Biuletyn Bezpieczeństwa Komputerowego

Cztery proste kroki dla własnego bezpieczeństwa

Wstęp

Bezpieczne korzystanie z technologii może wydawać się przytłaczające i zagmatwane. Jednak niezależnie od używanej technologii i sposobu jej użycia, przedstawiamy cztery proste kroki, które pomogą Ci zachować bezpieczeństwo.

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 jest w stanie włamać się do Twojego komputera. Pamiętaj, najlepszą obroną przed napastnikami jesteś Ty sam. Bądź czujny, używając zdrowego rozsądku jesteś w stanie zapobiec większości ataków.

2. Hasła: Obecne możliwości obliczeniowe komputerów sprawiły, że hasło zbudowane z 8 znaków jest łatwe do złamania, a tym samym bardziej podatne na zagrożenie. Kiedy witryna prosi o utworzenie hasła, powinieneś używać mocnych oraz unikalnych haseł dla każdego z urządzeń i kont online. Słowami kluczowymi są MOCNE oraz UNIKALNE. Mocne 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: “Kot Malwiny lubi jeździć koleją”. Im dłuższa kombinacja, tym silniejsza. Unikalne hasło oznacza używanie różnych haseł na każdym z urządzeń czy koncie online. W ten sposób jeżeli jedno z haseł zostanie złamane, reszta Twoich kont i urządzeń pozostanie bezpieczna. Nie jesteś w stanie zapamiętać tych wszystkich silnych i unikalnych haseł? Spokojnie, my też nie. Dlatego polecamy Ci korzystanie z menedżera haseł, który jest aplikacją zainstalowaną na smartfonie lub komputerze, potrafiącą przechowywać wszystkie Twoje hasła w zaszyfrowanej postaci.

Ponadto, jedną z najważniejszych metod ochrony Twoich kont jest włączenie dwuskładnikowego uwierzytelniania. Samo hasło może okazać się niewystarczające. Dwuskładnikowe uwierzytelnienie jest znacznie skuteczniejsze.

Wykorzystuje Twoje hasło, lecz ponadto wymaga wprowadzenia dodatkowego składnika (biometria, pin, token). Dwuetapowa weryfikacja jest prawdopodobnie jednym z najważniejszych elementów pomagających w ochronie i jest prostsza niż myślisz.

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 tą 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 bez mała wszystkich urządzeń podłączonych do sieci, takich jak telewizory, bezprzewodowe nianie elektroniczne, kamery, domowe routery, konsole do gier a nawet samochody.

4. Kopie zapasowe: Czasami, niezależnie od podjętych środków ostrożności, Twoje urządzenie może zostać zainfekowane. Jeśli tak się stało, wówczas często jedynym wyjściem, aby przywrócić wszystkie dane osobowe jest wykonanie kopii zapasowej. Upewnij się, że regularnie tworzysz kopie zapasowe wszystkich ważnych informacji i sprawdź, czy możesz z nich przywrócić swoje dane. Większość systemów operacyjnych i urządzeń przenośnych obsługuje automatyczne tworzenie kopii zapasowych.

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

Redaktor wydania

Steve Anson *jest certyfikowanym instruktorem Instytutu SANS. Udziela wskazówek zespołom ds. bezpieczeństwa IT i rządom na całym świecie w celu poprawy ich bezpieczeństwa. Steve jest też autorem książki 'Applied Incident Response' i udostępnia darmowe materiały edukacyjne na stronie internetowej* appliedincidentresponse.com.

Źródła

Socjotechnika:	https://www.sans.org/u/W3G
Spersonalizowane oszustwa:	https://www.sans.org/u/W3Q
Tworzenie haseł w prostszy sposób:	https://www.sans.org/u/W3V
Czy robisz kopie zapasowe?:	https://www.sans.org/u/W40