OUCH! | Luty, 2017

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu..

- **Przygotowanie**
- **Zgubione / skradzione urządzenia**
- **Dostęp do WiFi**
- **Komputery publiczne**

Bezpieczeństwo w podróży

Wstęp

Chcielibyśmy, abyś mógł zoptymalizować codzienne korzystanie z nowoczesnych technologii, także wtedy, kiedy jesteś w podróży. W bieżącym wydaniu opisujemy, jak bezpiecznie łączyć się z Internetem i korzystać z urządzeń mobilnych przebywając poza domem.

Redaktor gościnny

Mark Williams pracuje jako Enterprise Security Architect w BlueCross Blueshield w Tennessee. Jest instruktorem SANS i Przewodniczącym ISSA Chattanooga Chapter. Wiele podróżował i rozumie problematykę związaną z zabieraniem urządzeń mobilnych w drogę.

Przygotowanie

Podczas gdy sieć w Twoim domu czy miejscu pracy może być dobrze zabezpieczona, wszystkie sieci do których łączysz się w czasie podróży powinieneś traktować jako niezaufane. Nigdy nie wiesz, kto jeszcze z nich korzysta, ani jakie są jego zamiary. Poniżej znajduje się kilka prostych kroków, które pomagają wyraźnie podnieść bezpieczeństwo Twoje i Twoich danych zanim wyruszysz w podróż.

- Najbezpieczniejsza informacja, to informacja której nie posiadasz. Zweryfikuj, które dane nie będą Ci potrzebne i usuń je z zabieranych ze sobą urządzeń. Sprawi to, że utrata danych nie będzie aż tak znacząca w przypadku, gdy Twoje urządzenia zostaną skradzione, zgubione lub zatrzymane przez służby celne albo kontrolę graniczną. Jeżeli wybierasz się w podróż służbową, dowiedz się u pracodawcy czy dysponuje specjalnymi urządzeniami przeznaczonymi do pracy w czasie delegacji.
- Zabezpiecz swoje urządzenia mobilne za pomocą silnych haseł, co znacząco utrudni dostęp do danych przez osoby niepowołane w przypadku utraty sprzętu. Wykonaj ponadto pełne szyfrowanie dysku w swoim laptopie oraz danych na pozostałych urządzeniach. Dla niektórych smartfonów i tabletów funkcjonalność ta jest automatycznie uruchamiana z chwilą aktywacji blokady ekranu.
- Korzystaj z oprogramowania określającego położenie Twoich urządzeń. Dzięki niemu będziesz mógł monitorować ich lokalizację, a nawet zdalnie usunąć ich zawartość w przypadku kradzieży.
- Przed wyjazdem zaktualizuj do najnowszych wersji swoje urządzenia, aplikacje i oprogramowanie antywirusowe, włączając w to także bazy wirusów. Wiele ataków jest wymierzanych w systemy z nieaktualnym oprogramowaniem.
- Wykonaj pełną kopię danych, które posiadasz na urządzeniach. Gdyby w trakcie podróży coś się z nimi stało, masz szansę odzyskać duplikat z innej lokalizacji.
- Wybierając się za granicę, zweryfikuj u swojego operatora z jakiego planu taryfowego korzysta Twój telefon. Nierzadko

Bezpieczeństwo w podróży

operatorzy telefonii komórkowej naliczają wysokie opłaty za transmisję danych poza granicami kraju. Możesz poprosić o wyłączenie tej usługi na czas podróży. Jeżeli chcesz korzystać z transmisji danych, rozważ możliwość zakupu prepaidowej karty SIM w docelowym miejscu pobytu.

Zgubione / skradzione urządzenia

W czasie podróży zadbaj o fizyczne bezpieczeństwo swoich urządzeń. Nie zostawiaj ich w widocznych oraz łatwo dostępnych miejscach, np. w samochodzie, gdzie jedyne co musi zrobić złodziej, aby je ukraść, to wybić szybę. Kradzieże są ryzykiem, z którym muszą się liczyć wszyscy, jednak wg badań przeprowadzonych przez firmę Verizon posiadany sprzęt jest przez ludzi 100 razy częściej gubiony niż kradziony. Zawsze upewniaj się, że masz wszystkie urządzenia przy sobie, szczególnie wtedy gdy opuszczasz miejsce kontroli bezpieczeństwa na lotnisku, hotel, restaurację czy gdy wysiadasz z taksówki albo samolotu. Pamiętaj o sprawdzeniu schowków bagażowych i kieszeni w fotelach.

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

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 z dwóch powodów. Po pierwsze nie możemy mieć pewności kto taką sieć udostępnia, po drugie nie wiemy kto z niej w danej chwili korzysta. W związku z tym należy je traktować jako niezaufane, a posiadane urządzenia wcześniej zabezpieczać i przygotowywać do podróży. Warto wspomnieć, że sieci WiFi wykorzystują do komunikacji fale radiowe, co powoduje, że każdy kto znajdzie się w ich zasięgu 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 ikona 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 za niewielką opłatą możesz wykupić 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 transferu danych, zwłaszcza jeżeli korzystasz z roamingu.

Bezpieczeństwo w podróży

Komputery Publiczne

Nie używaj komputerów publicznych, np. dostępnych w hotelowym lobby, czy internetowych kafejkach do logowania się na jakiekolwiek konta lub przeglądania wrażliwych danych. Nigdy nie wiadomo kto korzystał z nich wcześniej i czy nie zostały celowo, lub przypadkowo zainfekowane złośliwym oprogramowaniem. Zawsze staraj się korzystać z urządzeń, które są pod Twoją kontrolą. Publicznie dostępne komputery są dobre, jeśli potrzebujesz uzyskać dostęp do danych, które są dostępne dla wszystkich (np. sprawdzić prognozę pogody albo wiadomości). Logowanie się z nich do kont, w których musisz podać swój login i hasło, np. Google, może stanowić zaproszenie dla hakerów.

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 securingthehuman.sans.org/ouch/archives 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

Źródła

Nowe oblicze hasła:	https://securingthehuman.sans.org/ouch/2015#april2015
Backup i odzyskiwanie danych:	https://securingthehuman.sans.org/ouch/2015#august2015
Czym jest złośliwe oprogramowanie:	https://securingthehuman.sans.org/ouch/2016#march2016
Szyfrowanie:	https://securingthehuman.sans.org/ouch/2016#june2016
OUCH Wydania archiwalne / Tłumaczenia:	https://securingthehuman.sans.org/ouch/archives

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Polski przekład (NASK/CERT Polska): Sebastian Kondraszuk, Michał Strzelczyk, Jacek Sikorski

