OUCH! | Maj 2015

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W TYM WYDANIU..

- Wstęp
- Podstawy
- Dzieci w odwiedzinach

Pokoleniowa cyber-luka

Wstęp

Wielu z nas czuje się swobodnie korzystając z technologii, równocześnie robiąc to w sposób bezpieczny. Jednak są osoby, które mogą nie czuć się tak swobodnie, zwłaszcza jeśli nie wychowywały się z komputerami i dostępem do Internetu. Poniżej znajdziesz kilka kroków, które można podjąć, aby pomóc zmniejszyć lukę pokoleniową w korzystaniu z technologii. Można również podjąć pewne kroki w celu zabezpieczenia swoich dzieci w domu, ale te same środki bezpieczeństwa z dużym prawdopodobieństwem nie będą istnieć, gdy dzieci odwiedzą np. dom krewnego. Dlatego przyjrzymy się również temu jak można stworzyć bardziej bezpieczne środowisko internetowe, gdy dzieci są poza naszym domem.

Redaktor gościnny

Brian Honan (Twitter **@GuyBruneau**) jest niezależnym konsultantem bezpieczeństwa w Dublinie w Irlandii, założycielem i szefem pierwszego irlandzkiego zespołu CERT, Specjalnym Doradcą Centrum Cyberprzestępczości Europolu (EC3) oraz wykładowcą zagadnień bezpieczeństwa informacji na University College w Dublinie. Jest autorem wielu książek i pisze dla różnych wydawnictw branżowych.

Podstawy

Wystarczy kilka podstawowych kroków, aby znacznie poprawić czyjeś bezpieczeństwo w Internecie. Oto podstawowe kroki, których wykonanie zalecamy każdemu członkowi rodziny. Jednak jeśli wiesz, że ktoś z nich nie rozumie tych kroków, być może trzeba będzie wyjaśnić mu je dokładniej lub wdrożyć samodzielnie.

- **Inżynieria społeczna**: Wyjaśnij pojęcie inżynierii społecznej na prostych przykładach, do których każdy może się odnieść. Oszustwa i oszuści istnieją od tysięcy lat i ataki tego typu to nic nowego. Jedyną różnicą jest to, że teraz stosuje się do tego Internet. Przedstaw przykłady najczęstszych oszustw, jakie można dzisiaj napotkać, takich jak popularne wiadomości phishingowe lub kampanie oszustów dzwoniących udając wsparcie techniczne firmy Microsoft. Upewnij się, że członkowie rodziny rozumieją, że nigdy nie powinni podawać nikomu swojego hasła lub umożliwiać zdalny dostęp do swojego komputera. Niech wiedzą, że jeśli czują się nieswojo lub mają zastrzeżenia do wiadomości e-mail lub kogoś dzwoniącego, najpierw powinni zadzwonić do Ciebie zanim zdecydują się podać jakiekolwiek informacje.
- **Domowa sieć Wi-Fi**: Poświęć trochę czasu, aby upewnić się, że sieć Wi-Fi w ich domu jest zabezpieczona. Jako minimum, sprawdź czy domyślne hasło administratora zostało zmienione, czy silne hasło chroni dostępu do domowej sieci Wi-Fi i czy połączenie sieciowe korzysta z najnowszych metod szyfrowania. Możesz też rozważyć skonfigurowanie sieci Wi-Fi tak, aby używać bezpiecznego DNS takiego jak www.opendns.org. Bezpieczne usługi DNS nie tylko pomagają powstrzymać użytkowników przed odwiedzeniem zainfekowanych stron internetowych, ale

Pokoleniowa cyber-luka

także dadzą Ci kontrolę nad wyborem, które strony internetowe będzie można lub nie będzie można odwiedzić, co może być przydatne kiedy z internetu korzystają dzieci.

