

Bezpieczeństwo w sieci - trata tożsamości i

życzenie?



Myśl przewodnia: „Gdyby postawić pytanie, co jest ważniejsze: sprzęt, oprogramowanie czy system, to chyba najlepsza odpowiedź brzmi: „ludzie, którzy potrafią z niego korzystać. „

Wyobraź sobie, iż co roku wraz z obchodzonym dniem bezpiecznego Internetu, każdy komputer, router i jakiegokolwiek inne urządzenie sieciowe jest zabezpieczone w taki sposób, że każda niepowołana osoba nie jest w stanie uzyskać dostępu do zasobów cudzej maszyny. Czy sądzisz zatem, że w tak optymistycznej wersji wydarzeń, Internet można nazwać bezpiecznym?

Do tego dążymy. Programiści piszą aplikacje pozwalające zabezpieczyć komputer w domu, szkole, pracy, w czasie gdy cyberprzestępcy wyszukują błędów i luk w dziełach programistów, umożliwiając tym samym uzyskanie nieautoryzowanego dostępu do zasobów Twojego komputera. Następnie specjaliści ds. bezpieczeństwa wydają audyty, „łatają” znalezione błędy by poprawić bezpieczeństwo samych aplikacji, gdy cyberprzestępcy wciąż walczą o „nie swoje”.

W dzisiejszych czasach nie wystarczy zabezpieczyć programowo komputer w 100% (czego notabene nie da się osiągnąć) by można stwierdzić iż korzystając z niego jesteś w pełni bezpieczny w sieci. Zatem kukuł tego dowiesz się jak zabezpieczyć siebie, nie swój komputer podczas korzystania z sieci.

Ewolucja - niekończąca się studnia

Dwadzieścia lat temu, pojęcie komputer było profesjonalnym określeniem zaawansowanego urządzenia zajmującego sporą przestrzeń niemałego pomieszczenia. Dziś, liczba

Komputerów w przeciętnym gospodarstwie domowym przekracza liczbę mieszkańców. Człowiek nato miast, nie używając naco dzień komputera jest nazywany „staromodnym”.

Gdy chcemy skontaktować się ze znajomym z bloku obok, uruchamiamy komunikator, gdy chcemy dowiedzieć się co dzieje się u cioci z zagranicy, piszemy e-maila, jeśli nato miast dzwoniemy, robimy to za pośrednictwem telefonu internetowego. By zakupić meble do sypialni, nie trzeba wybierać się do sklepu, aco najwyżej do kuchni po kawę by wybranie internet resującyca nas meble byfo przyjemniejsze. Oczywiście po wyborze należy uściśnić płatność, którą umożliwiają nam przelewy internetowe. Jak widać więc, z auto psji życia codziennego niejednego z nas, można wywnioskować że zdecydowana większość z nas żyje w internetcie. Zarówno jak i w życiu realnym, tak też w życiu wirtualnym, czekają na nas zagrożenia. Ewolucja nato miast tej technologii, sprzyja tylko rosnącemu niebezpieczeństwu napływającemu z sieci.

Sens cyberterroryzmu - władza.



W internecie towarem jest wszystko - w szczególności informacje o jego użytkownikach.

Robiąc małą ankietę odnośnie obchodzonego dnia bezpiecznego Internetu, zauważyłem jedną spójność w wypowiedziach, która w gruncie rzeczy mnie nie zdziwiła. Ludzie nato proste (bądź też nie) pytanie: Czym dla Ciebie jest bezpieczny Internet? Odpowiadał zazwyczaj - „Gdy mamy zainstalowany antywirus, firewall.”, „Gdy wiemy że nikt nie odczyta naszych plików tekstowych, nie obejrzy zdjęć i nie uruchomi aplikacji pochodzących z naszego komputera.” Jest to wszystko prawdą, jednak bardzo niewiele z nas zdaje sobie sprawę, a może zbyt poobowornie do tej sprawy podchodzi iż korzystając codziennie z Internetu zostawiamy po sobie masę śladów które w nieodpowiedni rękach stać się mogą niebezpiecznym narzędziem.

