Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu

- **Aktualizacje**
- **Wtyczki i dodatki**
- **Ustawienia bezpieczeństwa**
- **Prywatność**

Bezpieczeństwo i prywatność w przeglądarkach

EDYTOR GOŚCINNY

Mike Poor jest edytorem gościnnym tego wydania biuletynu OUCH! Mike jest starszym analitykiem bezpieczeństwa korporacji InGuardians Inc. (www.inguardians.com) oraz starszym instruktorem w SANS Institute, gdzie prowadzi jeden z najlepszych kursów SANS dotyczących wykrywania włamań „SEC503 Intrusion Detection".

WSTĘP

Twoja przeglądarka internetowa (Internet Explorer, Firefox, Chrome czy Safari) to jedno z podstawowych narzędzi używanych do interakcji z Internetem. Cyberprzestępcy doskonale o tym wiedzą i dlatego przeglądarka to jeden z podstawowych celów ich ataków. Ponadto przeglądarka może zgromadzić ogromną ilość prywatnych informacji o Tobie, czego możesz nie być świadomy. W tym biuletynie przedstawimy kroki jakie możesz podjąć aby chronić zarówno swój komputer jak i swoją prywatność.

AKTUALIZUJ SWOJĄ PRZEGLĄDARKĘ

Pierwszym krokiem do właściwej ochrony jest korzystanie z najnowszej wersji przeglądarki. Nie ma znaczenia jakiej przeglądarki używasz, najważniejsze aby było to jej najbardziej aktualne wydanie. Cyberprzestępcy ciągle szukają i znajdują błędy programistyczne oraz inne wady w przeglądarkach. Kiedy taki błąd zostaje znaleziony (często nazywa się go podatnością), może zostać wykorzystany dając atakującemu dostęp a czasem całkowitą kontrolę nad Twoim systemem. Firma która wyprodukowała Twoją przeglądarkę (np. Microsoft, Mozilla ,Google czy Apple) publikuje łatki aby naprawić te podatności. Mając zainstalowaną zawsze najnowszą wersję sprawiasz, że w Twojej przeglądarce wszystkie znane producentowi podatności zostały naprawione. Upewnij się, że jest włączona opcja automatycznych aktualizacji, zarówno przeglądarki jak i systemu operacyjnego. Niektóre przeglądarki aktualizują się same za każdym razem kiedy ponownie je uruchamiasz.

WTYCZKI I DODATKI

Wtyczki (czasem nazywane dodatkami) to programy, które możesz zainstalować w swojej przeglądarce aby zwiększyć jej funkcjonalność. Problemem z nimi związanym jest to, że mogą one narażać Ciebie i Twój system na dodatkowe ryzyko. Każdy taki program który dodajesz do swojej przeglądarki ma swoje własne słabości i podatności. Instaluj tylko te rozszerzenia, które są Ci rzeczywiście potrzebne i upewnij się, że pobierasz je z dobrze znanych, zaufanych stron. Czasami strona którą odwiedzasz może zażądać instalacji wtyczki. Bądź ostrożny, to mogą być próby nakłonienia Cię do instalacji złośliwego

Bezpieczeństwo i prywatność w przeglądarkach

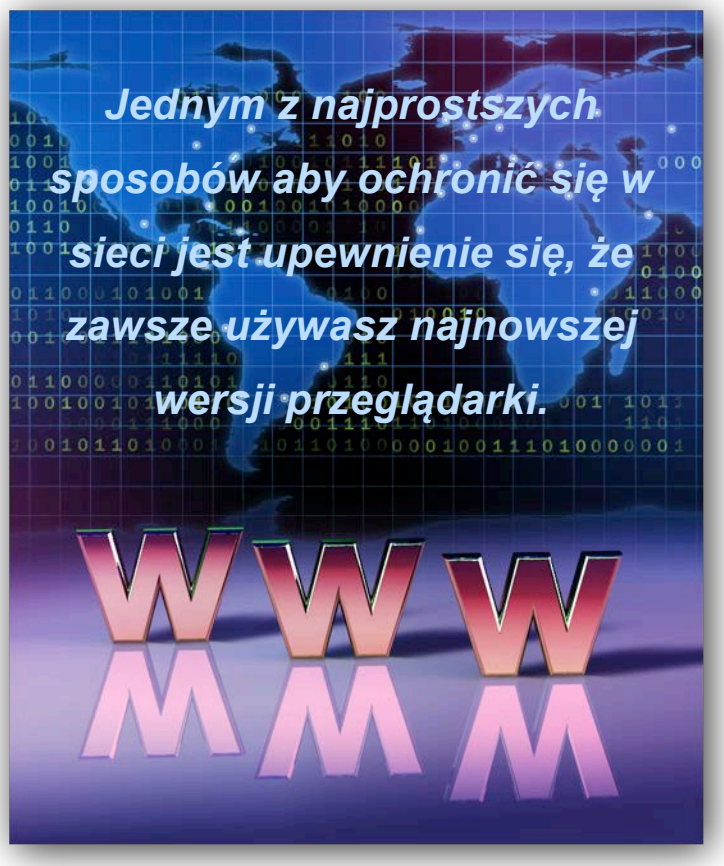
oprogramowania. O ile to możliwe zawsze pobieraj i instaluj wtyczki z oryginalnej strony jej producenta. Przykładowo, zawsze pobieraj i aktualizuj Flash Playera ze strony Adobe www.adobe.com. Po zainstalowaniu wtyczki dopilnuj aby była ona zawsze aktualna, tak samo jak Twoja przeglądarka. Niekoniecznie może być to proste, ze względu na to, że wiele wtyczek nie posiada funkcji automatycznej aktualizacji, wtedy trzeba je sprawdzać i instalować we własnym zakresie. Jeśli masz do czynienia z takim przypadkiem zalecamy sprawdzanie statusu wtyczek w Twojej przeglądarce przynajmniej raz w miesiącu. W części „Zasoby" znajdują się odnośniki do kilku zaufanych stron, które pomogą Ci tego dokonać.

