekspresów do kawy i sprzętu do ćwiczeń — różne typy urządzeń elektronicznych zawierają teraz zaawansowane komputery, a wiele z tych komputerów jest stale podłączonych do internetu.

Internet rzeczy (*Internet of Things*, IoT), jak zwykło się nazywać ten ekosystem połączonych urządzeń, w ciągu ostatnich lat rósł wykładniczo, ale zabezpieczenia urządzeń IoT często są, łagodnie mówiąc, niewystarczające. Wiele urządzeń nie zawiera technologii, która chroniłyby je przed włamaniami. Nawet te, które je zawierają, często nie są prawidłowo skonfigurowane. Hakerzy mogą wykorzystać urządzenia IoT, aby Cię szpiegować, kraść Twoje dane, atakować inne systemy i (lub) urządzenia, przeprowadzać ataki DoS na sieci lub urządzenia oraz powodować wiele innych szkód.

Sprzęt sieciowy

Sprzęt sieciowy można zhakować tak, aby kierował ruch do niewłaściwych witryn, przechwytywał dane, inicjował ataki, blokował dostęp do internetu itd.

Środowisko pracy

W swoim środowisku pracy możesz mieć wrażliwe dane — możesz też zostać narażony na ryzyko przez kolegów. Jeśli na przykład przyniesiesz jakieś urządzenia elektroniczne do pracy i podłączysz je do firmowej sieci, a następnie zabierzesz je do domu i podłączysz do sieci domowej, złośliwe oprogramowanie może przedostać się do Twojego urządzenia z komputerów pracodawcy lub współpracowników, którzy używają tej samej infrastruktury, a następnie przedostać się z Twojego urządzenia do innych komputerów w sieci domowej.

Oczywiście epidemia COVID-19 sprawiła, że wiele środowisk firmowych i domowych zlało się w jedno, często z niepokojącymi skutkami dla cyberbezpieczeństwa.

Identyfikowanie zagrożeń

Aby cokolwiek zabezpieczyć, musisz wiedzieć, co próbujesz ochronić; odpowiednie zabezpieczenie środowiska jest trudne, a wręcz niemożliwe, jeśli nie wiesz, co się w tym środowisku znajduje. (Jest to prastara mądrość; patrz cytat z Sun Tzu na początku rozdziału 3.).

Aby się więc zabezpieczyć, musisz zrozumieć, jakie masz zasoby — zarówno cyfrowe, jak i fizyczne — i co chcesz chronić. Zasoby te mogą, ale nie muszą znajdować się w jednym miejscu. W rzeczywistości niektóre mogą znajdować się w miejscach, do których nie masz fizycznego dostępu. Możesz na przykład mieć dane przechowywane w usłudze chmurowej, takiej jak Google Drive, Apple iCloud lub Microsoft OneDrive. Musisz też zrozumieć, na jakie zagrożenia narażone są te zasoby.

PUNKTY KOŃCOWE

Punkt końcowy to każde urządzenie komputerowe komunikujące się z siecią, do której jest podłączone. Twój laptop jest punktem końcowym, kiedy jest podłączony do Twojej sieci domowej; smartfon jest punktem końcowym, kiedy jest podłączony do Twojej sieci Wi-Fi albo do sieci 4G lub 5G operatora telefonii komórkowej. Nazwa bierze się stąd, że urządzenia te znajdują się na końcu ścieżki komunikacyjnej. Połączenia internetowe często przechodzą przez wiele pośrednich węzłów, aby dotrzeć do punktu końcowego, który jest ostatnim etapem podróży danych.

Wszystkie punkty końcowe stanowią zagrożenie, więc muszą być odpowiednio zabezpieczone. Laptopy, smartfony i tablety oraz inne urządzenia komputerowe powinny korzystać z oprogramowania zabezpieczającego, a urządzenia IoT powinny być chronione w takim stopniu, jakiego wymaga ich funkcja.

Firmy często centralnie zarządzają autoryzowanymi punktami końcowymi i mogą mieć scentralizowane systemy bezpieczeństwa, które komunikują się z oprogramowaniem klienckim w punktach końcowych, aby egzekwować zasady, wykrywać anomalie, zapobiegać wyciekom danych i powstrzymywać ataki.

Użytkownicy indywidualni zwykle nie korzystają z takich systemów, ale nadal powinni się upewnić, że wszystkie punkty końcowe w ich sieciach domowych są zabezpieczone w sposób opisywany w tym rozdziale i w całej książce.


WSKAZÓWKA

W przypadku użytkowników indywidualnych inwentaryzacja zasobów jest zwykle dość prosta. Zacznij od sporządzenia pisemnej listy wszystkich urządzeń podłączonych do Twojej sieci. Często wystarczy w tym celu zalogować się w routerze i przejść do sekcji „Podłączone urządzenia". Oczywiście możesz mieć jakieś urządzenia, które podłączasz do sieci tylko od czasu do czasu albo które wymagają zabezpieczenia, mimo że nie łączą się z Twoją siecią; pamiętaj, aby dopisać je do listy.

Dodaj do tej listy — w oddzielnej sekcji — wszystkie urządzenia pamięciowe, których używasz, w tym zewnętrzne dyski twarde, urządzenia USB i karty pamięci, a także usługi firm trzecich. Zapisz listę na kartce lub wydrukuj ją; pominięcie choćby jednego urządzenia może prowadzić do problemów.

Ochrona przed zagrożeniami

Kiedy ustalisz, co wymaga ochrony (patrz poprzedni podrozdział), musisz opracować i wdrożyć odpowiednie środki bezpieczeństwa, aby prawidłowo chronić te zasoby i ograniczyć skutki potencjalnego włamania.

W kontekście użytkowników domowych ochrona polega na wzniesieniu barier przed każdym, kto próbuje bez upoważnienia uzyskać dostęp do Twoich zasobów cyfrowych i fizycznych, wprowadzeniu (choćby nieformalnych) procesów i procedur ochrony wrażliwych danych oraz utworzeniu kopii zapasowych wszystkich danych konfiguracyjnych i podstawowych punktów przywracania systemu.

Do podstawowych aspektów ochrony należą:

- obrona granic,
- zapora sieciowa/router,
- oprogramowanie zabezpieczające,
- fizyczne zabezpieczenie komputerów i innych punktów końcowych,
- kopie zapasowe.

Aby skutecznie bronić się przed zagrożeniami, trzeba wiedzieć, jak wykrywać naruszenia cyberbezpieczeństwa, odpowiednio na nie reagować, przywracać zainfekowane urządzenia do pierwotnego stanu oraz poprawiać środki defensywne, żeby jeszcze bardziej ograniczyć ryzyko.