Czym są ślady o których mówimy? Oczywiście dane personalne osoby korzystającej z Internetu. Imię i nazwisko, miejsce zamieszkania, data i miejsce urodzenia, pesel, numer telefonu, adres e-mail, imiona rodziców, siostry, ulubiona, rozrywka, praca, informacje odnośnie naszego przeciętnego dnia..

Zdziwiony? Pomyśl, czy nigdy w życiu nie napisałeś na forum, grupie dyskusyjnej, na czacie internetowe wym jakiegokolwiek informacji o sobie? Co lubisz robić, czym się zajmujesz, jakie masz plany na przyszłość.. A swoje dane? Czy nigdy ale to nigdy, nie wypełniłeś za pośrednictwem Internetu żadnego formularza zawierającego Twoje dane osobowe? Nie jest istotne, czy jest to formularz przy zakładaniu konta bankowego czy formularz pochodzący z prywatnej strony - bo nigdy nie mamy 100% pewności, czy to co widzimy, jest w rzeczywistości tak tym jak o tym piszą. Można śmiało rzec, że żadna informacja w sieci nie ginie, a znajduje swoje miejsce, gdzie w połączeniu z innymi informacjami, tworzy elektroniczną księgę wiedzy o użytkownikach.

Portal, który ostatnimi czasy bije rekordy popularności i służy do wyszukiwania szkolnych znajomych, jest tego szczególnym przykładem. Zostawiamy tam ogrom wiedzy o nas samych. Nikt nie mówi tutaj o niekorzystaniu z tego portalu, jednak należy robić to rozważnie. Celem portalu jest znalezienie kontaktu do znajomych ze szkolnych lat. Często omylnie wykorzystujemy go do zdecydowanie innych celów, co z kolei mogą wykorzystać niepowołane osoby. Część osób decyduje się na korzystanie z opcji poprawiającej bezpieczeństwo i ukrycie informacji o sobie, przykładowo jedynie dla grona użytkowników dodanych do swoich znajomych. Jednak czy zastanawiamy się czasem, czy osoba, która rzekomo posiada profil o imieniu x,y jest w rzeczywistości tą osobą? Po co korzystamy z opcji 'ukryj dla znajomych', skoro bezmyślnie czasem akceptujemy kogoś przypadkiem? Głównie chodzi tutaj o rzekome kluby czy profile funkcyjne, które mają w zdecydowanej większości jeden cel - pozyskać informacje o jego użytkownikach.

Nie przekładajmy cyfrowej informacji ponad wszystko. Kontaktujmy się ze znajomymi również w tradycyjny sposób, a nie będziemy zmuszeni wyszukiwać informacji kontaktowych do ludzi w portalach stworzonych do tego celu.

Informacja, informacja. Gdzie jesteś?

Fora internetowe, komunikatory, portale społecznościowe, wszelkiego rodzaju czaty internetowe, a nawet prowadzone przez siebie strony blogów czy też strony internetowe. Co z tego że możemy podawać swój login zamiast imienia i nazwiska, skoro powielając ten sam login w wielu portalach o różnych tematykach (tym samym informację o tobie są coraz to szersze) dajemy osobom zainteresowanym naszą tożsamością, gdzie informacje jak tutaj. Niestety, wciąż w Internecie pozostawiamy po sobie tyle śladów (w przynajmniej części nieświadomie) że nasze dane osobowe a nawet hasła można wygooglować!

Wielu ludzi twierdzi że chroni się przed wyłudzeniami danych osobowych i informacji o własnej osobie nie rozsiwając idź na lewo i prawo. Fakt jednak jest taki, że często nie jesteśmy świadomi o tym że ktoś pozyskał nasze dane osobowe. Przykładem poparty autopsją - tematem na czasie jest oczywiście praca, najczęściej za granicą. Cyberprzestępca (tak będziemy nazywać osobę która próbuje wyłudzić nasze dane osobowe) podaje na portalu o nie małej popularności ogłoszenie - dam pracę. Piszę więc warunki, adres firmy (często adres ten jest poprawnym adresem firmy, jednak autorem ogłoszenia jest osoba zupełnie niezwiązana z nią) i proszę o przesłanie osób zainteresowanych ogłoszeniem swoje CV oraz skan dowodu osobistego bądź też w celu większej wiarygodności - prawa jazdy (w ogłoszeniu podana adnotacja - wymagane prawo jazdy kate gorn 'B') Oczywiście nigdy odzemu nie otrzymujemy.

