OUCH! | Październik 2017

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu..

- Wstęp
- Pięć kluczowych kroków
- Bezpieczeństwo dzieci poza domem

# O tym, jak pomóc innym być bezpiecznym

## Wstęp

Być może część z czytelników swobodnie korzysta z nowych technologii, stosując przy tym dobre praktyki bezpieczeństwa, jednak prawdopodobnie nie dotyczy to wszystkich ich znajomych oraz rodziny. Natłok nowych informacji i nowinek technologicznych może wzbudzać u niektórych lęk oraz powodować nieporadność w styczności z nimi, co sprawia, że stają się podatni na ataki przestępców. Bezpieczeństwo informatyczne nie musi być dla nich czarną magią, a w rzeczywistości będzie proste po zrozumieniu jego podstawowych założeń. Zazwyczaj potrzebny jest zwyczajnie dobry przewodnik, który pomoże przyswoić sobie podstawowe zasady.

**Redaktor gościnny**

Randy Marchany (Twitter: **@randymarchany**) pełni rolę dyrektora informatyki oraz bezpieczeństwa w Virginia Tech, a także certyfikowanego instruktora Instytutu SANS.

## Pięć prostych kroków

Prezentujemy pięć kroków, które mogą pomóc innym bezpiecznie korzystać z dobrodziejstw technologii. W źródłach poniższego biuletynu znajdują się linki do szczegółowego opracowania każdego z poniższych punktów.

1. **Inżynieria Społeczna**: Inżynieria społeczna jest powszechną techniką używaną przez przestępców do wprowadzania w błąd i nakłaniania do wykonania przez ofiarę konkretnej czynności, jak na przykład udostępnienia hasła, zainfekowania swojego urządzenia lub podania wrażliwych informacji. Nie jest to nic nowego, fałszywe wiadomości o rzekomej wygranej na loterii oraz oszuści istnieją od dawna, a obecni przestępcy wykorzystują podobne schematy w internecie. Chcąc pomóc innym zrozumieć zagrożenie związane z inżynierią społeczną, możesz przedstawić najczęstsze schematy postępowania oszustów, jak np. stwarzanie potrzeby szybkiej reakcji, przedstawiania sytuacji w sposób zbyt piękny by była prawdziwa lub gdy atakujący podszywa się pod znajomą osobę, lecz wiadomości od niej brzmią podejrzanie. Pomocne na pewno będzie pokazanie przykładów wiadomości phishingowych lub wyskakujących okien o potrzebie zainstalowania dodatkowego rozszerzenia w przeglądarce. Przede wszystkim do znudzenia powtarzaj, by nie udostępniać haseł oraz nie pozwalać na zdalny dostęp do komputera.
2. **Hasła**: Silne, a jednocześnie unikatowe hasło stanowi kluczowy punkt w zakresie bezpieczeństwa, zarówno urządzeń jak i kont internetowych. Przedstaw rodzinie sposoby na tworzenie bezpiecznych haseł, na przykład z wykorzystaniem łatwych do zapamiętania oraz wprowadzania fragmentów zdań lub połączonych słów (ang. passphrases). Pokaż jakie korzyści przynosi również korzystanie z menadżera haseł. Dzięki niemu łatwiej przestrzegać ważnej zasady unikania wielokrotnego użycia tego samego hasła dla różnych kont i urządzeń. Jeśli użycie menadżera będzie jednak zbyt trudne dla tej osoby, można zasugerować zapisanie haseł, a następnie zachowanie ich w bezpiecznym

## O tym, jak pomóc innym być bezpiecznym

miejscu. Pokaż jak ustawić weryfikację dwuetapową dla najważniejszych kont, co znacznie zwiększy bezpieczeństwo podczas logowania.