Obrona granic

Obrona cybergranic jest zasadniczo cyfrowym odpowiednikiem kopania fosy wokół zamku — próbą powstrzymania każdego, kto chce dostać się do środka inaczej niż autoryzowanym wejściem pod czujnym okiem strażników.

Aby zbudować tę cyfrową fosę, nigdy nie podłączaj żadnego komputera bezpośrednio do modemu internetowego. Zamiast tego podłącz zaporę/router do modemu, a komputery — do zapory/routera. (Jeśli Twój modem zawiera zaporę/router, to jest urządzeniem wielofunkcyjnym; jeżeli jesteś podłączony do części działającej jako zapora/router, a nie do samego modemu, wszystko jest w porządku). Zwykle połączenia między zaporami a modemami są przewodowe — to znaczy wykorzystują fizyczny kabel sieciowy. W niektórych przypadkach modem i zapora/router znajdują się nawet w tym samym fizycznym urządzeniu.

Zapora/router

Nowoczesne routery do użytku domowego mają wbudowane funkcje zapory sieciowej, które blokują większość ruchu przychodzącego, jeśli nie został on wygenerowany w wyniku działań zainicjowanych przez urządzenia chronione przez zaporę. Oznacza to, że zapora blokuje osoby z zewnątrz, które próbują skontaktować się z komputerem w Twoim domu, ale nie blokują serwera WWW, który odpowiada na żądanie strony internetowej zgłoszone przez Twój komputer. Routery używają wielu technologii, aby zapewnić taką ochronę.

Jedną z takich technologii jest translacja adresów sieciowych (*Network Address Translation*, NAT) pozwalająca komputerom w Twojej sieci domowej korzystać z adresów Internet Protocol (IP), które nie są przeznaczone do użytku w internecie, a tylko w sieciach prywatnych. Z perspektywy internetu wszystkie urządzenia w sieci z NAT wydają się mieć jeden adres — adres zapory, która jest usytuowana między nimi a internetem i realizuje funkcje NAT.

Poniższe zalecenia pomogą routerowi/zaporze chronić Twoją sieć:

- **Regularnie aktualizuj router**. Zainstaluj wszystkie dostępne aktualizacje, zanim po raz pierwszy podłączysz router do swojej sieci, i regularnie sprawdzaj dostępność nowych aktualizacji (chyba że Twój router ma funkcję automatycznej aktualizacji; w takim przypadku warto z niej skorzystać).


ZAPAMIĘTAJ

  Niezałatana luka w zabezpieczeniach routera może zapewnić osobom z zewnątrz dostęp do Twojej sieci.

- **Wymień router, kiedy przestanie być wspierany**. Jeśli producent nie zapewnia już wsparcia dla routera (w tym aktualizacji), prawdopodobnie czas go wymienić. Zważywszy na cykl życia takich urządzeń i cykl życia protokołów sieciowych, dodatkową korzyścią może być wyższa wydajność.
- **Zmień domyślne hasło administratora w zaporze/routerze na mocne hasło znane tylko Tobie**. Zapisz nowe hasło na kartce i schowaj ją w sejfie albo innym bezpiecznym miejscu. Nie przechowuj takich haseł w urządzeniach podłączonych do sieci. Przećwicz logowanie się w routerze — i powtarzaj to regularnie, żeby nie zapomnieć hasła.
- **Nie używaj domyślnej nazwy sieci Wi-Fi (identyfikatora SSID) ustawionej przez producenta routera**. Utwórz nową nazwę.
- **Skonfiguruj sieć Wi-Fi tak, aby używała przynajmniej standardu szyfrowania WPA2, a jeśli to możliwe, korzystaj z WPA3**. Są to aktualne standardy, kiedy piszę niniejszą książkę.
- **Ustaw hasło, które będzie musiało podawać każde urządzenie dołączające do Twojej sieci Wi-Fi**. Upewnij się, że jest to mocne hasło. Informacje o tworzeniu mocnych haseł, które łatwo zapamiętać, znajdziesz w rozdziale 8.
- **Jeśli wszystkie Twoje urządzenia sieciowe mogą korzystać z nowoczesnych protokołów sieciowych Wi-Fi 6 i (lub) Wi-Fi 5, wyłącz obsługę starszych protokołów w swoim routerze**. Wyłączenie protokołów takich jak 802.11b, 802.11g i 802.11n może zwiększyć wydajność i stopień bezpieczeństwa.
- **Włącz filtrowanie adresów MAC albo upewnij się, że wszyscy domownicy wiedzą, że nie powinni podłączać niczego do sieci przewodowej bez Twojego pozwolenia**. Filtrowanie adresów MAC przynajmniej teoretycznie uniemożliwia podłączenie urządzenia do sieci, jeśli wcześniej nie skonfigurujesz routera tak, aby na to pozwalał. Nie pozwalaj nikomu podłączać do sieci urządzeń, które nie zostały wcześniej zabezpieczone.
- **Umieść swój router bezprzewodowy w środku domu**. Dzięki temu będziesz mógł się cieszyć lepszym sygnałem, a jednocześnie ograniczysz siłę sygnału dostępnego na zewnątrz domu dla osób, które mogą próbować dostać się do Twojej sieci. Jeśli masz kratowy system routingu z wieloma punktami dostępowymi, rozmieść urządzenia zgodnie z instrukcją producenta.

- **Nie włączaj zdalnego dostępu do swojego routera**. Routerem należy zarządzać tylko z chronionych przez niego urządzeń, a nie ze świata zewnętrznego. Wygoda zdalnego zarządzania domową zaporą rzadko jest warta ryzyka, które wiąże się z włączeniem takiej funkcji.
- **Prowadź listę urządzeń podłączonych do Twojej sieci**. Dopisz do tej listy również urządzenia, którym zezwalasz na podłączanie się do Twojej sieci, a które obecnie nie są podłączone.
- **Jeśli chcesz zezwolić na dostęp gościom, włącz funkcję sieci gościnnej w swoim routerze i, podobnie jak w przypadku sieci prywatnej, uaktywnij szyfrowanie oraz egzekwowanie mocnych haseł**. Zezwól gościom na dostęp do sieci gościnnej, a nie do swojej sieci podstawowej. To samo dotyczy innych osób, którym musisz zapewnić dostęp do internetu, a którym w pełni nie ufasz, łącznie z członkami rodziny, na przykład dziećmi.
- **Jeśli masz wystarczającą wiedzę techniczną, aby wyłączyć DHCP i zmienić domyślny zakres adresów IP przypisywanych przez router urządzeniom w Twojej sieci wewnętrznej, zrób to**. W ten sposób zakłócisz działanie niektórych zautomatyzowanych narzędzi hakerskich i zyskasz inne korzyści związane z bezpieczeństwem. Jeśli te koncepcje nie są Ci znane lub nie masz pojęcia, co oznacza powyższe zdanie, po prostu zignoruj ten akapit. W takim przypadku korzyści wynikające z powyższej rady będą prawdopodobnie mniejsze niż problemy, które możesz napotkać z powodu dodatkowych komplikacji technicznych, jakie spowoduje wyłączenie DHCP i zmiana domyślnego zakresu adresów IP.

