Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu

- **Bezpieczeństwo na start**
- **Bezpieczeństwo na stałe**
- **Bezpieczeństwo na przyszłość**

Bezpieczny komputer w siedmiu krokach

REDAKTOR GOŚCINNY

Redaktorem gościnnym tego wydania biuletynu OUCH! jest Guy Bruneau. Guy jest certyfikowanym instruktorem Instytutu SANS oraz zajmuje się obsługą incydentów w SANS Incident Storm Center. Posiada certyfikat GIAC Security Expert oraz ukończony program szkoleniowy SANS Cyber Guardian. Więcej o jego zainteresowaniach można znaleźć na kanale Twittera @guybruneau.

WSTĘP

Urządzenia przenośne, takie jak smartfony i tablety, zaczynają dominować na rynku nowych technologii, jednakże to komputery osobiste są ciągle podstawowym narzędziem, którego używamy zarówno w domu jak i w pracy. W rezultacie to one pozostają podstawowym celem cyberataków. Siedem kroków opisanych w dalszej części artykułu pozwoli zabezpieczyć stację roboczą i uchronić ją przed efektem działania najpopularniejszych z obecnie występujących w Internecie zagrożeń.

1. BEZPIECZNY START

Komputer osobisty, aby był bezpieczny musi pochodzić z zaufanego źródła. W przypadku gdy kupujesz nowy komputer do domu ze znanego i cieszącego się dobrymi opiniami sklepu, wtedy możesz mieć pewność, że nie zawiera on żadnego złośliwego oprogramowania. Podobnie, gdy otrzymujesz nową stację roboczą w pracy. Przygotowaniem takich maszyn zajmuje się zespół profesjonalistów, którzy posiadają odpowiednią wiedzę i umiejętności, aby komputer, nawet jeżeli wcześniej był używany przez innego pracownika, nie zawierał żadnego niebezpiecznego oprogramowania.

W przypadku gdy kupujesz używany komputer, nie powinieneś ufać żadnej zainstalowanej na nim aplikacji. Zdarza się, że na dysku takiego komputera można znaleźć całą masę wirusów, które wkradły się tam nawet bez wiedzy poprzedniego właściciela. Takiej maszyny nie da się zabezpieczyć i pierwszym krokiem jaki powinieneś zrobić to całkowite usunięcie starych danych z dysku i instalacja świeżej kopii systemu operacyjnego. Jeżeli nie potrafisz tego zrobić sam, poproś znajomego, który może Ci w tym pomóc. Wykonanie tego kroku to podstawa do dalszych działań.

2. AKTUALIZACJE

Kolejnym są aktualizacje. Cyberprzestępcy nieustannie wyszukują nowe błędy i podatności w systemach operacyjnych i aplikacjach. Gdy takie błędy wychodzą na jaw, twórcy oprogramowania udostępniają aktualizacje swoich produktów, które maja na celu go naprawić oraz załatać lukę. W przypadku, gdy kupujesz komputer lub reinstalujesz system operacyjny, z całą pewnością jest on już nieaktualny. Teraz powinieneś podłączyć go do Internetu i zainstalować wszystkie dostępne poprawki. Ale pamiętaj, że komputer który nie ma jeszcze zainstalowanych poprawek jest podatny na ataki

Bezpieczny komputer w siedmiu krokach

z Internetu, dlatego podłączaj go zawsze do zaufanej sieci chronionej przez firewall lub do domowej sieci WiFi. Obecnie wiele systemów operacyjnych oraz aplikacji posiada opcję automatycznej instalacji aktualizacji w momencie, gdy stają się one dostępne. Jeżeli opcja ta nie jest jeszcze włączona, zrób to koniecznie i jeśli jest taka możliwość ustaw codziennie sprawdzanie dostępności nowych aktualizacji. Taka konfiguracja zapewni, że będziesz mógł bez obaw używać komputera w codziennej pracy. W przypadku, gdy używasz aplikacji, które nie mają opcji automatycznej aktualizacji, sprawdzaj dostępność nowych wersji ręcznie i instaluj poprawki tak szybko jak to możliwe.

3. OPROGRAMOWANIE

Po pełnej aktualizacji systemu i aplikacji przychodzi czas na zainstalowanie dodatkowego oprogramowania, które podniesie poziom bezpieczeństwa w systemie operacyjnym. Najpopularniejsze to antywirusy i tzw. ściany ogniowe (z ang. firewall). Antywirus ma za zadanie wykryć i zablokować złośliwe pliki (zarówno aplikacje jak i dokumenty) przed wykonaniem nieuprawnionych działań. Firewall działa jak “wirtualny ochroniarz” - decyduje kto może, a kto nie połączyć się z Twoim komputerem. Wielu z dostawców oprogramowania oferuje zintegrowane rozwiązania, które zawierają jednocześnie antywirusa, firewall, a także inne przydatne narzędzia - wszystko w jednej paczce. Często taki zestaw jest tańszy niż gdyby kupić każde z tych rozwiązań oddzielnie.

