SANS SECURITY AWARENESS

OUCH!

Biuletyn Bezpieczeństwa Komputerowego

Tak, jesteś celem ataków

Wstęp

Wielu ludzi błędnie uważa, że nie są celem działań cyberprzestępców: że ich systemy lub konta nie mają dla nikogo żadnej wartości. Nic bardziej mylnego. Jeśli używasz technologii jakkolwiek, w pracy lub w domu, zaufaj nam – stanowisz wartość dla ludzi o złych zamiarach. Ale na szczęście Ty możesz być swoją najlepszą ochroną przed cyberatakami.

Dlaczego cyberprzestępcy interesują się Tobą?

W internecie obecnych jest wielu cyberprzestępców, którymi kierują różne motywacje. Dlaczego więc któryś z nich miałby Cię zaatakować? Odpowiedź jest jedna, atakując Cię przybliżają się do osiągnięcia swojego celu. Oto dwa typowe przykłady cyberprzestępców oraz powody jakimi się kierują.

⚠ **Cyberprzestępcy:** nastawieni na zarobienie jak największej ilości pieniędzy. Internet jest dla nich bardzo wartościowy, gdyż mogą zaatakować każdego za pomocą naciśnięcia jednego przycisku. Jest wiele sposobów, dzięki którym mogą pozyskać Twoje pieniądze. Przykładem może być kradzież pieniędzy z konta bankowego, nieuprawnione użycie karty płatniczej, wykorzystanie Twojego komputera w celu włamania się do innych osób, przejęcie konta w mediach społecznościowych lub serwisach dla graczy oraz odsprzedanie ich innym przestępcom. Lista sposobów w jaki przestępcy mogą dokonać kradzieży Twoich pieniędzy jest niemal nieograniczona. Tysiące atakujących każdego ranka budzi się z decyzją oszukania jak największej liczby osób, łącznie z Tobą.

☆ **Ukierunkowani atakujący:** to świetnie wyszkoleni cyberprzestępcy, często pracujący dla rządów, zorganizowanych grup przestępczych lub konkurencji. Może czujesz, że Twoja praca nie przyciąga zbyt wielkiej uwagi, mógłbyś się jednak bardzo zdziwić.

- Informacje, którymi zarządzasz w pracy mają ogromną wartość dla różnych firm czy rządów.
- Przestępcy mogą atakować Cię w pracy nie dlatego, że chcą ukraść Twoje pieniądze, ale dlatego, aby za pomocą Twojego komputera zaatakować jednego ze współpracowników lub inne systemy.
- Tego typu napastnicy mogą wziąć Cię na celownik w pracy z powodu innych firm, z którymi współpracujesz.

Nic mi nie grozi, bo mam program antywirusowy

Pewnie uważasz, że jesteś celem cyberprzestępców ale zainstalujesz program antywirusowy wraz z zaporą sieciową i będziesz chroniony, prawda? Cóż, niestety nie. Wiele osób uważa, że jeśli zainstalują jakikolwiek program antywirusowy to będą bezpieczni. Niestety, nie do końca jest to prawdą. Cyberprzestępcy korzystają z coraz to nowych metod ataków i wiele z nich potrafi omijać zabezpieczenia. Na przykład, często tworzą złośliwie oprogramowanie, którego program antywirusowy nie wykrywa jako zagrożenie. Pomijają Twoje filtry poczty e-mail przy pomocy ukierunkowanych ataków phishingowych lub ataków typu vishing podczas rozmowy telefonicznej, wykradają Twoje pieniądze, hasła lub dane karty płatniczej. Technologia odgrywa ważną rolę w ochronie Ciebie, ale ostatecznie Ty jesteś najlepszą ochroną dla samego siebie.

Na szczęście bycie bezpiecznym nie jest aż tak trudne. Zdrowy rozsądek i trzymanie się podstawowych zasad bezpieczeństwa stanowią najlepszą formę obrony. Kiedy otrzymujesz wiadomość e-mail, sms albo połączenie telefoniczne, które wydaje się dziwne lub podejrzane, miej świadomość, że może to być forma ataku. Podnieś swoje bezpieczeństwo włączając automatyczne instalowanie aktualizacji. Używaj silnego, unikalnego hasła dla każdego z posiadanych kont. Dbaj o budowanie świadomości w zakresie bezpiecznego korzystania z cyberprzestrzeni. Nie wiesz, od czego zacząć? Rozważ subskrybowanie comiesięcznego biuletynu o bezpieczeństwie komputerowym SANS OUCH! na https://www.sans.org/ouch

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 Gościnny

Matt Bromiley *(@mbromileyDFIR) jest specjalistą ds. reagowania na incydenty oraz ekspertem w dziedzinie informatyki śledczej z ponad 8 letnim doświadczeniem. Współpracuje z wieloma organizacjami i analizuje incydenty z różnych stron świata. Matt jest również instruktorem w zakresie informatyki śledczej i reagowania na incydenty. Prowadzi kursy SANS FOR508 i FOR572.*

SANS SECURITY AWARENESS

Przydatne linki

Powstrzymaj złośliwe oprogramowanie:	https://www.sans.org/u/L1J
Socjotechnika:	https://www.sans.org/u/L1O
Ataki telefoniczne:	https://www.sans.org/u/L1T
Bezpieczne hasła:	https://www.sans.org/u/L1Y
Plakat – You Are a Target (“jesteś celem”):	https://www.sans.org/u/L23

Biuletyn OUCH! powstaje w ramach programu „Security Awareness” Instytutu SANS i jest wydawany na licencji Creative Commons BY-NC-ND 4.0 license. Powielanie treści biuletynu jest dozwolne jedynie w celach niekomercyjnych oraz pod warunkiem zachowania informacji o źródle pochodzenia kopiowanych treści oraz nienaruszania zawartości samego biuletynu. Informacje kontaktowe: www.sans.org/security-awareness/ouch-newsletter. Editorial Board: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Polski przekład (NASK/CERT Polska): Sebastian Kondraszuk, Michał Strzelczyk, Jacek Sikorski