Oprogramowanie zabezpieczające

Jak używać oprogramowania zabezpieczającego, żeby się skutecznie chronić?

- Używaj oprogramowania zabezpieczającego we wszystkich komputerach i urządzeniach mobilnych. Oprogramowanie to powinno oferować przynajmniej funkcje ochrony antywirusowej oraz osobistej zapory.
- Używaj oprogramowania antyspamowego w każdym urządzeniu, na którym czytasz pocztę.
- Włącz funkcję zdalnego wymazywania danych w każdym urządzeniu mobilnym.
- Wymagaj mocnego hasła do zalogowania się w każdym komputerze i urządzeniu mobilnym.
- Włącz automatyczne aktualizacje wszędzie, gdzie to możliwe, i regularnie aktualizuj swoje urządzenia.

Twoje fizyczne komputery i inne punkty końcowe

Aby fizycznie zabezpieczyć swój komputer i inne punkty końcowe:

- **Kontroluj fizyczny dostęp do komputera i trzymaj go w bezpiecznym miejscu**. Jeśli na przykład każdy, kto wchodzi do Twojego domu, może dostać się do komputera, urządzenie to może względnie łatwo zostać skradzione, wykorzystane lub uszkodzone bez Twojej wiedzy.
- **Jeśli to możliwe, nie udostępniaj swojego komputera członkom rodziny**. Jeśli musisz udostępnić swój komputer, utwórz oddzielne konta dla każdego członka rodziny i nie przyznawaj nikomu przywilejów administratora urządzenia.
- **Nie ograniczaj się do zwykłego usunięcia danych przed wyrzuceniem, darowaniem lub sprzedażą starego urządzenia**. Użyj systemu wielokrotnego wymazywania danych ze wszystkich dysków twardych i stacji SSD. Najlepiej wyjąć nośniki pamięciowe z komputera przed pozbyciem się go i fizycznie je zniszczyć.

Pamiętaj też, że niektóre urządzenia komputerowe, które trzeba zabezpieczyć, mogą nie być prawdziwymi „punktami końcowymi" w tym sensie, że mogą być do nich podłączone inne urządzenia. Na przykład koncentrator systemu inteligentnego domu albo bezprzewodowy system kamer mogą łączyć się z urządzeniami inteligentnymi i (lub) kamerami za pośrednictwem niestandardowych mechanizmów komunikacyjnych; oczywiście one również muszą być odpowiednio zabezpieczone.

Kopie zapasowe

Regularnie twórz kopie zapasowe. Jeśli nie wiesz, co w Twoim przypadku oznacza „regularnie", prawdopodobnie nie robisz kopii zapasowych wystarczająco często.

Więcej informacji o kopiach zapasowych znajdziesz w rozdziale 14.

Detekcja

Detekcja odnosi się do wdrażania mechanizmów, które umożliwiają jak najszybsze wykrywanie zdarzeń związanych z cyberbezpieczeństwem. Choć większość użytkowników domowych nie może sobie pozwolić na nabycie wyspecjalizowanych produktów do detekcji, nie oznacza to, że fazę detekcji można zignorować.

Dziś większość oprogramowania zabezpieczającego do komputerów osobistych ma różne funkcje detekcji. Upewnij się, że każde urządzenie, którym zarządzasz, ma oprogramowanie zabezpieczającego, na przykład szukające oznak włamania. Więcej informacji o wykrywaniu potencjalnych włamań znajdziesz w rozdziale 12.

Reakcja

Reakcja odnosi się do działań podejmowanych w odpowiedzi na incydent. Większość programów zabezpieczających albo automatycznie podejmuje działania, albo zachęca użytkownika do podjęcia działań w razie wykrycia potencjalnych problemów. Więcej informacji o reakcji znajdziesz w rozdziale 13.

Przywracanie

Przywracanie odnosi się do działań mających na celu przywrócenie komputera, sieci lub urządzenia — oraz wszystkich jego istotnych funkcji — do prawidłowego stanu po zdarzeniu naruszenia cyberbezpieczeństwa. Więcej informacji o przywracaniu znajdziesz w rozdziałach 13., 15. i 16.


ZAPAMIĘTAJ

Najlepiej zawczasu sporządzić formalny, pisemny, prosty, określający priorytety plan przywracania. Większość użytkowników domowych nie tworzy planu przywracania, choć może to być bardzo korzystne. W większości domów taki plan powinien zmieścić się na jednej stronie.

Poprawa

Ci, którzy nie uczą się na własnych błędach, powinni się wstydzić. Każdy incydent naruszenia cyberbezpieczeństwa oferuje lekcje, które warto wprowadzić w życie, aby ograniczyć przyszłe ryzyko. Przykłady uczenia się na błędach znajdziesz w rozdziale 20.

Ocena bieżących środków bezpieczeństwa

Kiedy już wiesz, co i jak musisz chronić, możesz określić różnicę między tym, czego potrzebujesz, a tym, czym dysponujesz obecnie.

W poniższych punktach opisano kilka elementów, które należy wziąć pod uwagę. Nie wszystkie są istotne w każdym przypadku.

Oprogramowanie

Jeśli chodzi o cyberbezpieczeństwo oprogramowania w każdym z Twoich urządzeń, zadaj sobie następujące pytania:

- Czy całe oprogramowanie (w tym sam system operacyjny) pozyskano legalnie?
- Czy całe oprogramowanie (w tym sam system operacyjny) pozyskano z wiarygodnych źródeł, które zawsze (albo przynajmniej tak często, jak to możliwe) dostarczają legalne wersje?

