

OUCH!

W tym wydaniu

- Wstęp
- Systemy operacyjne
- Aplikacje
- Rozszerzenia przeglądarek

Aktualizowanie oprogramowania

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

W tym miesiącu przyjrzymy się bliżej temu, dlaczego aktualizacje systemu operacyjnego, aplikacji i wtyczek do przeglądarek internetowych są niezbędne aby czuć się bezpiecznie i zadbać o swoją prywatność. Przedstawione zostaną również narzędzia i sposoby pomocne w utrzymaniu aktualnego i bezpiecznego komputera.

Podatności to błędy lub słabości w oprogramowaniu, które mogą zostać w każdej chwili wykorzystane przez cyberprzestępców. Niestety nowe i nieznanne podatności są ciągle odkrywane. Tacy producenci oprogramowania jak Microsoft czy Apple regularnie wydają aktualizacje (lub łatki) dla swoich produktów aby naprawić te podatności. Dlatego właśnie aktualizowanie oprogramowania jest zasadniczym krokiem do własnej ochrony.

SYSTEMY OPERACYJNE

Każdy komputer i urządzenie przenośne posiadają system operacyjny, czyli oprogramowanie pozwalające na interakcję z urządzeniem. Przykładami takich systemów działających na komputerach stacjonarnych jest Microsoft Windows lub Mac OS X. Z kolei systemami na urządzenia mobilne są na przykład Apple's iOS czy Android OS.

Microsoft Windows, wieloletni ulubiony cel ataków, posiada narzędzie sprawdzające i aktualizujące system operacyjny automatycznie. Microsoft Update dba o aktualizację, nie tylko samego systemu Windows, ale także wielu innych zainstalowanych na komputerze aplikacji firmy Microsoft, takich jak Office. Mac OS X posiada podobną funkcjonalność dbającą o utrzymanie składników systemu operacyjnego oraz pakietów oprogramowania wydanych przez Apple w aktualnej wersji.

Należy pamiętać, że oprócz włączenia automatycznych aktualizacji oprogramowania, komputer musi mieć możliwość ich pobrania i zainstalowania oraz że niektóre aktualizacje wymagają ponownego uruchomienia systemu operacyjnego żeby zacząć działać. Aby usługa automatycznych aktualizacji działała jak najefektywniej, zalecamy ustawić sprawdzanie dostępnych aktualizacji w trybie codziennym, wybrać porę dnia, kiedy system jest włączony i aktywny (nie w stanie wstrzymania lub hibernacji) i ma dostęp do Internetu. Kiedy zostanie wyświetlony monit o ponowne uruchomienie komputera, należy to zrobić bezzwłocznie. Aktualizacje automatyczne Windows i Mac OS X mogą być również wyzwalane ręcznie jeśli zachodzi taka potrzeba.

System iOS dla urządzeń mobilnych jak iPhone i iPad nie posiada narzędzia do automatycznej aktualizacji oprogramowania. Użytkownik musi sam ręcznie sprawdzić i zainstalować aktualizacje przy pomocy iTunes. Android 2.x posiada wbudowane narzędzie automatycznych aktualizacji, które dba zarówno o system operacyjny jak i

Aktualizowanie oprogramowania

zainstalowane aplikacje. Wymaga ono zgody użytkownika na zainstalowanie aktualizacji kiedy są one gotowe.

APLIKACJE

Aplikacje to wszystkie dodatkowe programy nie wchodzące w skład systemu operacyjnego, instalowane na komputerze lub urządzeniu przenośnym. Niezwykle ważne dla bezpieczeństwa komputera czy urządzenia przenośnego jest bycie świadomym jakie aplikacje zostały na nim zainstalowane, czy posiadają one wbudowane narzędzia aktualizacji i czy narzędzia te są włączone. Im więcej aplikacji zostało zainstalowanych na urządzeniu, tym większe ryzyko, że jest ono podatne na włamanie. To bardzo istotny powód dla którego powinno się instalować tylko te aplikacje, które są rzeczywiście regularnie używane i odinstalować te niepotrzebne i nieużywane. Pewna liczba najbardziej znanych aplikacji, takich jak MS Office, Adobe Acrobat Reader czy Java, posiada wbudowaną usługę automatycznych aktualizacji, jednak większość niestety nie. W wypadku jakichkolwiek wątpliwości, najlepiej jest odwiedzić stronę producenta aplikacji aby dowiedzieć się co można zrobić aby była ona aktualna.

Takie śledzenie wszystkich aplikacji na swoim komputerze i ich aktualizacji może być nie lada wyzwaniem. Na szczęście istnieją narzędzia, które mają w tym pomóc. Godnym polecenia jest Secunia "Personal Software Inspector" (PSI). PSI skanuje komputer w poszukiwaniu zainstalowanych aplikacji, podejmuje próbę ustalenia, które z nich są nieaktualne i podaje linki, dzięki którym można uaktualnić swoje oprogramowanie. Niestety nie ma porównywalnego narzędzia dla Mac OS X, które byłoby godne polecenia na obecną chwilę. Jedynie pewną funkcjonalność wskazywania nieaktualnego oprogramowania oferuje Mac App Store, ale tylko dla aplikacji w nim zakupionych.

Aktualizacje automatyczne nie są wbudowane w iOS Apps i tylko od użytkownika zależy czy ściągnie je poprzez iTunes ręcznie. Natomiast Android 2.x posiada wbudowane narzędzie aktualizacji automatycznych które dba zarówno o aplikacje jak i o system operacyjny, wymaga jedynie zgody użytkownika na ich instalację.

Regularne aktualizowanie systemu operacyjnego, aplikacji i rozszerzeń do przeglądarek to jeden z najlepszych sposobów dla zabezpieczenia Twojego komputera.



ROZSZERZENIA PRZEGLĄDAREK/ROZSZERZENIA/DO DATKI

Wreszcie ostatnim elementem na który należy zwrócić uwagę są rozszerzenia przeglądarek internetowych, zwane również wtyczkami lub dodatkami (ang. plug-ins, add-ons). To niewielkie aplikacje które zwiększają funkcjonalność standardowej przeglądarki, takie jak Adobe Flash Player, Apple QuickTime czy Microsoft Silverlight. W miarę jak ilość

Aktualizowanie oprogramowania

wtyczek w przeglądarkach znacznie się zwiększyła, stały się one popularnym celem cyberataków, ponieważ utrzymanie ich w najnowszej wersji nie jest wcale proste. I tutaj znów kluczem do własnej ochrony jest wiedza jakie dodatki są zainstalowane i czy są one aktualne. Większość przeglądarek daje możliwość sprawdzenia jakie wtyczki są zainstalowane i w jakiej wersji. Niektóre popularne wtyczki aktualizują się automatycznie.

Sprawdzanie które wtyczki są aktualne może być czasochłonne. Qualys's Browser Check to proste, łatwe w obsłudze i dostępne przez stronę internetową narzędzie, które pozwala szybko stwierdzić jakie wtyczki są zainstalowane, które z nich są nieaktualne i podpowiada w jaki sposób je uaktualnić. Ponadto, jak już wspomniano, najpopularniejsze przeglądarki posiadają wbudowane narzędzia do sprawdzania i aktualizacji swoich wtyczek.

- Mozilla posiada webowe narzędzie dla Firefox'a, które wykrywa wtyczki innych producentów i wskazuje skąd można pobrać ich aktualizacje.
<http://preview.tinyurl.com/firefox-plugincheck>
- Chrome całkowicie wyłącza wszystkie nieaktualne wtyczki automatycznie. Kliknięcie „Aktualizuj wtyczkę” przekierowuje użytkownika na stronę producenta wtyczki, gdzie można pobrać jej najnowszą wersję.
<http://preview.tinyurl.com/444vc59>
- Safari posiada automatyczne aktualizacje wtyczek (rozszerzeń), nie są one jednak domyślnie włączone. Aby to zrobić, należy otworzyć okno Preferencje w przeglądarce Safari i wybrać zakładkę Rozszerzenia. Następnie wybrać opcję „Uaktualnienia” na dole listy rozszerzeń i zaznaczyć „Instaluj uaktualnienia automatycznie”.
<http://preview.tinyurl.com/3bou9z6>

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.

Aktualizacja Windows: <http://preview.tinyurl.com/26glz4q>
Aktualizacja OS X: <http://preview.tinyurl.com/4qmuqs>
Aktualizacja iOS: <http://preview.tinyurl.com/55freg>
Aktualizacja Android: <http://preview.tinyurl.com/3ycw2zr>
Secunia's Personal Software Inspector (PSI):
<http://preview.tinyurl.com/5wu6xo>
Qualys's Browser Check:
<http://preview.tinyurl.com/3m9gjr5>

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>

Biuletyn OUCH! powstaje w ramach programu „Securing The Human” Instytutu SANS i jest wydawany na licencji [Creative Commons BY-NC-ND 3.0 license](http://creativecommons.org/licenses/by-nc-nd/3.0/). Powielanie treści biuletynu jest dozwolone jedynie w celach niekomercyjnych oraz pod warunkiem zachowania informacji o źródle pochodzenia kopiowanych treści jak i samego biuletynu. Informacje kontaktowe: ouch@securingthehuman.org.

Redakcja: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner, Carmen Ruyle Hardy
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak and Paweł Jacewicz