4. KONTA UŻYTKOWNIKÓW.

Każda z osób, która korzysta z Twojego komputera powinna mieć swoje własne, prywatne konto w systemie, chronione przez unikalne i silne hasło. Nigdy nie dziel się swoim kontem z innym użytkownikiem! W przypadku komputera domowego, stwórz oddzielne konto dla każdego z domowników, zwłaszcza dla dzieci. Dzięki temu możesz zaaplikować różne poziomy nadzoru dla każdego z kont, np. konta dla małych dzieci powinny mieć włączoną ochronę rodzicielską oraz śledzenie działań (zwłaszcza w

Wystarczy tylko kilka prostych kroków, aby komputer stał się bezpieczny.

sieci Internet). Nie nadawaj pełnych uprawnień administracyjnych dla żadnego z kont w systemie, włączając w to swoje. Znacznie lepszym rozwiązaniem jest stworzenie specjalnego konta w systemie, które będzie używane tylko w przypadku instalacji nowego oprogramowania lub poważnych zmian w konfiguracji.

5. BEZPIECZEŃSTWO MOBILNE

Jeżeli posiadasz komputer mobilny, taki jak laptop, powinieneś się zastanowić nad szyfrowaniem całego dysku twardego (z ang. Full Disk Encryption - FDE). Szyfrowanie zapewnia, że nawet w przypadku utraty sprzętu Twoje dane są nadal bezpieczne. Dodatkowo, upewnij się, że w momencie gdy nie jesteś przy swoim komputerze, ekran urządzenia pozostaje zablokowany. Taką funkcjonalność mają np. wygaszacze ekranu. Najnowsze urządzenia mobilne są wyposażone w usługę umożliwiającą ich lokalizację lub w przypadku kradzieży zdalne kasowanie danych. Pamiętaj jednak, że po uruchomieniu funkcji zdalnego kasowania danych z reguły nie ma możliwości ich odzyskania, nawet jeśli urządzenie zostanie odnalezione.

Bezpieczny komputer w siedmiu krokach

6. BEZPIECZNE WYKORZYSTANIE.

Żadna ilość zabezpieczeń nie jest w stanie uchronić Twój komputer przed każdym typem zagrożenia. Wszystko, co było opisane do tej pory, pomoże zabezpieczyć Twój komputer, ale ostatnim elementem zawsze pozostaniesz Ty, użytkownik. Zrozum i zapamiętaj, że przestępcy zawsze starają się Cię oszukać. Jeśli otrzymasz wiadomość, która wygląda podejrzanie lub po prostu jest z nią coś nie tak, nie klikaj w żaden link ani nie otwieraj załączników. Jeżeli ktoś zadzwoni do Ciebie twierdząc, że masz zainfekowany komputer i jedynym sposobem, aby usunąć wirusa jest instalacja dodatkowego "pomocniczego" oprogramowania - to jest to najprawdopodobniej próba oszustwa. W większości przypadków to nie technologia, a właśnie Ty - użytkownik - jesteś najlepszą ochroną dla swojego komputera.

7. KOPIE ZAPASOWE.

Nawet jeśli wykonałeś wszystkie wyżej opisane kroki, zawsze istnieje ryzyko, że Twój komputer może paść ofiarą cyfrowych włamywaczy, ulec zniszczeniu lub po prostu się popsuć. Ostatnią deską ratunku w takich przypadkach pozostają kopie bezpieczeństwa. Gorąco zalecamy, aby wykonywać je regularnie, zwłaszcza w przypadku naprawdę ważnych danych. Dobrym i od dawna sprawdzonym rozwiązaniem jest wykonywanie kopii zapasowych na zewnętrznych dyskach twardych, ale ostatnio coraz bardziej popularne staje się wykonywanie kopii bezpieczeństwa w chmurze, czyli w serwisach takich jak np. Dropbox.

ŹRÓDŁA

W celu poprawy czytelności tekstu niektóre odnośniki w biuletynie zostały skrócone przy użyciu usługi TinyURL. Dla zachowania bezpieczeństwa, OUCH! używa funkcji podglądu TinyURL, która pozwala podejrzeć docelowy adres odnośnika oraz pyta o pozwolenie przed wejściem na stronę o docelowym adresie.

Free Security Checkups:
http://preview.tinyurl.com/bxph6a8

Microsoft Security:
http://preview.tinyurl.com/sd8

Mac OS X Security:
http://preview.tinyurl.com/abl6xm7

Common Security Terms:
http://preview.tinyurl.com/6wkpae5

SANS Security Tip of the Day:
http://preview.tinyurl.com/6s2wrkp

DOWIEDZ SIĘ WIĘCEJ

Zasubskrybuj comiesięczny Biuletyn Bezpieczeństwa Komputerowego – SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS z zakresu 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

Redakcja: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak, Paweł Jacewicz, Łukasz Siewierski