- Czy wszystkie programy (w tym sam system operacyjny) są obecnie wspierane przez odpowiednich producentów?
- Czy wszystkie programy (w tym sam system operacyjny) są aktualne?
- Czy wszystkie programy (w tym sam system operacyjny) są skonfigurowane tak, aby aktualizowały się automatycznie?
- Czy w urządzeniu działa oprogramowanie zabezpieczające?
- Czy oprogramowanie zabezpieczające jest skonfigurowane tak, aby aktualizowało się automatycznie?
- Czy oprogramowanie zabezpieczające jest aktualne?
- Czy oprogramowanie zabezpieczające zawiera technologię chroniącą przed złośliwym oprogramowaniem — i czy ta funkcja jest w pełni aktywna?
- Czy skonfigurowano uruchamianie skanowania antywirusowego po zastosowaniu każdej aktualizacji?
- Czy oprogramowanie zabezpieczające zawiera technologię zapory — i czy ta funkcja jest w pełni aktywna?
- Czy oprogramowanie zabezpieczające zawiera technologię antyspamową — i czy ta funkcja jest w pełni aktywna? Jeśli nie, czy zainstalowane i uruchomione jest inne oprogramowanie antyspamowe?
- Czy oprogramowanie zabezpieczające zawiera technologię zdalnego blokowania i (lub) zdalnego wymazywania — i czy ta funkcja jest w pełni aktywna? Jeśli nie, czy zainstalowane i uruchomione jest inne oprogramowanie do zdalnego blokowania/wymazywania?
- Czy włączone są wszystkie inne funkcje oprogramowania zabezpieczającego? Jeśli nie, które nie są?
- Czy uruchomione jest oprogramowanie do backupu, które tworzy kopię zapasową urządzenia w ramach strategii backupu?
- Czy włączone jest szyfrowanie przynajmniej wrażliwych danych przechowywanych w urządzeniu?
- Czy uprawnienia oprogramowania są skonfigurowane prawidłowo — blokują osoby, które mogą mieć dostęp do urządzenia, ale nie powinny mieć dostępu do oprogramowania?
- Czy skonfigurowano uprawnienia, które uniemożliwiają oprogramowaniu dokonywanie niepożądanych zmian w komputerze (na przykład czy jakiś program działa z przywilejami administratora, choć nie powinien)?

Oczywiście wszystkie te pytania odnoszą się do oprogramowania w urządzeniu, którego używasz, ale nie narażasz na użycie przez niezaufane osoby z zewnątrz.

Jeśli masz urządzenia, do których uzyskują dostęp użytkownicy zewnętrzni — na przykład serwer WWW — musisz rozważyć wiele innych kwestii bezpieczeństwa; ich opis wykracza poza ramy niniejszej książki.

Sprzęt

Jeśli chodzi o urządzenia, zadaj sobie następujące pytania:

- Czy urządzenie nabyto od zaufanego sprzedawcy? (Jeśli kupiłeś kamerę IP bezpośrednio z Chin, od jakiegoś internetowego detalisty, o którym nigdy nie słyszałeś przed dokonaniem zakupu, odpowiedź na to pytanie może nie być twierdząca).
- W jakim stopniu jesteś pewien odpowiedzi na poprzednie pytanie — a jeśli jesteś bardzo pewien, to z jakiego powodu?
- Czy urządzenie zostało wyprodukowane przez firmę, której produktów rząd Stanów Zjednoczonych zabrania używać swoim agencjom, ponieważ nie ufa, że są one wystarczająco zabezpieczone przed zagranicznymi szpiegami albo zagrożeniami cyfrowymi?
- Czy cały sprzęt komputerowy w Twoim domu jest odpowiednio chroniony przed kradzieżą i uszkodzeniem (deszczem, przepięciami itd.)?
- Co chroni Twoje urządzenia podczas podróży?
- Czy masz zasilacz awaryjny albo wbudowaną baterię, która chroni urządzenie przed nagłym wyłączeniem w razie choćby chwilowej przerwy w dostawie prądu?
- Czy cały Twój sprzęt używa najnowszego oprogramowania układowego — i czy pobrałeś to oprogramowanie układowe z godnego zaufania źródła, na przykład z witryny producenta albo jako aktualizację zainicjowaną przez narzędzie do konfiguracji urządzenia?
- W przypadku routerów (i zapór), czy Twoje urządzenie spełnia kryteria wymienione w punkcie „Zapora/router” wcześniej w tym rozdziale?
- Czy masz ustawione hasło do BIOS-u, które uniemożliwia korzystanie z urządzenia, dopóki użytkownik nie wprowadzi prawidłowego hasła?
- Czy wyłączyłeś wszystkie protokoły bezprzewodowe, których nie potrzebujesz? Jeśli na przykład nie używasz protokołu Bluetooth w laptopie, wyłącz radio Bluetooth, co nie tylko poprawi bezpieczeństwo, ale również wydłuży czas pracy na zasilaniu bateryjnym.

Ubezpieczenie

Mniejsze firmy i użytkownicy indywidualni rzadko ubezpieczają się od naruszeń cyberbezpieczeństwa, choć jest to dobry sposób na ograniczenie niektórych zagrożeń cyfrowych. W zależności od specyfiki Twojej sytuacji zakup polisy chroniącej przed konkretnymi zagrożeniami może mieć sens.

Jeśli masz małą firmę, która może zbankrutować, jeżeli dojdzie do naruszenia cyberbezpieczeństwa, oczywiście musisz wdrożyć mocne zabezpieczenia. Ponieważ jednak żadne środki bezpieczeństwa nie dają stuprocentowej gwarancji, polisa chroniąca przed katastrofalnymi sytuacjami może być rozsądną inwestycją.

Choć ubezpieczenia od naruszenia cyberbezpieczeństwa jeszcze niedawno były dostępne tylko dla dużych przedsiębiorstw, w niedawnych latach zaczęto oferować również polisy dla użytkowników indywidualnych i małych firm.

Edukacja

Odrobina edukacji może przyczynić się do tego, że inne osoby w Twoim domu (albo organizacji) nie staną się piętą achillesową cyberbezpieczeństwa. Na poniższej liście wymieniono kilka tematów wartych przemyślenia i przedyskutowania:

- Czy wszyscy członkowie rodziny znają swoje prawa i obowiązki odnośnie do technologii używanej w domu, podłączania urządzeń do sieci oraz pozwalania gościom na łączenie się z siecią domową (albo siecią gościnną)?
- Czy przeszkoliłeś domowników w zakresie zagrożeń, których powinni być świadomi, na przykład phishingu? Czy jesteś pewien, że „załapali”?
- Czy upewniłeś się, że każdy członek rodziny, który używa urządzeń, zna zasady cyberhigieny (na przykład wie, żeby nie klikać łączy w wiadomościach e-mail)?
- Czy upewniłeś się, że każdy członek rodziny, który używa urządzeń, zna zasady wybierania i ochrony haseł?
- Czy upewniłeś się, że każdy członek rodziny, który używa mediów społecznościowych, zna zagrożenia związane z nadmiernym udostępnianiem informacji i rozumie, co można bezpiecznie udostępniać, a czego nie można?
- Czy upewniłeś się, że każdy członek rodziny rozumie, że najpierw trzeba myśleć, a potem działać?

Podstawy prywatności

Technologia zagraża prywatności na wiele sposobów: wszechobecne kamery regularnie Cię obserwują, firmy technologiczne śledzą Twoje zachowania online za pomocą różnych metod technicznych, a urządzenia mobilne śledzą Twoją lokalizację.

