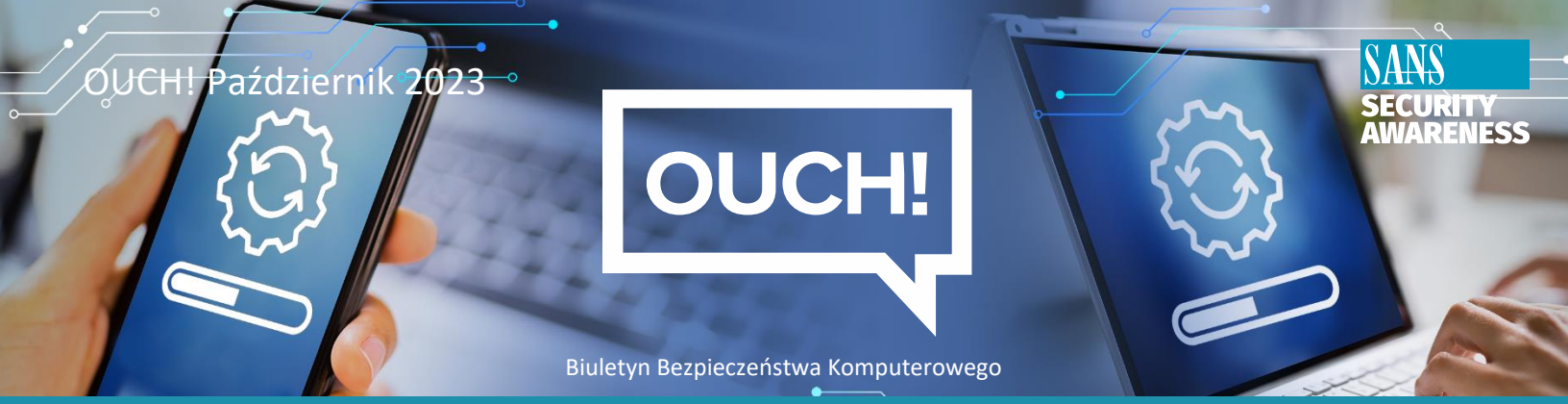

Moc aktualizacji

Wstęp

Cyberprzestępcy nieustannie poszukują i wykorzystują podatności w oprogramowaniu, z którego korzystasz na co dzień. Podatność w zabezpieczeniach to zazwyczaj pewnego rodzaju błąd podczas tworzenia oprogramowania. Narażone na zagrożenie oprogramowanie może być uruchamiane na wieli urządzeniach m.in. na laptopie, smartfonie, a nawet w niani elektronicznej i innych urządzeniach w domu i nie tylko. Cyberprzestępcy wykorzystują te podatności, aby włamać się do systemów i przejąć na nimi kontrolę. Jednocześnie dostawcy oprogramowania i urządzeń stale opracowują poprawki podatności i wypuszczają je jako aktualizacje oprogramowania. Jednym z najlepszych sposobów ochrony jest upewnienie się, że urządzenia mają wgrane najnowsze aktualizacje. Te aktualizacje nie tylko naprawiają znane luki w zabezpieczeniach, ale często dodają nowe funkcje bezpieczeństwa, znacznie utrudniając cyberprzestępcom włamanie się do nich.

Jak działa aktualizacja

Gdy w oprogramowaniu zostaje odkryta podatność, dostawca oprogramowania utworzy poprawkę dla tej właśnie luki (nazywaną łatką) i publikuje aktualizację. System następnie pobiera i instaluje tę aktualizację. Przykłady oprogramowania, które należy zaktualizować, to:

- Systemy operacyjne laptopów (np. Microsoft Windows lub Apple macOS) lub smartfonów (np. Android lub iOS)
- Domowy sprzęt sieciowy (np. router) lub inteligentne domowe urządzenia, takie jak termostaty, dzwonki do drzwi, sprzęt gospodarstwa domowego lub kamery
- Programy działające na urządzeniach, takie jak przeglądarka internetowa laptopa lub aplikacje mobilne w telefonie

Dlatego za każdym razem, gdy kupujesz nowy program komputerowy lub aplikację mobilną, najpierw sprawdź, czy producent systematycznie je aktualizuje. Im dłużej oprogramowanie działa bez żadnych aktualizacji, tym bardziej prawdopodobne jest, że znane są już podatności w zabezpieczeniach, które mogą wykorzystać cyberprzestępcy. Właśnie dlatego wielu dostawców, takich jak Microsoft, automatycznie wydaje nowe poprawki bezpieczeństwa co miesiąc. Jeśli nie używasz już któregoś z programu komputerowego, oprogramowania lub aplikacji mobilnej, usuń je z systemu. Im mniej zainstalowanego oprogramowania, tym mniej potencjalnych luk w zabezpieczeniach i tym większe bezpieczeństwo.

Jeśli którekolwiek z twoich urządzeń lub aplikacji jest stare i nie jest już obsługiwane przez dostawcę, zalecamy zastąpienie ich nowszymi wersjami, które są na bieżąco aktualizowane i wspierane.

Jak wykonać aktualizację

Istnieją dwa sposoby aktualizacji systemów.

1. **Ręczny (trudny sposób)**: Gdy dostępna jest aktualizacja, należy ją ręcznie pobrać i zainstalować. Daje to większą kontrolę nad tym, jakie aktualizacje są instalowane i kiedy to następuje. Wadą ręcznych aktualizacji jest to, że wymaga to znacznie więcej pracy, ponieważ musisz śledzić, kiedy każde z urządzeń lub programów wymaga aktualizacji i należy je aktualizować ręcznie.

2. **Automatyczny (prosty sposób)**: Włączasz automatyczne aktualizacje na wszystkich urządzeniach, co oznacza, że za każdym razem, gdy pojawia się nowa łatka, urządzenie automatycznie ją pobiera i instaluje. Zaletą automatycznych aktualizacji jest to, że większość pracy jest wykonywana za Ciebie. Wadą automatycznych aktualizacji jest to, że zaktualizowany program może powodować utratę funkcjonalności lub utratę danych. Co prawda, jest to rzadkie w przypadku osobistych urządzeń, ale może się zdarzyć w bardziej złożonych środowiskach, takich jak duże korporacje. Po włączeniu automatycznych aktualizacji pamiętaj o regularnym sprawdzaniu systemu, aby upewnić się, że aktualizacje są wykonywane.

Z tych dwóch podejść zdecydowanie zalecamy włączenie i korzystanie z automatycznych aktualizacji na wszystkich urządzeniach osobistych. Dzięki temu wszystkie używane urządzenia, od smartfonów i laptopów po monitory i zamki do drzwi, są wyposażone w najnowsze oprogramowanie. Urządzenia i programy na bieżąco aktualizowane znacznie utrudniają atakującym złamanie zabezpieczeń.

Redaktor gościnny

Dr Janell Straach jest wykładowczynią na Rice University, gdzie wykłada cyberbezpieczeństwo i sztuczną inteligencję. Janell jest przewodniczącą Rady ds. Kobiet w Cyberbezpieczeństwie (WiCyS). Dr Straachl jest dostępna pod adresemjanell@wicys.org.

Źródła

Cyfrowe wiosenne porządki w 7 krokach: https://www.sans.org/newsletters/ouch/digital-spring-cleaning-7-simple-steps/
Czy potrzebne są dodatkowe narzędzia zabezpieczające?: https://www.sans.org/newsletters/ouch/security-software/
Działania na emocjach - jak cyberprzestępcy oszukują: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz