Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu

- **Planowanie przed podróżą**
- **Publiczne sieci**
- **Używanie publicznych komputerów**

Bezpieczny Internet w czasie podróży

REDAKTOR GOŚCINNY

Kwietniowe wydanie biuletynu OUCH! powstało pod redakcją Raula Silesa – założyciela oraz starszego analityka firmy Taddong (http://www.taddong.com). Autor wielu artykułów i instruktaży dla SANS od lat jest miłośnikiem tematyki bezpieczeństwa komputerowego (http://www.raulsiles.com). Chętni mogą śledzić informacje jakie publikuje na blogu blog.taddong.com oraz w serwisie Twitter (@taddong).

WPROWADZENIE

Korzystanie z Internetu stało się codziennością. Spodziewamy się dostępu do sieci niezależnie w jakim miejscu się znajdujemy. W czasie podróży wakacyjnych lub służbowych nie jest to zawsze łatwe. Często za dostęp musimy zapłacić, a prędkość połączenia pozostawia wiele do życzenia. Największym problemem jest jednak ryzyko związane z korzystaniem z publicznych sieci bezprzewodowych lub kafejek internetowych. Świadomość zagrożeń jakie mogą na nas czyhać, rozwaga i przygotowanie są niezbędne, by w czasie podróży czuć się bezpiecznie w sieci.

PLANOWANIE PRZED PODRÓŻĄ

Najprostszą i najbardziej efektywną metodą, która znacząco podniesie poziom naszego bezpieczeństwa w czasie podróży jest wcześniejsze wykonanie kilku łatwych czynności:

- Aktualizacja systemu operacyjnego zarówno laptopa oraz smartfonu, a także aktualizacja wszystkich zainstalowanych w nich aplikacji. Zredukuje to możliwość powodzenia ataków wykorzystujących znane i załatane luki.
- Włącznie firewalla systemowego. Dzięki temu inne komputery z sieci nie będą mogły nieuprawnione połączyć się z naszym urządzeniem.
- Włączenie oprogramowania antywirusowego oraz zaktualizowanie bazy sygnatur. Można wówczas uniknąć przypadkowej infekcji komputera, gdy otrzymany email lub plik od osoby, co do której nie mamy 100% zaufania zawierał wirusa.
- Laptopy i smartfony są łatwym łupem dla potencjalnych złodziei. Dobrym nawykiem jest zabezpieczenie dostępu do konta w komputerze hasłem, a w smartfonie kodem PIN oraz włączenie automatycznego blokowania. Utrudni to złodziejowi dostęp do danych zapisanych w urządzeniu.
- Dołączenie do urządzenia etykiety z danymi kontaktowymi właściciela daje szansę na jego odzyskanie. Oferta nagrody jest zawsze dodatkową motywacją dla znalazcy.
- W przypadku, gdy laptop lub smartfon zawiera prywatne lub poufne dane, dobrym zabezpieczeniem przed niepowołanym dostępem jest ich zaszyfrowanie. Przed wyjazdem sprawdź polityki bezpieczeństwa w Twojej firmie, aby

Bezpieczny Internet w czasie podróży

dowiedzieć się jakiego oprogramowania najlepiej do tego celu użyć.

- Jeżeli opuszczając miejsce pracy uruchamiamy automatyczne powiadamianie o nieobecności, postarajmy się znaleźć współpracownika, który może posłużyć jako alternatywny kontakt. Dobrą praktyką jest także limitowanie odpowiedzi autorespondera jedynie do adresów znajdujących się w książce adresowej.
- Wcześniejszy kontakt z działem IT w celu sprawdzenia jakie usługi są dostępne dla pracowników będących poza firmą może znacznie wspomóc i przyspieszyć rozwiązywanie problemów jakie możemy napotkać będąc w drodze.

Oprócz przygotowania sprzętu do podróży niemniej istotne jest zapoznanie się z potencjalnymi zagrożeniami, jakie mogą nas spotkać podczas korzystania z sieci w nieznanych nam miejscach.

PUBLICZNE SIECI

Publiczna sieć oferuje usługi dostępu do Internetu każdemu, bez względu na intencje. Takie sieci możemy najczęściej spotkać na lotniskach, w hotelach, restauracjach lub kafejkach w postaci otwartych sieci WiFi. Gdy używamy takiej sieci, nasza aktywność może być monitorowana przez innych. Dodatkowo, użytkownicy o złych zamiarach mogą ustanawiać własne sieci bezprzewodowe i zachęcać innych do ich używania przejmując jednocześnie przesyłane informacje.