Chociaż technologia z pewnością sprawiła, że zachowywanie prywatności jest znacznie trudniejsze niż kilka lat temu, sprawa nie jest przegrana. Możesz zrobić dużo, aby lepiej chronić swoją prywatność, nawet w erze świata połączonego siecią.

Pomyśl, zanim udostępnisz

Ludzie często udostępniają zbyt dużo informacji, kiedy ktoś ich o to poprosi.

Tak, dotyczy to również Ciebie i mnie.

Weźmy na przykład formularz w typowym gabinecie lekarskim w Stanach Zjednoczonych, o którego wypełnienie pacjent jest proszony podczas pierwszej wizyty. Chociaż odpowiedzi na wiele pytań są istotne i mogą zawierać informacje, które są potrzebne do właściwej diagnozy i leczenia, inne prawdopodobnie nie. Wiele (jeśli nie większość) takich formularzy prosi pacjentów o podanie numeru ubezpieczenia społecznego. Informacje te były potrzebne dziesiątki lat temu, kiedy towarzystwa ubezpieczeń medycznych powszechnie używały ich jako identyfikatorów ubezpieczonych, ale ta niebezpieczna praktyka już dawno się skończyła. Niektóre placówki wykorzystują numer ubezpieczenia społecznego, aby zgłosić pacjenta do biur kredytowych, jeśli ten nie płaci rachunków, ale w większości przypadków pytanie to jest niebezpiecznym reliktem przeszłości, a odpowiednie pole można pozostawić puste.


ZAPAMIĘTAJ

Nawet jeśli nie podejrzewasz, że ktoś proszący Cię o dane osobowe kiedykolwiek nadużyłby zgromadzonych informacji, w miarę jak rośnie liczba instytucji dysponujących prywatnymi informacjami na Twój temat, a ilość i jakość tych danych się zwiększa, rośnie również prawdopodobieństwo, że dojdzie do naruszenia Twojej prywatności wskutek włamania.

Jeśli chcesz skuteczniej chronić swoją prywatność, rozważ, jakie ujawniasz informacje o sobie i swoich bliskich, zanim je udostępnisz. Dotyczy to interakcji z agencjami rządowymi, korporacjami, instytucjami medycznymi i innymi osobami. Jeśli nie musisz podawać prywatnych informacji, nie rób tego. Zakładając, że pozostałe czynniki pozostaną niezmienne, im mniej prywatnych informacji ujrzy „światło dzienne" i im mniej jest miejsc, w których są one przechowywane, tym mniejsze ryzyko naruszenia Twojej prywatności.

Pomyśl, zanim opublikujesz

Dobrze się zastanów, zanim opublikujesz jakiś post w mediach społecznościowych — może to mieć różne negatywne konsekwencje, łącznie z naruszeniem prywatności informacji. Przestępcy mogą na przykład wykorzystać wiedzę o Twoich relacjach rodzinnych, zatrudnieniu i zainteresowaniach do kradzieży tożsamości albo włamania się na Twoje konta przy użyciu socjotechniki.

OSTRZEŻENIE

Jeśli z własnego wyboru albo zmuszony przez politykę dostawcy używasz panieńskiego nazwiska matki jako faktycznego hasła, upewnij się, że nie ułatwiasz przestępcom znalezienia tego nazwiska poprzez wskazanie swojej matki na Facebooku albo zawieranie znajomości na Facebooku z wieloma kuzynami, których nazwisko jest takie samo jak nazwisko panieńskie matki. Aby poznać nazwisko panieńskie czyjejś matki, często wystarczy wybrać z listy znajomych na Facebooku najczęściej występujące nazwisko, które nie jest takie samo jak nazwisko posiadacza konta.

Udostępnianie informacji o dzieciach i planach może prowadzić do najróżniejszych problemów, w tym potencjalnie porwania, włamania do Twojego domu, kiedy jesteś w drodze do pracy, oraz do innych szkodliwych działań.

Udostępnianie wpisów dotyczących zdrowia może prowadzić do ujawnienia wrażliwych, prywatnych informacji. Na przykład zdjęcia lub dane lokalizacyjne wskazujące, że dana osoba przebywała w pewnej instytucji medycznej, mogą ujawnić, że osoba ta cierpi na jakąś chorobę, w której leczeniu specjalizuje się dana placówka.

Udostępnianie wpisów lub zdjęć może wpłynąć na osobiste relacje użytkownika i upublicznić prywatne informacje na ich temat.

Udostępnianie wpisów lub zdjęć może ujawnić prywatne informacje o potencjalnie kontrowersyjnych działaniach użytkownika, takich jak spożywanie alkoholu, korzystanie z rekreacyjnych narkotyków, używanie broni, uczestnictwo w kontrowersyjnych organizacjach itd. Nawet ujawnienie, że ktoś przebywał w określonym miejscu w określonym czasie, może nieumyślnie naruszyć prywatność wrażliwych informacji.

ZAPAMIĘTAJ

Pamiętaj również, że problem nadmiernego udostępniania informacji nie jest ograniczony do sieci społecznościowych. To samo dotyczy czatów, poczty elektronicznej i grup dyskusyjnych. Czasem ludzie nie uświadamiają sobie, że udostępniają za dużo informacji, a czasem przypadkowo wklejają niewłaściwe dane lub załączają niewłaściwe pliki do wiadomości e-mail.

Ogólne wskazówki dotyczące prywatności

Poza tym, że zaczniesz zastanawiać się przed opublikowaniem informacji, możesz zmniejszyć ryzyko związane z ich nadmiernym udostępnianiem na kilka innych sposobów:

- **Używaj ustawień prywatności w serwisach społecznościowych**. Oprócz nieudostępniania prywatnych informacji (patrz poprzedni punkt) upewnij się, że Twoje ustawienia prywatności w serwisach społecznościowych chronią dane przed wyświetlaniem przez ogół użytkowników — chyba że post jest przeznaczony do publicznej konsumpcji.
- **Ale na nich nie polegaj**. Nigdy jednak nie licz na to, że ustawienia bezpieczeństwa w mediach społecznościowych zagwarantują prywatność Twoich informacji. Regularnie odkrywane są poważne luki, które ograniczają efektywność środków kontroli bezpieczeństwa na różnych platformach.

- **Trzymaj prywatne dane z dala od chmury, chyba że je zaszyfrujesz**. Nigdy nie przechowuj prywatnych informacji w chmurze bez ich uprzedniego zaszyfrowania. Nie licz na to, że szyfrowanie zapewnione przez dostawcę usług chmurowych zagwarantuje Ci prywatność. Jeśli dostawca padnie ofiarą włamania, w niektórych przypadkach może to również naruszyć bezpieczeństwo szyfrowania. Jeśli więc musisz zapisać wrażliwe informacje w chmurze, zaszyfruj je sam przed przesłaniem — niezależnie od szyfrowania używanego przez dostawcę. Są aplikacje, które upraszczają to w przypadku największych usług chmurowych, na przykład automatycznie szyfrując i kopiując do chmury wszystkie pliki umieszczone w specjalnym folderze na Twoim komputerze.

