OUCH! | Październik 2014

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W TYM NUMERZE..

5 kroków dla własnego bezpieczeństwa

Wstęp

Technologia zyskuje coraz większą rolę w naszym życiu, a wraz z tym rośnie także jej złożoność. Biorąc pod uwagę jak szybko się zmienia, próbując nadążyć za coraz nowszymi poradami dotyczącymi bezpieczeństwa można się pogubić. Co chwilę pojawiają się nowe wytyczne dotyczące tego, co powinno lub czego nie powinno się robić. Jednak, podczas gdy szczegóły jak pozostać bezpiecznym mogą się zmieniać w czasie, istnieją podstawowe zasady, których należy się zawsze trzymać. Niezależnie od tego, jakiej technologii używasz lub gdzie to robisz, zalecamy stosowanie się do poniższych pięciu podstawowych kroków.

Redaktor gościnny

Lenny Zeltser zajmuje się zabezpieczaniem operacji informatycznych klientów w NCR Corp i uczy w Instytucie SANS jak zwalczać złośliwe oprogramowanie. Lenny jest aktywny na Twitterze, jako **@lennyzeltser** i prowadzi blog o bezpieczeństwie na **blog.zeltser.com**.

5 kluczowych kroków

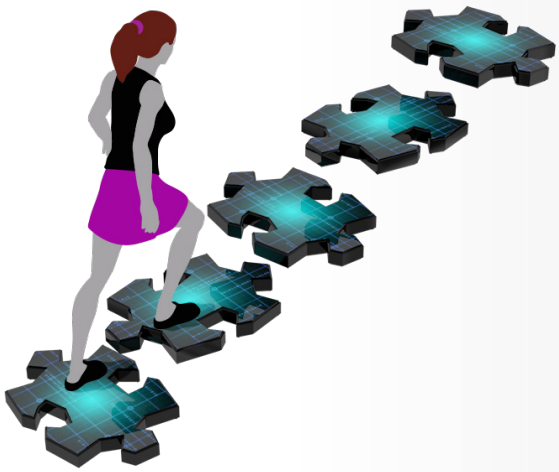
Każdy z pięciu poniższych kroków stanowi zarys danego problemu. Więcej informacji o każdym z nich, zawarte jest w sekcji “Przydatne linki” na końcu biuletynu.

1. **Ty**: Przede wszystkim pamiętaj, że sama technologia nie jest w stanie Cię chronić. Atakujący już dawno się nauczyli, że najprostszym sposobem na ominięcie najbardziej wyrafinowanych technologii zabezpieczeń jest po prostu zaatakowanie Ciebie. Jeśli chcą uzyskać hasło lub numer karty kredytowej, najłatwiejszym dla nich rozwiązaniem jest skłonienie samego użytkownika do dobrowolnego oddania im tej informacji. Ktoś może na przykład zadzwonić udając pomoc techniczną firmy Microsoft, twierdząc, że Twój komputer jest zainfekowany. W rzeczywistości będzie to cyberprzestępca, który chce uzyskać do niego dostęp. Innym razem możesz otrzymać e-mail z zawiadomieniem, że paczka do Ciebie nie mogła być dostarczona i prosić o kliknięcie w link w celu potwierdzenia Twojego adresu, podczas gdy w rzeczywistości link będzie prowadził do złośliwej witryny, przez którą będzie można się włamać do Twojego komputera. Pamietaj, że najlepszą obroną przed napastnikami jesteś Ty. Mając oczy szeroko otwarte i zachowaniu zdrowego rozsądku, można zauważyć i zapobiec większości ataków.

2. **Aktualizacje**: Upewnij się, że komputery, urządzenia mobilne, aplikacje i wszystko inne podłączone do sieci używa najnowszej wersji oprogramowania. Cyberprzestępcy nieustannie szukają luk w technologiach, z których korzystasz. Kiedy odkrywają te słabości, używają specjalnych programów wykorzystujących daną lukę i włamują się na urzadzenie. Działa to w ten sam sposób niezależnie od rodzaju sieci, komputera czy urządzenia mobilnego jakich używasz. Tymczasem firmy, które stworzyły te technologie ciężko pracują, aby były one aktualne i bezpieczne. Kiedy

5 kroków dla własnego bezpieczeństwa

tylko luka staje się im znana, tworzą łatkę, w celu naprawy problemu i publikują ją, aby mogła być szybko zastosowana przez każdego. Poprzez zapewnienie swoim urządzeniom najnowszych aktualizacji, możesz zmniejszyć liczbę znanych luk w zainstalowanym oprogramowaniu, co znacznie utrudni włamanie. Aby mieć na bieżąco instalowane wszystkie łatki, w miarę możliwości włącz automatyczne aktualizacje. Zasada ta ma zastosowanie do niemal wszystkich urządzeń podłączonych do sieci, włączając w to inteligentne telewizory, elektroniczne nianie, routery, konsole do gier i zapewne już niedługo także samochody. Jeśli system operacyjny Twojego komputera, smartfonu lub jakiegokolwiek innego urządzenia, nie jest już wspierany przez producenta oznacza to, że nie będzie już otrzymywał żadnych aktualizacji. W takim przypadku zalecamy zaopatrzenie się w nową wersję, która jest aktualizowana.



