OUCH! | Październik 2016

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu..

- TY
- Hasła
- Aktualizacje
- Kopie zapasowe

Cztery kroki dla własnego bezpieczeństwa

Wstęp

Technologia odgrywa coraz ważniejszą rolę w naszym życiu stając się jednocześnie coraz bardziej złożoną. Kłopotliwym może być nadążenie za coraz to nowszymi poradami dotyczącymi bezpieczeństwa. Co chwilę pojawiają się nowe poradniki mówiące 'co robić' i czego 'nie robić'. Jednak, podczas gdy zmieniają się szczegóły, istnieją podstawowe zasady, które pomogą Ci chronić siebie. Niezależnie jakiej technologii używasz oraz gdzie jej używasz, zalecamy stosowanie się do poniższych czterech zasad. W sekcji Źródła znajdziesz więcej informacji na temat opisywanych porad.

Redaktor gościnny

Ryan Johnson uczy zaawansowanych dochodzeń sieciowych w Instytucie SANS. W swojej pracy skupia się na przygotowywaniu organizacji na nieuniknione włamania. Możesz znaleźć go na Twitterze **@ForensicRJ**.

1. **Ty**: Po pierwsze i najważniejsze, pamiętaj, że sama technologia nie jest w stanie Cię ochronić. Atakujący nauczyli się, że najłatwiejszym sposobem na ominięcie nawet najbardziej zaawansowanych zabezpieczeń jest zaatakowanie Ciebie. Jeżeli celem są hasła, numery kart lub dane osobowe, najłatwiejszym sposobem jest nakłonienie ofiary do podania tej informacji. Na przykład, atakujący może zadzwonić podając się za pomoc techniczną firmy Microsoft, twierdząc, że Twój komputer został zainfekowany. W rzeczywistości przestępca chce uzyskać dostęp do Twojego komputera. Innym razem możesz otrzymać wiadomość e-mail, która informuje, że paczka nie została dostarczona oraz jesteś proszony o potwierdzenie adresu kliknięciem. Tymczasem zostaniesz przekierowany do stron ze złośliwym oprogramowaniem, które są w stanie włamać się do Twojego komputera. Ataki tego typu używane są przez ransomware lub strony phishingowe. Pamiętaj, najlepszą obroną przed napastnikami jesteś Ty sam. Bądź czujny, używając zdrowego rozsądku jesteś w stanie zapobiec większości ataków.

2. **Hasła**: Następnym krokiem jest używanie silnych oraz unikalnych haseł dla każdego z urządzeń i kont online. Słowami kluczowymi są SILNE oraz UNIKALNE. Silne hasło oznacza takie, które nie może być w prosty sposób odgadnięte przez hackera lub służący temu automat. Czujesz niechęć do tworzenia, zapamiętywania oraz wpisywania złożonych haseł? Spróbuj użyć serii słów łatwych do zapamiętania np: "Gdzie jest moja kawa?". Im dłuższa kombinacja, tym silniejsza. Unikalne hasło

Cztery kroki dla własnego bezpieczeństwa

oznacza używanie różnych haseł na każdym z urządzeń czy koncie online. W ten sposób jeżeli jedno z haseł zostanie złamane, pozostałe z Twoich kont i urządzeń pozostaną bezpieczne. Nie jesteś w stanie zapamiętać tych wszystkich silnych i unikalnych haseł? Spokojnie, my też nie. Dlatego polecamy Ci korzystanie z menadżera haseł, który jest specjalną aplikacją instalowaną na smartfonie lub komputerze, potrafiącą przechowywać wszystkie Twoje hasła w zaszyfrowanej postaci.

Ponadto, jedną z najważniejszych metod ochrony Twoich kont jest włączenie weryfikacji dwuetapowej. Samo hasło może okazać się niewystarczające. Dwuetapowa weryfikacja jest znacznie skuteczniejsza. Wykorzystuje Twoje hasło, lecz ponadto wymaga wprowadzenia dodatkowego elementu (biometria, token). Używaj tej opcji na każdym z kont posiadającym taką możliwość, nawet w menedżerze haseł. Dwuetapowa weryfikacja jest prawdopodobnie jednym z najważniejszych elementów pomagających w ochronie i jest prostsza niż myślisz.

Przestrzegając opisanych czterech zasad, chronisz siebie podczas korzystania z nowoczesnych technologii.

3. **Aktualizacje**: Upewnij się, że komputery, urządzenia mobilne, aplikacje i wszystko co jest podłączone do sieci, używa najnowszej wersji oprogramowania. Hakerzy nieustannie szukają podatności w używanym codziennie oprogramowaniu. Kiedy odkryją tę podatność, wykorzystują specjalnie przygotowane programy w celu włamania się na Twoje urządzenie. Równolegle firmy, które stworzyły podatne oprogramowanie, ciężko pracują tworząc kolejne aktualizacje żeby temu zapobiec. Poprzez zapewnienie swoim urządzeniom najnowszych aktualizacji, zmniejszasz znacząco ich podatność na włamania. Żeby być na bieżąco, wystarczy włączyć automatyczne aktualizacje. Zasada ta dotyczy niemalże wszystkich urządzeń podłączonych do sieci, takich jak telewizory, domowe rutery, konsole do gier, i zapewne już niedługo także samochody. Jeżeli system operacyjny komputera bądź innego urządzenia nie będzie już dłużej wspierany aktualizacjami, zalecamy zaopatrzenie się w nowszą wersję, która jest aktualizowana.

4. **Kopie zapasowe**: Czasami, niezależnie od tego jak bardzo jesteś ostrożny, możesz paść ofiarą hakerów. Jeśli tak się stanie, często jedynym wyjściem dla uzyskania całkowitej pewności pozbycia się wirusów z urządzenia, jest zupełne wyczyszczenie i zainstalowanie wszystkiego od początku. Zdarza się także, że włamywacz może pozbawić Cię dostępu do

Cztery kroki dla własnego bezpieczeństwa

Twoich prywatnych plików, zdjęć lub innych danych zgromadzonych na zaatakowanym urządzeniu. Zazwyczaj pozostaje wtedy tylko przywrócenie danych z kopii zapasowej. Upewnij się, że tworzysz kopie zapasowe ważnych danych oraz, że jesteś w stanie odzyskać je stamtąd. Większość systemów operacyjnych i urządzeń mobilnych umożliwia tworzenie kopii automatycznie. Ponadto, w celu skutecznej ochrony przeciwko hakerom, polecamy przechowywanie kopii zapasowych zarówno w chmurze jak i poza siecią.

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

Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
Menedżer haseł:	https://securingthehuman.sans.org/ouch/2015#october2015
Dwuetapowa weryfikacja:	https://securingthehuman.sans.org/ouch/2015#september2015
Skuteczne hasła:	https://securingthehuman.sans.org/ouch/2015#april2015
Kopie zapasowe:	https://securingthehuman.sans.org/ouch/2015#august2015

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Polski przekład (NASK/CERT Polska): Paweł Jacewicz, Małgorzata Dębska, Przemysław Zielony