  Nie przechowuj prywatnych informacji w aplikacjach chmurowych zaprojektowanych pod kątem udostępniania i współpracy. Nie zapisuj na przykład listy haseł, fotografii prawa jazdy lub paszportu ani poufnych informacji medycznych w dokumencie Google. Może wydawać się to oczywiste, ale wiele osób i tak to robi.

- **Wykorzystaj ustawienia prywatności w przeglądarce — a najlepiej używaj sieci Tor**. Jeśli za pomocą przeglądarki uzyskujesz dostęp do materiałów, które nie powinny być wiązane z Tobą, włącz przynajmniej tryb prywatny/incognito (który oferuje tylko częściową ochronę), a jeśli to możliwe, użyj przeglądarki takiej jak Tor Browser Bundle (która oferuje utajniony routing, rygorystyczne domyślne ustawienia prywatności oraz różne wstępnie skonfigurowane dodatki chroniące prywatność).

  Jeśli nie zachowasz ostrożności podczas korzystania z przeglądarki, będziesz śledzony. Jeśli na przykład wyszukasz szczegółowe informacje o jakimś schorzeniu w zwykłym oknie przeglądarki, ktoś zapewne spróbuje wykorzystać te dane. Prawdopodobnie widziałeś efekty takiego śledzenia, na przykład kiedy na jednej stronie pojawiają się reklamy dotyczące czegoś, co wyszukiwałeś na drugiej.

- **Nie publikuj prawdziwego numeru swojego telefonu komórkowego**. Zdobądź numer do przekazywania połączeń w usłudze takiej jak Google Voice i podawaj go zamiast prawdziwego numeru. Pomaga to zabezpieczyć się przed wieloma zagrożeniami — podmianą SIM, spamem itd.

- **Przechowuj prywatne materiały offline**. Szczególnie wrażliwe materiały najlepiej przechowywać offline, na przykład w ognioodpornym sejfie albo bankowej skrytce depozytowej. Jeśli musisz przechowywać je w postaci elektronicznej, zapisz je w komputerze bez dostępu do sieci.

- **Szyfruj wszystkie prywatne informacje**, takie jak dokumenty, obrazy, wideo itd. Jeśli nie jesteś pewien, czy coś powinno być zaszyfrowane, zapewne powinieneś to zaszyfrować.

- **Jeśli korzystasz z czatów online, używaj szyfrowania „od końca do końca”**. Wszystkie Twoje wiadomości tekstowe wysłane za pośrednictwem zwykłej sieci telefonicznej (SMS-y) mogą być potencjalnie przeczytane przez osobę z zewnątrz.

Najlepiej nie udostępniać wrażliwych informacji na piśmie. Jeśli musisz to zrobić, zaszyfruj dane.

Najprostszym sposobem zabezpieczenia danych jest użycie aplikacji czatu, która oferuje szyfrowanie „od końca do końca” (*end-to-end*). Oznacza to, że wiadomości są szyfrowane w Twoim urządzeniu oraz deszyfrowane w urządzeniu odbiorcy i odwrotnie, przez co dostawca usług w praktyce nie jest w stanie ich odszyfrować; jeśli hakerzy włamią się do serwerów dostawcy, odczytanie Twoich wiadomości zajmie im znacznie więcej czasu. (Czasem dostawcy twierdzą, że hakerzy w ogóle nie mogą odczytać takich wiadomości, co nie jest do końca prawdą z dwóch przyczyn: 1. Hakerzy mają dostęp do metadanych, na przykład z kim czatowałeś i kiedy; 2. Jeśli hakerzy przejmą kontrolę nad wystarczającą liczbą serwerów, mogą umieścić w sklepie z aplikacjami „zatrutą” wersję aplikacji zawierającą jakieś „tylne drzwi”). Prawdopodobnie najpopularniejszą aplikacją, która używa szyfrowania „od końca do końca”, jest WhatsApp.

- **Praktykuj właściwą cyberhigienę**. Ponieważ znaczna część informacji, które chcesz chronić, jest przechowywana w postaci elektronicznej, praktykowanie właściwej cyberhigieny ma kluczowe znaczenie dla zachowania prywatności. Wskazówki znajdziesz w rozdziale 18.

WŁĄCZANIE TRYBU PRYWATNEGO

Aby włączyć tryb prywatny:

- **Chrome**. Naciśnij *Control+Shift+N* albo wybierz z menu polecenie *Nowe okno incognito*.
- **Firefox**. Naciśnij *Control+Shift+P* albo wybierz z menu polecenie *Nowe okno prywatne*.
- **Opera**. Naciśnij *Control+Shift+N* albo wybierz z menu polecenie *Nowe okno prywatne*.
- **Edge**. Naciśnij *Control+Shift+N* albo wybierz z menu polecenie *Nowe okno InPrivate.*
- **Vivaldi**. Naciśnij *Control+Shift+N* albo wybierz z menu polecenie *Nowe okno prywatne*.
- **Safari**. Naciśnij *Command+Shift+N* albo wybierz z menu *Plik* polecenie *Nowe okno prywatne*.
- **Tor Browser Bundle**. W tej wersji Firefoksa tryb prywatny jest włączony domyślnie (a sieć Tor dodatkowo chroni prywatność, jak opisano w rozdziale 21.).

Bezpieczna bankowość online

Unikanie bankowości online z powodu obaw o bezpieczeństwo jest po prostu niepraktyczne dla większości osób żyjących w dzisiejszych czasach. Zwiększałoby to zresztą podatność na inne zagrożenia związane z bankowością telefoniczną lub osobistą.

Na szczęście nie trzeba rezygnować z wygód bankowości online, aby pozostać bezpiecznym. Ja sam doskonale zdaję sobie sprawę z ryzyka, ponieważ korzystam z bankowości internetowej, od kiedy usługa ta została wprowadzona po raz pierwszy przez kilka dużych instytucji finansowych w połowie lat 90. jako zamiennik „wdzwanianych" usług telefonicznych.

