OUCH! | Luty 2015

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W TYM NUMERZE..

Bezpieczeństwo w podróży

Wstęp

W tym wydaniu opisujemy sposoby jak bezpiecznie podłączyć się i pracować w sieci w czasie podróży.

Redaktor gościnny

Steve Armstrong jest Dyrektorem Technicznym zarządzania kryzysowego w firmie Logically Secure, certyfikowanym instruktorem Instytutu SANS, a także byłym autorem kursów SANS. Jest aktywnym użytkownikiem Twittera (**@Nebulator**) oraz Google plus (**+SteveArmstrongSecurity**).

Przygotowanie

Sieci w domu czy w pracy zazwyczaj są dobrze zabezpieczone, jednak będąc w podróży każdą sieć, z którą się łączymy musimy traktować jako potencjalnie niebezpieczną. Nie wiemy, kto jeszcze z nich korzysta, ani czy nie ma potencjalnie wrogich zamiarów. Kilka prostych środków zaradczych może znacząco podnieść poziom naszego bezpieczeństwa w podróży i pomóc chronić nasze dane. Tydzień lub dwa przed podróżą:

- Sprawdź dane przechowywane na urządzeniach, które planujesz zabrać ze sobą w podróż i usuń lub przenieś te informacje, które nie są Ci w podróży potrzebne. Sprawi to, że utrata danych nie będzie aż tak znacząca w przypadku gdy Twoje urządzenie zostanie skradzione, zgubione lub zatrzymane przez służby celne lub kontrolę graniczną. Jeżeli udajesz się w podróż służbową, dowiedz się u pracodawcy czy dysponuje specjalnymi urządzeniami przeznaczonymi do pracy w czasie delegacji.
- W przypadku podróży zagranicznych, sprawdź jaki typ gniazdka elektrycznego jest używany w kraju do którego się udajesz i zaopatrz się w odpowiedni adapter. Sprawdź także stawki w roamingu Twojego operatora komórkowego, zwłaszcza dotyczące przesyłu danych, za który opłaty mogą być bardzo wysokie. Radzimy wyłączyć przesył danych w sieci komórkowej w czasie przebywania za granicą lub wykupić usługę tańszego transferu danych w roamingu.
- Zainstaluj na urządzeniach aplikacje, które umożliwią Ci śledzenie gdzie aktualnie się znajdują oraz umożliwią zdalne ich wyczyszczenie w przypadku, gdy zostaną skradzione lub zgubione. Wiele z urządzeń mobilnych ma wbudowaną taką funkcję i jedyne co trzeba zrobić to ją włączyć. Pamiętaj jednak, że takie aplikacje potrzebują dostępu do Internetu, co może wiązać się z kosztami.

Dzień lub dwa przed podróżą:

- Uaktualnij swoje urządzenia, aplikacje oraz program antywirusowy włącznie z bazą sygnatur.
- Uaktywnij zabezpieczenia w swoich urządzeniach, np. zaporę sieciową.

Bezpieczeństwo w podróży

- Zabezpiecz urządzenia silnymi hasłami, co znacząco utrudni dostęp do danych przez osoby niepowołane w przypadku, gdy stracisz swoje urządzenie.
- Zaszyfruj wszystkie urządzenia, aby uniemożliwić dostęp do swoich danych osobom niepowołanym. Niektóre z urządzeń automatycznie szyfrują dane po uaktywnieniu w nich zabezpieczenia hasłem lub kodem PIN.
- Wykonaj pełną kopię bezpieczeństwa danych na swoich urządzeniach. Zapewni to, że jeżeli nawet coś się stanie z Twoim urządzeniem, dane pozostaną bezpieczne i możliwe do odzyskania.

Podstawową zasadą zachowania bezpieczeństwa w czasie podróży jest wcześniejsze zabezpieczenie wszystkich urządzeń, ich ochrona oraz szyfrowanie całej aktywności online.

