Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W TYM NUMERZE..

Koniec ery Windows XP

Wstęp

Windows XP stał się jednym z najpowszechniej używanych systemów operacyjnych w historii komputerów. W pewnym momencie był zainstalowany na większości komputerów na świecie. Jednak obecnie Windows XP jest już przestarzałym systemem operacyjnym i wsparcie dla niego ze strony firmy Microsoft wkrótce się skończy. Planowaną datą jest 8 kwietnia 2014 roku. Oznacza to, że więcej nie będą pojawiać się uaktualnienia i łatki, które naprawiałyby w nim błędy. Nadal około 25% komputerów na świecie korzysta z systemu Windows XP i w momencie kiedy skończy się czas życia tego systemu (z ang. End Of Life, EOL) miliony użytkowników będą narażone na niebezpieczeństwo. Należy pamiętać, że nie mówimy tu tylko o komputerach domowych, ale także tych w biurach, fabrykach (systemy sterowania produkcją), bankomatach (to także normalny komputer często z Windows XP), szpitalach (komputery obsługujące np. systemy podtrzymywania życia), sklepach (kasy fiskalne i systemy POS) oraz całej masie innych urządzeń. W dalszej części artykułu opisujemy jakie jest ryzyko związane z wygaśnięciem wsparcia dla Windows XP oraz co można zrobić, aby nadal pozostać bezpiecznym gdy to nastąpi.

Redaktor gościnny

Jason Fossen pracuje w firmie Enclave Consulting LLC gdzie zajmuje się bezpieczeństwem systemów z rodziny Microsoft Windows. Jest także autorem kursu Securing Windows with the Critical Security Controls (SEC505) w Instytucie SANS oraz autorem skryptów PowerShell dostępnych na jego blogu **http://cyber-defense.sans.org/blog/**.

Cykl życia systemu operacyjnego

Może nie zdajecie sobie z tego sprawy, ale system operacyjny Waszego komputera ma ograniczony czas życia. Wydawca systemu operacyjnego udostępnia dla niego łatki oraz uaktualnienia, dodaje nowe funkcje, usprawnia stabilność i wydajność oraz stara się, aby system operacyjny pozostawał zabezpieczony. Kłopot pojawia się wtedy, gdy wydawca przestaje wspierać starszy system operacyjny i skupia swoje zasoby na nowych i doskonalszych produktach oraz technologiach. Oznacza to, że dla starszego systemu operacyjnego przestaną pojawiać się uaktualnienia i łatki bezpieczeństwa, nawet jeśli znane będą w nim luki umożliwiające przejęcie nad nim kontroli przez cyberprzestępców. To właśnie stanie się z Windowsem XP w kwietniu tego roku.

Jak się zabezpieczyć

W celu pozostania bezpiecznym i odpornym na zagrożenia należy używać systemu opracyjnego, który jest aktywnie wspierany przez producenta. Jeśli masz bardzo stary komputer, może to oznaczać, że nie będzie wspierany przez najnowsze systemy operacyjne. Niestety oznacza to, że będziesz musiał zaopatrzyć się w nowy sprzęt. W przypadku gdy Twój komputer jest zgodny z najnowszymi systemami operacyjnymi wystarczy zakup wersji systemu, która jest wspierana. Firmy i instytucje powinny zastanowić się nad uaktualnieniem wszystkich maszyn z systemem Windows XP do wersji z systemem Windows 7, a nie Windows 8. Wynika to z faktu, że interfejs systemu Windows 7 jest

Koniec ery Windows XP

znacznie bardziej zbliżony w wyglądzie i obsłudze do systemu Windows XP i nie powinien sprawiać kłopotów użytkownikom. Jednakże Windows 8 jest znacznie bardziej bezpieczny ze względu na ulepszenia w oprogramowaniu. Dodatkowo, poza Windows, istnieją także inne systemy operacyjne, jak np. Apple Mac OS X lub Ubuntu Linux, których używanie możesz rozważyć. Którykolwiek byś nie wybrał, teraz nadchodzi czas na zmianę i nie możesz zbyt długo czekać. Jeśli nie uda Ci się zmienić systemu przed kwietniem, rozważ następujące kroki:

W chwili gdy Windows XP przestanie być wspierany najlepszą metodą, aby zapewnić sobie bezpieczeństwo jest zmiana na nowy system operacyjny, który jest regularnie aktualizowany.