Oto kilka rad, które pomogą Ci bezpieczniej korzystać z bankowości online:

- **Twoje hasło do banku internetowego powinno być mocne, niepowtarzalne i zapamiętane**. Nie powinieneś przechowywać go w bazie danych, menedżerze haseł ani w żadnej innej formie elektronicznej. (Jeśli chcesz zapisać je na papierze i przechowywać w skrzynce depozytowej, prawdopodobnie będzie bezpieczne, ale rzadko jest to konieczne).
- **Wybierz losowy kod PIN do karty bankomatowej i (lub) na potrzeby identyfikacji telefonicznej**. Żaden PIN, którego używasz do celów bankowych, nie powinien być powiązany z innymi znanymi Ci informacjami. Nie wykorzystuj ponownie PIN-u, którego używasz do innych celów, i nie twórz innych PIN-ów ani haseł na podstawie tego, który wybrałeś dla karty bankomatowej. Nigdy nie zapisuj swojego PIN-u. Nigdy nie dodawaj go do żadnego pliku komputerowego. Nigdy nie podawaj nikomu swojego PIN-u, nawet pracownikom banku.
- **Dowiedz się, czy bank może wystawić Ci kartę bankomatową, która nie może być używana jako karta debetowa**. Choć takie karty nie pozwalają kupować towarów i usług, jeśli robisz zakupy przy użyciu kart kredytowych, nie potrzebujesz funkcji zakupu w karcie bankomatowej. Uniemożliwiając użycie jej jako karty debetowej, zwiększasz prawdopodobieństwo, że tylko ktoś, kto zna Twój PIN, będzie mógł wypłacić pieniądze z konta. Być może równie ważne jest to, że taka „okaleczona" karta bankomatowa nie może zostać wykorzystana przez oszustów do robienia zakupów.


ZAPAMIĘTAJ

Jeśli oszust użyje Twojej karty debetowej, tracisz pieniądze, a ich odzyskanie bywa problematyczne. Jeśli użyje Twojej karty kredytowej, nie tracisz żadnych pieniędzy, chyba że dochodzenie dowiedzie, że to Ty próbowałeś je zdefraudować.

- **Loguj się w banku internetowym tylko z zaufanych urządzeń, które kontrolujesz, w których zainstalowałeś oprogramowanie zabezpieczające i które są stale aktualizowane**.
- **Loguj się w banku internetowym tylko z zabezpieczonych sieci, którym ufasz**. Jeśli jesteś w podróży, używaj sieci swojego operatora komórkowego, a nie publicznego Wi-Fi. (Więcej informacji na ten temat znajdziesz w rozdziale 21.). Nie loguj się w banku ani w innych wrażliwych aplikacjach w miejscach, w których operatorów komunikacyjnych podejrzewa się o próby zainfekowania urządzeń podłączających się do ich sieci złośliwym oprogramowaniem.
- **Loguj się w banku internetowym z przeglądarki internetowej albo oficjalnej aplikacji banku**. Nigdy nie loguj się z aplikacji firmy trzeciej albo aplikacji pobranej z jakiegokolwiek innego miejsca niż oficjalny sklep z aplikacjami dla Twojej platformy.

- **Zapisz się na powiadomienia od banku**. Skonfiguruj swoje konto tak, żebyś był powiadamiany SMS-em za każdym razem, kiedy zostanie dodany nowy odbiorca płatności, zostaną wypłacone pieniądze itd.
- **Korzystaj z uwierzytelniania wieloskładnikowego i chroń każde urządzenie używane do takiego uwierzytelniania**. Jeśli na przykład generujesz hasła jednorazowe na swoim telefonie, a ktoś Ci go ukradnie, drugi składnik uwierzytelniania będzie (przynajmniej czasowo) dostępny dla złodzieja, a nie dla Ciebie.
- **Nie pozwalaj przeglądarce na zapisanie hasła do banku internetowego**. Twoje hasło do bankowości online nie powinno być nigdzie zapisane, a już na pewno nie w systemie, który wprowadzi je automatycznie, kiedy ktoś użyje Twojej przeglądarki.
- **Wprowadzaj adres URL banku za każdym razem, kiedy odwiedzasz jego stronę**. Nigdy nie klikaj łączy do strony.
- **Jeśli to możliwe, do bankowości online używaj innego komputera niż do zakupów internetowych, czytania poczty i przeglądania mediów społecznościowych**. Jeśli jest to niemożliwe lub niepraktyczne, używaj innej przeglądarki internetowej — i pamiętaj o jej aktualizowaniu.

Dodatkowym środkiem ostrożności może być skonfigurowanie przeglądarki tak, aby zapamiętała błędne hasło do witryny. Jeśli ktoś dostanie się do Twojego laptopa lub telefonu, będzie mniej prawdopodobne, że uda mu się zalogować w tej witrynie przy użyciu Twoich poświadczeń.

- **Zabezpiecz wszystkie urządzenia, na których używasz bankowości online**. Obejmuje to bezpieczeństwo fizyczne (nie zostawiaj telefonu na stole w restauracji, kiedy idziesz do łazienki), ustawienie hasła do odblokowywania urządzenia oraz włączenie zdalnego wymazywania danych.
- **Monitoruj swoje konto pod kątem nieautoryzowanej aktywności**.

Bezpieczne używanie urządzeń inteligentnych

Jak opisuję szczegółowo w rozdziale 18., urządzenia inteligentne i tzw. internet rzeczy stwarzają najróżniejsze zagrożenia. Oto kilka rad, które pomogą Ci bezpieczniej korzystać z takich urządzeń:

- **Upewnij się, że żadne z Twoich urządzeń IoT nie stworzy zagrożenia w przypadku awarii**. Nigdy nie doprowadzaj do sytuacji, w której inteligentny zamek uniemożliwiłby Ci opuszczenie pokoju w czasie pożaru albo wpuścił włamywaczy do domu podczas awarii zasilania lub sieci.
- **Jeśli to możliwe, urządzenia IoT powinny działać w innej sieci niż Twoje komputery**. Sieć IoT powinna być chroniona przez zaporę.

- **Dbaj o aktualizowanie urządzeń IoT**. Hakerzy wykorzystują luki w zabezpieczeniach urządzeń IoT, aby przejmować nad nimi kontrolę i przeprowadzać dalsze ataki. Jeśli urządzenie ma funkcję automatycznej aktualizacji oprogramowania układowego, warto ją włączyć.
- **Prowadź pełną, aktualną listę wszystkich urządzeń podłączonych do Twojej sieci**. Prowadź też listę urządzeń, które nie są obecnie podłączone, ale autoryzowane do łączenia się z siecią.
- **Jeśli to możliwe, odłączaj urządzenia, kiedy ich nie używasz**. Jeśli urządzenie nie jest dostępne w sieci, oczywiście nie może być zhakowane przez kogoś, kto nie ma do niego fizycznego dostępu.
- **Chroń wszystkie urządzenia hasłami**. Nigdy nie używaj haseł domyślnych, z którymi dostarczono urządzenia. Każde urządzenie powinno mieć unikatowy identyfikator logowania i hasło.
- **Sprawdź ustawienia urządzeń**. Wiele urządzeń ma domyślne ustawienia, które pod względem bezpieczeństwa wołają o pomstę o nieba.
- **Dbaj o fizyczne i cyfrowe bezpieczeństwo swojego smartfona**. Prawdopodobnie działają w nim aplikacje, które mają dostęp do niektórych lub wszystkich Twoich urządzeń.
- **Jeśli to możliwe, wyłącz niepotrzebne funkcje urządzeń**. Ogranicza to „powierzchnię ataku", czyli liczbę punktów, przez które haker może potencjalnie włamać się do urządzenia, jednocześnie zmniejszając prawdopodobieństwo, że ujawni możliwą do wykorzystania lukę w zabezpieczeniach oprogramowania.