3. **Aktualizacje**: Sprawdzanie czy system oraz aplikacje są aktualne należy również do kluczowych procedur zachowania bezpieczeństwa. Nie chodzi jedynie o aktualizacje komputera czy urządzeń mobilnych, ale wszystkiego co jest podłączone do internetu, jak na przykład konsoli do gier, kamer czy telewizorów. Najlepszym rozwiązaniem, jeśli jest taka możliwość jest włączenie opcji automatycznych aktualizacji.
4. **Oprogramowanie antywirusowe**: Ludzie nie są nieomylni, każdemu może zdarzyć się błąd i nacisnąć przez przypadek lub zainstalować coś co mogło doprowadzić do infekcji systemu operacyjnego. Oprogramowanie antywirusowe zostało stworzone do tego by chronić nas w przypadku popełnienia takich błędów. Oprogramowanie to nie jest w stanie zatrzymać każdego złośliwego oprogramowania, ale pomaga wykryć zagrożenie oraz zatrzymać bardziej typowe ataki. Sprawdź czy komputer posiada uruchomione oprogramowanie antywirusowe z aktualną bazą sygnatur złośliwego oprogramowania. Warto również zastanowić się nad zastosowaniem dodatkowych rozwiązań, takich jak firewall oraz ochrona przeglądarki internetowej, których funkcjonalności często są już wbudowane w oprogramowanie antywirusowe.
5. **Kopie zapasowe**: Kiedy wszystkie metody ochrony zawiodą i zarazimy się np. ransomwarem lub przypadkiem zdarzy się nam usunięcie plików, kopia zapasowa jest często jedynym rozwiązaniem by przywrócić stan sprzed takiego incydentu. Sprawdź czy rodzina oraz znajomi posiadają działającą funkcję automatycznego tworzenia kopii systemu. Zazwyczaj najprościej jest korzystać z rozwiązań opartych o chmurę, tworzących kopię co godzinę lub po modyfikacji pliku. Takie kopie zapasowe są również łatwe do wykorzystania podczas procedury przywracania wersji plików.

*Pomóż innym się zabezpieczyć i przekaż informacje o pięciu krokach mogących poprawić ich bezpieczeństwo w sieci.*

## Bezpieczeństwo dzieci poza domem

Jeśli czujesz się swobodnie korzystając z technologii, prawdopodobnie nie tylko ty stosujesz się do zasad jej bezpiecznego używania, ale również starasz się chronić swoje dzieci przed zagrożeniami w sieci. Czasem jednak gdy dzieci odwiedzają inne osoby, które niekoniecznie są biegłe w kontakcie z nowinkami technologicznymi, jak na przykład osoby starsze, może dojść do sytuacji, w której bezpieczeństwo dzieci w sieci nie będzie wystarczająco zachowane. Poniżej prezentujemy kroki, które należy wdrożyć by chronić dzieci poza domem.

- **Reguły**: Upewnij się, że osoby, pod których opieką zostawiasz dzieci są zaznajomione ze stosowanymi przez ciebie zasadami względem bezpieczeństwa w sieci. Na przykład, określ jak długo dziecko może korzystać z internetu, z kim może rozmawiać lub w jakie gry może grać. Zaufaj nam, lepiej nie pozwalać dziecku na samodzielne przekazanie

## O tym, jak pomóc innym być bezpiecznym

opiekunom tych zasad. Dobrym pomysłem jest stworzenie spisanego zbioru reguł, który możesz udostępnić często odwiedzanym znajomym.

- **Kontrola**: Jeśli okaże się, że dziecko ma lepsze obycie z technologią niż osoba ją nadzorująca, na pewno nie umknie to uwadze dziecka i to wykorzysta. Na przykład dziecko może poprosić dziadków o dostęp do konta administracyjnego komputera by móc zainstalować grę, w którą nie pozwalasz mu grać. Upewnij się, że opiekunowie rozumieją zasadę ograniczenia dostępu, która została wcześniej ustalona oraz będą ją stosować.

Oczywiście warto polecić znajomym i rodzinie subskrybowanie takich biuletynów jak OUCH! by mogli uczyć się również we własnym zakresie. Biuletyn jest udostępniany darmowo co miesiąc w ponad 20 językach. Zapisz się pod adresem: https://securingthehuman.sans.org/ouch.

## 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

| | |
|---|---|
| Inżynieria społeczna: | https://securingthehuman.sans.org/ouch/2017#january2017 |
| Silne hasła: | https://securingthehuman.sans.org/ouch/2017#april2017 |
| Menadżery haseł: | https://securingthehuman.sans.org/ouch/2017#september2017 |
| Weryfikacja dwuetapowa: | https://securingthehuman.sans.org/ouch/2015#september2015 |
| Kopie zapasowe: | https://securingthehuman.sans.org/ouch/2017#august2017 |
| Bezpieczeństwo dzieci w sieci: | https://securingthehuman.sans.org/ouch/2017#may2017 |



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