USTAWIENIA BEZPIECZEŃSTWA

Każda przeglądarka ma swoje własne ustawienia opcji związanych z bezpieczeństwem. Warto poświecić chwilę na dokładne przyjrzenie się im. Podstawową funkcją niemal wszystkich przeglądarek jest ostrzeganie użytkownika, kiedy odwiedza on potencjalnie złośliwą stronę. Twoja przeglądarka ma dostęp to aktualnej listy tysięcy stron uznanych za złośliwe. Jeśli podejmiesz próbę odwiedzenia jednej z takich stron Twoja przeglądarka powstrzyma Cię i wyświetli ekran ostrzegawczy. Kiedy natkniesz się na taką wiadomość, nie przechodź dalej do strony mimo, że będziesz miał taką możliwość. Miej zawsze na uwadze, że powinieneś być zawsze ostrożny na stronach które odwiedzasz. Twoja przeglądarka nie będzie zawsze mogła nadążyć za cybeprzestępcami, ani być w posiadaniu informacji o wszystkich stronach, które są złośliwe.

PRYWATNOŚĆ

Możesz sobie nie zdawać sprawy z tego, że Twoja przeglądarka może przechowywać ogromne ilości informacji o Twojej aktywności w sieci, w tym ciasteczka, strony zachowane w pamięci podręcznej i historię.



Ciasteczka to niewielkie pliki, które strony internetowe wysyłają do Twojej przeglądarki i dzięki nim korzystanie z sieci jest nieco prostsze (na przykład poprzez zapamiętywanie wprowadzonych na stronach preferencji). Jednak ciasteczka pozwalają też firmom na śledzenie Twoich zachowań w sieci. Z kolei strony zachowane w pamięci podręcznej mają pomóc w ulepszeniu wydajności systemu, ale mogą też mieć do nich dostęp nieautoryzowani użytkownicy. I wreszcie wiele przeglądarek przechowuje historię odwiedzonych przez Ciebie stron. Dzięki tej funkcji przeglądarka może szybciej przenieść Cię do najczęściej odwiedzanych miejsc w sieci.
Aby chronić swoją prywatność możesz wyłączyć niektóre z tych funkcji. Zazwyczaj przeglądarki dają możliwość ręcznego usunięcia przechowywanych danych albo

Bezpieczeństwo i prywatność w przeglądarkach

automatycznego ich usuwania za każdym razem kiedy zamykasz swoją przeglądarkę. Wszystkie przeglądarki wspierają też tzw. „tryb prywatności", wtedy wszystkie opcje zbierania danych zostają wyłączone, w tym pamięć podręczna, ciasteczka i historia. W tym trybie nie są zbieranie żadne informacje dotyczące Twojego przeglądania stron, jednak może to ograniczyć możliwość interakcji z niektórymi stronami. Sprawdź ustawienia prywatności swojej przeglądarki, aby zmienić niektóre z tych ustawień.

Kiedy tylko to możliwe upewnij się, że połączenia z Twojej przeglądarki są szyfrowane. To pozwala, aby Twoja aktywność w sieci, nawet jeśli zostałaby przechwytywana, nie zostanie odczytana. Szyfrowane połączenia często nazywane są HTTPS. Na przykład strony takie jak Twitter, Facebook czy Google pozwalają na ustawienie, aby za każdym połączeniem z tymi stronami łączyć się przy użyciu HTTPS, czyli połączenia szyfrowanego. Można to potwierdzić upewniając się że adres rozpoczyna się od https:// lub pojawiającej się w przeglądarce ikony kłódki.

ŹRÓDŁA

Niektóre odnośniki w biuletynie zostały skrócone przy użyciu usługi TinyURL dla lepszej czytelności tekstu. 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.

Narzędzie sprawdzające aktualność wtyczek BrowserCheck:
http://preview.tinyurl.com/3m9gjr5

Sprawdź wtyczki do Firefoxa:
http://preview.tinyurl.com/3ojhl69

Bezpieczeństwo przeglądarki Chrome:
http://preview.tinyurl.com/36sgakv

Bezpieczeństwo przeglądarki Internet Explorer 9:
http://preview.tinyurl.com/3ly6wyv

Bezpieczeństwo przeglądarki Safari:
http://preview.tinyurl.com/aesqpl

Bezpieczeństwo przeglądarki Firefox:
http://preview.tinyurl.com/6ee3kx6

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 reagownia 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, Carmen Ruyle Hardy
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak and Paweł Jacewicz