  Funkcja Universal Plug and Play (UPnP) upraszcza konfigurację urządzenia, ale zarazem ułatwia hakerom odkrywanie urządzeń i atakowanie ich, m.in. dlatego, że wiele implementacji UPnP zawiera luki w zabezpieczeniach, UPnP czasem pozwala złośliwemu oprogramowaniu omijać procedury bezpieczeństwa w zaporach sieciowych, a hakerzy czasem mogą wykorzystać UPnP do uruchamiania poleceń w routerach.
- **Nie podłączaj urządzeń IoT do niezaufanych sieci**.

Bezpieczeństwo kryptowalut

Upraszczając, termin **kryptowaluta** odnosi się do „pieniędzy" śledzonych przy użyciu księgi rachunkowej, której kopie są rozpowszechniane wśród „węzłów" zarządzających siecią kryptowalutową (co oznacza, że liczne osoby na całym świecie mają kopię księgi rachunkowej z listą wszystkich transakcji, których kiedykolwiek dokonano przy użyciu tej konkretnej kryptowaluty). Większością kryptowalut zarządza się nie centralnie, a poprzez konsensus większości użytkowników, przy czym definicja tego, kto jest uwzględniany w obliczaniu większościowego konsensusu, zależy od kryptowaluty.

Najlepiej znaną i historycznie pierwszą kryptowalutą jest bitcoin. Kiedy ktoś posiada bitcoina (lub jego ułamek), informacja o tym jest przechowywana w księdze rachunkowej — nie pod nazwiskiem właściciela, ale pod jego adresem. Na przykład adres 123 otrzymał jednego bitcoina od adresu 321, co oznacza, że adres 123 ma teraz jednego bitcoina.

Właściciel bitcoina w rzeczywistości niczego nie posiada; ma po prostu kontrolę nad odpowiednim adresem bitcoin. W poprzednim przykładzie osoba, która ma tajny klucz niezbędny do autoryzowania wszystkich transakcji dokonywanych z adresu 321, kontroluje wszystkie bitcoiny przechowywane pod tym adresem.

Choć omówienie technologii używanych przez bitcoina wykracza poza ramy niniejszej książki, ważną kwestią bezpieczeństwa, o której powinny wiedzieć osoby zainteresowane kryptowalutami, jest to, że tajny klucz wymagany do dokonywania transakcji zasadniczo definiuje własność. Gdyby właściciel bitcoina spod adresu 321 zgubił klucz do tego adresu, nie miałby już dostępu do przechowywanego tam bitcoina i prawdopodobnie na zawsze straciłby wszystkie środki przechowywane pod tym adresem.

Podobnie, gdyby ktoś inny uzyskał klucz do adresu 321 i wykorzystał go bez upoważnienia właściciela do przekazania bitcoinów pod inny adres, transakcja ta w niemal wszystkich przypadkach zostałaby uznana za poprawną, a prawowity właściciel straciłby bitcoiny.

ZAPAMIĘTAJ

W związku z tym ochrona tajnych kluczy związanych z posiadanymi kryptowalutami ma, nomen omen, kluczowe znaczenie.

Jednym z rozwiązań jest przechowywanie tajnych kluczy w specjalnym urządzeniu nazywanym portfelem sprzętowym. Urządzenie takie przechowują klucze offline, dzięki czemu nie ma ryzyka, że zostaną ukradzione przez hakera. Kiedy prawowity właściciel chce przeprowadzić transakcję kryptowalutową, musi podłączyć sprzętowy portfel do komputera (często przez USB) i odblokować portfel (zwykle za pomocą jakiegoś hasła), aby wykorzystać klucze przechowywane w portfelu.

ZAPAMIĘTAJ

Portfele sprzętowe nie przechowują kryptowaluty, ale klucze używane do autoryzowania operacji na określonych adresach w księdze rachunkowej.

Pamiętaj również, że kiedy ktoś trzyma kryptowalutę na giełdzie kryptowalutowej, to giełda przechowuje związane z nią klucze. Jeśli ktoś wykradnie poświadczenia użytkownika służące do logowania się na giełdzie, może ukraść również jego kryptowalutę.


PROGRAM
PARTNERSKI
GRUPY HELION
1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ
Zmień swoją stronę WWW w działający bankomat!
Dowiedz się więcej i dołącz już dzisiaj!
http://program-partnerski.helion.pl
GRUPA
Helion

Prosto o cyberbezpieczeństwie

Cyberbezpieczeństwo dotyczy dziś każdego. Nowe, zaktualizowane wydanie *Cyberbezpieczeństwa dla bystrzaków* pomoże Ci chronić osobiste informacje i zabezpieczyć dane biznesowe. Dowiedz się, co się dzieje z plikami, które przechowujesz online. Pracuj bezpiecznie w domu i unikaj dezinformacji. Upewnij się, że Twoje zdjęcia, hasła i inne ważne dane są chronione przed hakerami. A jeśli wpadną w niepowołane ręce? Wyjaśniamy, jak zidentyfikować problem i jak go rozwiązać. Pozwól, by ta książka stała się Twoim cyfrowym obrońcą.

W książce:

- broń się przed cyberatakami
- określ mocne i słabe punkty swojego cyberbezpieczeństwa
- skuteczniej chroń dane osobowe i biznesowe
- usuwaj skutki naruszeń bezpieczeństwa
- poznaj możliwości kariery w branży cyberbezpieczeństwa

Joseph Steinberg to mistrz cyberbezpieczeństwa. Jest jedną z nielicznych osób, które zdobyły komplet zaawansowanych certyfikatów w dziedzinie bezpieczeństwa informacji, między innymi CISSP®, ISSAP®, ISSMP® i CSSLP®. Autor kilku książek poświęconych bezpieczeństwu cyfrowemu, obecnie jest konsultantem w zakresie bezpieczeństwa informacji i biegłym sądowym w sprawach związanych z cyberbezpieczeństwem.

dla bystrzaków

Cena: 69,00 zł

ISBN 978-83-8322-286-8