Przestrzegając tych pięciu kluczowych porad, zrobisz duży krok w stronę ochrony siebie jednocześnie bezproblemowo korzystając z najnowszych technologii.

3. **Hasła**: Następnym krokiem do zabezpieczenia istotnych dla nas danych jest używanie silnego, unikatowego hasła dla każdego z urządzeń, kont internetowych i aplikacji. Słowami kluczowymi są tu silne i unikatowe. Silne hasło oznacza takie, które nie może być łatwo odgadnięte ani przez człowieka ani przez służące do tego zautomatyzowane narzędzia. Zamiast jednego słowa, używaj ciągu znaków złożonego z wielu słów przeplatanych symbolami i cyframi w odpowiedniej liczbie. Używanie unikatowych haseł oznacza, że posiada się inne hasło dla każdego urządzenia i konta online. W ten sposób jeśli któreś z nich jest zagrożone, inne konta i urządzenia są nadal bezpieczne. Myslisz, że nie jesteś w stanie zapamiętać tych wszystkich skomplikowanych haseł? Nie martw się, my też nie. Dlatego zalecamy korzystanie z menedżera haseł, który jest specjalistyczną aplikacją w smartfonie lub komputerze, w której można bezpiecznie przechowywać wszystkie hasła w postaci zaszyfrowanej. Ponadto, jeśli któreś z Twoich kont obsługuje weryfikację dwuetapową, zawsze zalecamy ją włączyć, gdyż jest to jeden z najlepszych sposobów ochrony konta.

4. **Szyfrowanie**: Naszym kolejnym zaleceniem jest stosowanie szyfrowania. Jego użycie zapewnia, że tylko Ty lub osoby którym ufasz mogą uzyskać dostęp do Twoich informacji. Dane mogą być szyfrowane na dwa sposoby: statycznie oraz w czasie przesyłania. Statyczne szyfrowanie danych oznacza ich ochronę podczas przechowywania w postaci plików zapisanych na dysku twardym lub pamięci USB. Większość systemów operacyjnych pozwala na automatyczne szyfrowanie wszystkich danych przy użyciu takich opcji jak całkowite zaszyfrowanie dysku (Full Disk Encryption). Zalecamy włączyć tę opcję. Szyfrowanie danych w czasie przesyłania oznacza szyfrowanie danych podczas komunikacji komputera lub innego urządzenia z Internetem, na przykład kiedy korzysta się z bankowości elektronicznej. Prostym sposobem, aby sprawdzić, czy szyfrowanie jest włączone podczas przeglądania strony, to upewnienie się, że jej adres zaczyna się od „https://" a obok znajduje się ikona zamkniętej kłódki.

5 kroków dla własnego bezpieczeństwa

5. **Kopie zapasowe**: Czasami, niezależnie od podjętych środków ostrożności, Twoje urządzenie może zostać zainfekowane. Jeśli tak sie stało, wówczas czesto jedynym wyjściem, aby Twój komputer lub urządzenie mobilne było wolne od złośliwego oprogramowania jest jego zupełne wyczyszczenie i zainstalowanie wszystkiego od początku. Niekiedy atakujący jest w stanie nawet uniemożliwić Ci dostęp do osobistych plików, zdjęć i innych informacji przechowywanych na zainfekowanym systemie. Jedynym rozwiązaniem może być przywrócenie wszystkich osobistych danych z kopii zapasowej. Upewnij się, że regularne tworzysz kopie zapasowe wszytskich ważnych informacji i sprawdź, czy możesz z nich przywrócić swoje dane. Większość systemów operacyjnych i urządzeń przenośnych obsługuje automatyczne tworzenie kopii zapasowych.

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

Źródła

Email i ataki phishingowe:	http://www.securingthehuman.org/ouch/2013#february2013
Zabezpiecz swój nowy tablet:	http://www.securingthehuman.org/ouch/2013#december2013
Silne hasła:	http://www.securingthehuman.org/ouch/2013#may2013
Systemy zarządzania hasłami:	http://www.securingthehuman.org/ouch/2013#october2013
Dwustopniowe uwierzytelnianie:	http://www.securingthehuman.org/ouch/2013#august2013
Szyfrowanie:	http://www.securingthehuman.org/ouch/2014#august2014
Backup i przywracanie danych:	http://www.securingthehuman.org/ouch/2013#september2013

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