Przecież rozważając opcję wysłania przykładowo swojego CV zadajemy sobie pytanie - co nam szkodzi? Mogę wysłać kopię swojego CV i nie stanie, a może trafi się praca o którą się staram. Nie zadajemy sobie jednak pytania czy firma która się reklamuje (ogłoszenie w Internecie przecież może umieścić niemal każdy) jest w rzeczywistości tą firmą. Warto wspomnieć że najczęściej w tego typu ogłoszeniach niepoprawny jest jedynie e-mail którym przesyłamy informacje do cyberprzestępcy! Należy więc przed przesłaniem jakichkolwiek informacji o sobie, znaleźć informację o danej instytucji w bazie firm i skontaktować się telefonicznie by zweryfikować wiarygodność ogłoszenia.

Gdzie granica?

Przeskanowany dowód osobisty jest dokumentem. Dokumentem w wersji elektronicznej, lecz zawsze dokumentem. Mamy tam wypisane swoje podstawowe dane personalne i przede wszystkim własnoręczny podpis czyli w tym przypadku tzw. podpis cyfrowy. W jakim celu może posłużyć przeskanowany dowód osobisty? W bardzo szerokim. Przede wszystkim podszycanie się pał jego właściciela. Przy dzisiejszym rozwoju technologii możemy dzięki niemu założyć konto bankowe na tą osobę, a nawet zrobić zakupy na nie-małe sumy. Zastanówmy się przez chwilę, jak byśmy się poczuli, gdyby ciężarówka wypełniona sprzętem AGD/RTV stojąca przed naszym domem czekała na rozładunek, a Ty sam nie masz pojęcia skąd to wszystko się wzięło - wiesz jednak że kierowca wymaga od Ciebie pokrycia kosztów?

Kolejnym scenariuszem jest popełnienie przestępstwa w Twoim imieniu. Brzmi nieprzekonująco? Wyobraźmy sobie więc, że cyberprzestępca pozyskał Twój dowód tożsamości. Celowo pozostawia go na dysku swojego komputera, wybiera się w miejsce gdzie może skorzystać z darmowego Internetu bezprzewodowego i przykładowo włamuje się na stronę banku. Laptop porzuca zacierając przy tym na pozór ślady, a gdzieś w 'starym' folderze plików tymczasowych rzekomo przypadkowo zostawia swój przeskanowany dowód osobisty. Lub nawet niekoniecznie. Przecież odzyskiwanie danych dziś z spalonych dosłownie dysków czy uszkodzonych mechanicznie nie jest niczym niezwykłym. Czy wiesz już gdzie policja wybierze się najpierw, by wyjaśnić tą sprawę?

Może sprzedaż. Cyberprzestępca tworzy własną witrynę internetową, bądź też sklep. Korzystając z innych (tylko te ostatnie!) nieistotnych danych typu baza adresów mail, rozsyła reklamy. Ma możliwość sprzedaży wszelkiego rodzaju sprzętu elektronicznego, świadczenia usług lub czegokolwiek innego mogącego zainteresować szerokie grono użytkowników. Wszędzie wyraża się profesjonalnie, a możliwość (z której zapewne skorzysta nie jeden) przesłania przeskanowanego dowodu osobiste go, utwierdza klienta w przekonaniu że będzie prowadził interesy z osobą kompetentną. W tym przypadku czy występujemy w rolę klienta, czy osoby której cyberprzestępca pozyskał przeskanowany dokument tożsamości - jesteśmy ofiarami.

Można powiedzieć że nie każda informacja o nas nie jest tak cenna, jednak wystarczy tylko troszkę wyobraźni i postawienia się w perspektywie cyberprzestępcy, by rozwiać te wątpliwości.

Wiele osób pytanych przeze mnie odnośnie podawania numeru telefonu w Internecie, odpowiada: „Cóż może się stać? Ktoś zadzwonił i powie mi że zostałem zhakowany?” - dodają ironicznie.