Zawsze gdy to możliwe używaj sieci WiFi, do których jest pewność, że są udostępnianie przez znane i zaufane organizacje. Często nazwy takich sieci zawierają fragment nazwy hotelu, restauracji lub innej organizacji, np. operatora telekomunikacyjnego. Są one z reguły bezpieczniejsze niż sieci otwarte - nieznane i często

Wcześniejsze przygotowanie się oraz świadomość zagrożeń to klucz do bezpiecznego korzystania z Internetu w czasie podróży.

wybierane tylko ze względu na darmowy dostęp. W przypadku, gdy to możliwe zawsze wybieraj sieci zapewniające szyfrowanie przesyłanych danych. W kolejności od szyfrowania najsilniejszego wyróżniamy sieci z szyfrowaniem WPA2, WPA oraz WEP.

Niestety, nawet używając sieci z szyfrowaniem, nasze dane mogą zostać podsłuchane przez innych użytkowników tej samej sieci bezprzewodowej. Metodą, która temu zapobiega jest używanie dodatkowych szyfrowanych kanałów komunikacyjnych jak VPN (wirtualnie sieci prywatne) lub bezpiecznych protokołów takich jak HTTPS (SSL/TLS). Protokół HTTPS, używany przez wiele serwisów internetowych takich jak Google, Gmail, Twitter

Bezpieczny Internet w czasie podróży

czy Facebook, zapewnia poufność przesyłanych danych. Przeglądarki internetowe z reguły w specjalny sposób zaznaczają, że jest on używany i nie ma obaw o to, że nasze informacje wpadną w niepowołane ręce lub zostaną zmodyfikowane bez naszej zgody.

Wirtualna sieć prywatna ustanawia dodatkowy kanał komunikacyjny pomiędzy naszym komputerem a serwerem udostępniającym usługę VPN. Całość komunikacji jest szyfrowana podobnie jak w przypadku używania bezpiecznych protokołów SSL/TLS. Skontaktuj się ze swoim działem wsparcia IT i sprawdź czy Twoja organizacja umożliwia zdalny dostęp za pomocą technologii VPN. Istnieje też możliwość zakupu za niewielką opłatą usługi u prywatnych operatorów.

Kolejną z metod jest użycie smartfonu jako bezprzewodowego punktu dostępowego. Skontaktuj się ze swoim operatorem telekomunikacyjnym w celu sprawdzenia, czy istnieje taka możliwość – zwykle wiąże się ona z dodatkowymi opłatami za transfer danych, zwłaszcza poza granicami kraju. Jeżeli smartfon nie posiada funkcji opisanej jako „osobisty punkt dostępowy WiFi" lub podobnej, często umożliwia obsługę skrzynki email oraz przeglądanie zasobów WWW. Jest to dobra alternatywa dla otwartych sieci WiFi, gdyż bezpieczeństwo przesyłanych danych jest zapewniane przez operatora telekomunikacyjnego.

UŻYWANIE PUBLICZNYCH KOMPUTERÓW

Publiczne komputery, podobnie do publicznych sieci, mogą być używane przez każdego. Możemy je znaleźć w bibliotekach, hotelach oraz kafejkach często pozbawionych jakiegokolwiek nadzoru. Nie ma możliwości sprawdzenia kto używał danego komputera wcześniej i do jakich celów. Należy założyć, że może on być zarażony niebezpiecznym oprogramowaniem, a każda informacja jaką przesyłamy będzie przechwycona przez osoby niepowołane. Przy korzystaniu z komputerów w tego typu miejscach należy bezwzględnie wystrzegać się podawania loginów i haseł do jakichkolwiek serwisów. W przypadku, gdy nie mamy wyboru i musimy dokonać operacji, która ujawnia nasze dane, po powrocie lub przy pierwszej nadarzającej się okazji skorzystania z bezpiecznego połączenia powinniśmy je zmienić. Komputery o otwartym dostępie mogą być swobodnie wykorzystywane do takich rzeczy jak sprawdzanie rozkładów lotów, czy wyszukiwanie ciekawych miejsc do zwiedzania w czasie podróży.

DOWIEDZ SIĘ WIĘCEJ

Zasubskrybuj comiesięczny Biuletyn Bezpieczeństwa Komputerowego – SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS z zakresu 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 reagownia 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

Redakcja: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner, Carmen Ruyle Hardy
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak, Paweł Jacewicz, Łukasz Juszczyk, Piotr Kijewski