Zgubione lub skradzione urządzenia

W czasie podróży powinno się zapewnić bezpieczeństwo fizyczne swoim urządzeniom. Nie należy ich zostawiać w widocznych oraz łatwo dostępnych miejscach, np. w samochodzie, gdzie jedyne co musi zrobić złodziej, aby je ukraść, to wybić szybę. Jednym z proponowanych rozwiązań jest używanie specjalnej linki zabezpieczającej, którą można przykuć laptopa, gdy musimy go gdzieś zostawić. Kradzieże są ryzykiem, z którym muszą się liczyć wszyscy, jednak wg badań przeprowadzonych przez firmę Verizon, urządzenia są znaczenie częściej gubione niż kradzione. Zawsze upewniaj się, że masz wszystkie urządzenia przy sobie zwłaszcza gdy opuszczasz miejsce kontroli bezpieczeństwa na lotniskach, hotel, restaurację czy gdy wychodzisz z taksówki lub samolotu.

Dostęp do WiFi

Uzyskiwanie dostępu do Internetu w czasie podróży często oznacza konieczność podłączania się do publicznych sieci WiFi, np. w hotelach, kawiarniach czy na lotniskach. Takie sieci są problematyczne, bo nie dość, że nie możemy mieć pewności kto taką sieć udostępnia to także nie wiemy kto z niej w danej chwili korzysta. W związku z tym należy je traktować jako niezaufane i dlatego urządzenia powinno się wcześniej zabezpieczać i przygotowywać do podróży. Sieci WiFi wykorzystują fale radiowe do komunikacji, co także powoduje, że każdy kto jest w zasięgu ich odbioru może próbować podsłuchiwać cały ruch.

W związku z tym musisz mieć pewność, że podczas korzystania z takich sieci cała Twoja komunikacja z Internetem jest szyfrowana. Na przykład gdy przeglądasz strony WWW upewnij się, że adres każdej z przeglądanych witryn zaczyna się od **https://** oraz że w pasku adresu jest ikonka zamkniętej kłódki. Dodatkowo możesz zabezpieczyć dostęp do Internetu korzystając z wirtualnych sieci prywatnych (z ang. VPN - Virtual Private Network), które zapewniają poufność przesyłanych danych. Dostęp do takich sieci często umożliwiają pracodawcy lub możesz za niewielką opłatą wykupić

Bezpieczeństwo w podróży

taką usługę w Internecie. Jeśli nie możesz znaleźć punktów WiFi, którym jesteś w stanie zaufać, pomyśl o wykorzystaniu telefonu jako metody dostępu do Internetu. Pamiętaj jednak, że może to wiązać się z dużymi kosztami przesyłu danych, zwłaszcza w roamingu.

Komputery publiczne

Nie używaj komputerów publicznych, np. dostępnych w hotelowym lobby, bibliotekach czy kafejkach. Nigdy nie wiadomo kto korzystał z nich wcześniej i czy nie są zainfekowane złośliwym oprogramowaniem. Zawsze staraj się korzystać z urządzeń, które są pod Twoją kontrolą, a jeśli nie masz wyboru i musisz skorzystać z komputera publicznego - nigdy nie korzystaj z serwisów w których musisz podać swój login i hasło.

Dowiedz się więcej

Zasubskrybuj comiesięczny biuletyn o bezpieczeństwie komputerowym SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS dotyczące bezpieczeństwa komputerowego i osobowego.
Odwiedź http://www.securingthehuman.org i dowiedz się więcej.

Polski przekład

CERT Polska jest zespołem działającym w strukturach NASK powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w polskiej sieci Internet. Należy do organizacji FIRST, w ramach której współpracuje z podobnymi zespołami na całym świecie.
WWW: http://www.cert.pl
Twitter: @CERT_Polska
Facebook: http://facebook.com/CERT.Polska

Przydatne linki

Systemy zarządzania hasłami:	http://www.securingthehuman.org/ouch/2013#may2013
Dwustopniowe uwierzytelnianie:	http://www.securingthehuman.org/ouch/2013#august2013
Szyfrowanie:	http://www.securingthehuman.org/ouch/2014#august2014
Zabezpiecz swój nowy tablet:	http://www.securingthehuman.org/ouch/2013#december2013
Raport Verizon DBIR 2014 (ang.):	http://www.verizonenterprise.com/DBIR/2014/

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak, Paweł Jacewicz, Łukasz Siewierski