- **Łatki**: Utrzymywanie zaktualizowanych systemów jest jednym z najbardziej podstawowych kroków, jakie można podjąć w celu zabezpieczenia wszelkich technologii. Upewnij się czy wszystkie urządzenia domowe (w tym urządzenia mobilne) oraz aplikacje są w załatane. Najprostszym sposobem zapewnienia tego jest włączenie automatycznych aktualizacji.
- **Antywirus**: Ludzie popełniają błędy. Czasami zdarza się kliknąć lub zainstalować rzeczy, których się nie powinno. Antywirus nie zatrzyma działania każdego złośliwego oprogramowania, ale pomaga wykryć i zatrzymać popularne ataki. Upewnij się, że wszystkie domowe komputery mają zainstalowany program antywirusowy i że jest on aktualny i aktywny. Więcej o antywirusach możesz przeczytać w wydaniu OUCH! z grudnia 2014 roku.

Starsze pokolenia mogą potrzebować pomocy w zabezpieczeniu ich domowych komputerów i stworzeniu bezpiecznego środowiska w czasie wizyt dzieci.

- **Hasła**: Silne hasła są kluczem do ochrony urządzeń i wszelkich kont internetowych. Przeprowadź członków rodziny przez proces jak tworzyć silne hasła. Wyrażenia hasłowe (patrz OUCH! kwiecień 2015) mogą być dla nich najprostsze do użytku i łatwe do zapamiętania. Innym pomysłem jest zainstalowanie menedżera haseł i nauczenie ich, jak go używać. Jeśli to nie zadziała, ostatecznie można nauczyć ich zapisać hasła, a następnie przechowywać je w bezpiecznym miejscu, do którego tylko oni mają dostęp. Dla najważniejszych kont internetowych dobrym pomysłem jest skonfigurowanie dwustopniowego uwierzytelniania (patrz OUCH! sierpień 2013).
- **Kopie zapasowe**: Kiedy wszystko inne zawiedzie, tylko kopie zapasowe mogą Cię uratować. Upewnij się, że członkowie rodziny mają prosty i niezawodny system do tworzenia kopii zapasowych swoich plików. Więcej o tworzeniu kopii zapasowych znajdziesz w wydaniu OUCH! z września 2013 roku.

Dobrze jest sprawdzać powyższe punkty miesięcznie lub kwartalnie, aby upewnić się, że wszystko jest pod kontrolą. Jako rozwiązanie ostatecznie można rozważyć zainstalowanie oprogramowania do zdalnego administrowania urządzeniem. Jednak upewnij się, że jest ono zabezpieczone zarówno szyfrowaniem transmisji oraz silnym, unikalnym hasłem.

Dzieci w odwiedzinach

Bardzo często, gdy małe dzieci odwiedzają domy krewnych, zasady które stosujesz w swoim domu, mogą nie mieć zastosowania. Wśród nich mogą być te, zaprojektowane, aby pomóc chronić dzieci w Internecie. Oto kilka kroków, które można podjąć w celu ochrony dzieci.

Pokoleniowa cyber-luka

- **Zasady**: Upewnij się, że jeśli ustanowiłeś jakieś zasady w celu zapewnienia bezpieczeństwa swoich dzieci, krewni o nich wiedzą. Na przykład, czy są jakieś zasady jak długo dzieci mogą grać online lub kiedy mogą mieć dostęp do swoich urządzeń mobilnych? Nie zostawiaj dzieciom wyjaśnienia zasad dziadkom lub innym członkom rodziny. Dobrym pomysłem jest stworzenie „karty zasad" i podzielenie się nią ze wszystkimi krewnymi, których Twoje dziecko odwiedza.
- **Kontrola**: Jeśli Twoje dzieci rozumieją technologię lepiej niż ich opiekunowie, mogą to wykorzystać. Na przykład, dzieci mogą poprosić lub uzyskać prawa administracyjne do komputera u dziadków i robić na nim co chcą, np. instalować grę, w którą nie chcesz żeby grały. Upewnij się, że krewni rozumieją, że nie należy dawać dzieciom dodatkowego dostępu poza tym, co zostało ustalone.

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

Socjotechnika:	http://www.securingthehuman.org/ouch/2014#november2014
Zabezpieczenie sieci domowej:	http://www.securingthehuman.org/ouch/2014#january2014
Szyfrowane frazy:	http://www.securingthehuman.org/ouch/2015#april2015
Antywirusy:	http://www.securingthehuman.org/ouch/2014#december2014
Ochrona dzieci on-line:	http://www.securingthehuman.org/ouch/2013#april2013
Plakat bezpieczeństwo w domu:	http://www.securingthehuman.org/resources/posters

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