Przeanalizujmy więc sytuację może mniej poważną niż powyższe. Osoba, nie dążąca nas sympatią, dorywa w Internecie nasz numer telefonu. Postanawia zrobić sobie mały przyjemny żart. W portalu aukcyjnym lub ogłoszeniowym umieszcza informację o bardzo atrakcyjnej ofercie sprzedaży przykładowo samochodu, jednak z uwagą na drugo zmianowy plan pracy, prosi o telefony tylko po godzinie 23. Jeśli powieł to ogłoszenie w kilku serwisach, albo będziemy musieli wyłączać swoje telefony na noc które przecież są nam potrzebne - a gdyby coś się stało? Lub jesteście zmuszeni zmienić numer.

Pomysłów jest miliony. Nie cel jednak by wypisać wszystkie lub większość z nich i robić wszystko na przekór temu, a by „jedynie” czujnie podejmować nawet najprostsze kroki, zwykle kliknięcia myszy.

Recepta na bezpieczeństwo

Recepta jest banalna, a mimo tak rzadko się do niej odwołujemy. Według niektórych wskazań. Według myśli przewodniej którą możemy przeczytać u góry artykułu, to człowiek jest narzędziem bezpieczeństwa i niebezpieczeństwa w sieci. Pamiętajmy że nigdy nie mamy pewności kto znajduje się po drugiej stronie kabla, a my możemy stać się narzędziem przestępstwa. Należy więc podawać o sobie jak najmniej informacji w sieci, trzeba myśleć o sobie samemu - postawić się w sytuacji gdybyśmy to ja był tym złym - i działać tak by utrudnić wykonanie wszelkich niemoralnych kroków. Ponadto podchodzić do wszystkiego co znajduje się w sieci z sporym dystansem i pamiętać że dzień bezpiecznego Internetu jest symbolem, a prawdziwy sens obchodzonego święta powinien być do sowany na co dzień. W Internecie nie jesteś śmy anonimowi i zawsze musimy być świadomi iż ponosimy odpowiedzialność za swoje czyny, a jeśli będziemy używać Internetu bez zachowania jakichkolwiek środków bezpieczeństwa - możemy zostać postawieni w sytuacji, że będziemy odpowiadać za czyny innych.

Podsumowanie

Prawda jest jedna - można żyć bez Internetu krótszy lub dłuższy czas, jednak skrajnie jednostki decydują się na takie rozwiązanie i najczęściej tylko po to, by sprawdzić samego siebie - czy damy radę to zrobić. Sieć Internet to oprócz rozrywki i centrum wiedzy, wygodniście które stało się już czasami codziennością i którego ciężko się wyprzeć. Dzięki rozwojowi tej technologii dziennie oszczędzamy ogromne ilości czasu i to w przyjemny sposób, więc dlaczego miałibyśmy z tego zrezygnować?

Nie widać horyzontu gdzie zaprzestaniemy jakichkolwiek działań w sieci, bo cóż za różnica czy dziennie używamy Internetu 15 minut czy pół doby, skoro używamy go niebezpiecznie? Wśród niekończącego się wyścigu o bezpieczne oprogramowanie i systemy komputerowe, starajmy się zachować czujność by uzbroić się w najlepsze narzędzie umożliwiające bezpieczeństwo w sieci - ludzkie, świadome działanie.

Mam nadzieję, że po przeczytaniu tego artykułu, strata ważnych danych takich jak prace magisterskie u schyłku ukończenia, listy kontaktów, e-maile bankowe i inne istotne dane przechowywane i przetwarzane przez Twój komputer, będą dla Ciebie błahostką, gdyż łącząc się z siecią w każdej chwili możemy stracić o wiele więcej - np. tożsamość.

Wszystkie przedstawione fakty i informacje zostały poparte autopsją - reportażem, artykułami w prasie i wszystkie powyższe, mają swoje źródło i użyte czynniki dzięki wszechobecnemu dostępowi do Internetu.

Autorzy: Krzysztof Parkitny (administrator), Florian Richter (flojet), Wiktor Kołodziejczyk (vicking)