- Używaj systemu Windows XP tylko do wykonywnia absolutnie zadań i aplikacji, które nie mogą funkcjonowac w żadnym nowszym systemie operacyjnym. W takim przypadku staraj się nie używać tego komputera do przeglądania Internetu lub czytania poczty elektronicznej.

- Jeśli musisz używać tego komputera do przeglądania poczty, to nie korzystaj z Internet Explorera. Zainstaluj inną przeglądarkę, np. Firefoxa, Chrome-a lub Operę. Upewnij się, że zawsze korzystasz z najnowszej wersji oraz wydawca przeglądarki nadal ją aktualizuje dla systemu Windows XP.

- Przestań używać innych aplikacji systemu Windows XP, które potrafią otwierać pliki ściągane z Internetu lub otwierać bezpośrednio zasoby z sieci, jak np. Microsoft Media Player. Podobnie jak w punkcie wcześniej, zainstaluj aplikacje, których wydawcy nadal udostępniają ich aktualizacje dla systemu Windows XP.

- Używaj serwisów wspierających bezpieczeństwo Twojego komputera, jak np. darmowy OpenDNS. Takie serwisy blokują dostęp do znanych złośliwych stron. Dodatkowo niektóre z nich potrafią wykryć, jeśli Twój komputer próbuje łączyć się ze znanymi kontrolerami botnetów, co jednoznacznie wskazuje, że Twój komputer jest zainfekowany.

- Upewnij się, że używasz jednego z programów wspierających bezpieczeństwo Twojego komputera, jak np. programy antywirusowe. Pamiętaj, żeby też upewnić się, że taki program jest nadal wspierany i aktualizowany dla systemu Windows XP.

- Jeśli Twój komputer nie musi być podłączony do Internetu (np. jeśli używasz go tylko do pisania dokumentów), to najlepiej będzie jeśli odłączysz go od sieci. Jeśli to nie jest możliwe, upewnij się, że sieć jest chroniona przez firewall oraz masz zainstalowany swój prywatny firewall i jest on aktywny (blokuje niechciany ruch do Twojego komputera). W przypadku sieci korporacyjnych, dobrą praktyką jest odseparowanie komputerów z Windows XP w odrębną sieć, aby w przypadku infekcji nie zagrażały innym maszynom.

Koniec ery Windows XP

- Rób regularny backup danych, aby móc je odzyskać w przypadku infekcji komputera wirusem. Jedna z kopii powinna być przechowywana offline, tzn. nie być na medium, które jest stale podłączone do komputera z którego wykonujemy backup. Jeśli musisz odzyskać dane w przypadku infekcji lub awarii, zalecamy aby wykonać to na maszynie z nowym systemem operacyjnym. Jeśli przywrócisz backup na maszynie z systemem Windows XP, to prawdopodobnie w krótkim czasie znowu może dojść do infekcji.

Jeśli używasz systemu Windows XP w swojej firmie, Twój pracodawca może wymagać dodatkowych kroków poza opisanymi wcześniej. Pamiętaj jednak, że to tylko chwilowe środki zaradcze i nie zapewnią bezpieczeństwa jakie daje poprawnie skonfigurowany system operacyjny wspierany i regularnie aktualizowany przez wydawcę. Prędzej czy później będziesz musiał zmienić swój stary system operacyjny na nowy.

Dowiedz się więcej

Zasubskrybuj comiesięczny biuletyn o bezpieczeństwie komputerowym SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS dotyczące 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

Źródła

Microsoft EOL Announcement:
http://www.microsoft.com/pl-pl/windows/enterprise/endofsupport.aspx
OpenDNS:
www.opendns.org
OUCH!: Backup i przywracanie osobistych danych:
http://www.securingthehuman.org/ouch/2013#september2013

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak, Paweł Jacewicz, Łukasz Siewierski