Biuletyn Bezpieczeństwa Komputerowego

Przeglądarki internetowe

Wstęp

Dziesiątki milionów ludzi codziennie do przeglądania internetu korzysta z przeglądarek internetowych. Najpopularniejszymi przeglądarkami internetowymi są Google Chrome, Microsoft Edge, Apple Safari oraz Mozilla Firefox. Używa się ich do czytania wiadomości, sprawdzania poczty elektronicznej, robienia zakupów online, oglądania filmów i grania w gry. W związku z tym, przeglądarki są również celem cyberataków.
Wiele osób zakłada, że przeglądanie stron internetowych jest bezpieczne, jeśli odwiedza się tylko znane, zaufane witryny. Jednak dość łatwo jest przypadkowo kliknąć lub odwiedzić niebezpieczną stronę internetową, czasem nawet o tym nie wiedząc. Co więcej, same strony internetowe, które znasz i którym ufasz, mogą zostać zhakowane, a cyberprzestępcy mogą zainstalować na nich złośliwe oprogramowanie. Dzisiejsze przeglądarki posiadają wiele nowych funkcji, które często mogą być mylące, a w przypadku błędnej konfiguracji narażają użytkownika na jeszcze większe niebezpieczeństwa.

Bezpieczne korzystanie z przeglądarki

Oto niezbędne kroki do zabezpieczenia się:

Aktualizacja: Zawsze używaj najnowszej wersji przeglądarki. Korzystanie z najnowszych wersji oprogramowania eliminuje ryzyko występowania znanych błędów i zwiększa bezpieczeństwo. Zalecamy włączenie opcji automatycznej aktualizacji przeglądarki internetowej. Tylko wtedy mamy pewność, że korzystamy z narzędzia pozbawionego znanych podatności. W przypadku niektórych programów, wymagane będzie ponowne uruchomienie przeglądarki za każdym razem, gdy informuje Cię, że jest nowa aktualizacja. Po wgraniu aktualizacji warto sprawdzić czy nie pojawiły się nowe opcje zabezpieczeń.

Ostrzeżenia: Dzisiejsze przeglądarki często potrafią rozpoznać szkodliwe witryny internetowe, które zostały stworzone do różnego rodzaju oszustw. Jeśli zauważyłeś, że przeglądarka ostrzega Cię, że strona, którą zamierzasz odwiedzić jest niebezpieczna, zamknij tę kartę przeglądarki i znajdź to, czego potrzebujesz na innej stronie.

Synchronizacja: Nigdy nie synchronizuj przeglądarki służbowej z przeglądarką osobistą ani z żadnymi kontami osobistymi. Poprzez synchronizację umożliwiamy przeglądarkom na różnych urządzeniach, wymianę ustawień oraz udostępnienie informacji, takich jak historia przeglądania, zakładki oraz inne zapisane informacje.

Hasła: Przeglądarki internetowe umożliwiają zapisanie haseł którymi się logujesz do różnych serwisów. Zamiast przechowywać hasła w przeglądarce, zalecamy korzystanie z dedykowanych narzędzi, tzw. menedżerów haseł. Menedżery haseł to aplikacje, które mają możliwość przechowywania loginów i haseł do serwisów. Posiadają wiele funkcji oraz zabezpieczeń.

Wtyczki: Wtyczki lub rozszerzenia to dodatki do przeglądarek internetowych, które dodają dodatkowe funkcjonalności. Trzeba mieć jednak na uwadze, że instalowana do przeglądarki wtyczka może posiadać podatności, które pozwolą atakującym na przechwycenie wrażliwych danych. W przypadku komputera służbowego dodawaj tylko te wtyczki, które znasz, które są autoryzowane i zatwierdzone. Dodatkowo tak samo jak w przypadku przeglądarki, nie zapomnij o aktualizowaniu wtyczek. Jeśli nie korzystać już z wybranej wtyczki, pozbądź się jej.

Prywatny tryb: Większość przeglądarek oferuję opcję prywatności (zwaną również "trybem incognito"). Oznacza to, że gdy otwierasz kartę przeglądarki w trybie prywatnym, ograniczasz jakie informacje są o Tobie zbierane. Na przykład przeglądarka nie gromadzi plików cookies, nie śledzi historii przeglądania i nie przechowuje ani nie rozpowszechnia wrażliwych informacji o użytkowniku.

Chat na żywo: Niektóre strony internetowe oferują funkcję czatu na żywo, gdzie można zadawać pytania. Korzystaj wyłącznie z tych czatów online, które dostępne są na znanych, zaufanych stronach. Ponadto ogranicz informacje, którymi dzielisz się podczas sesji czatu na żywo. Nie masz pojęcia, kto zbiera te informacje, co z nimi robi i komu może je sprzedać lub udostępnić w przyszłości.

Uważaj na zdalny dostęp: Podejrzane strony internetowe mogą próbować przejąć kontrolę nad urządzeniem. Jednym ze sposobów oszustów jest wyświetlanie fałszywych powiadomień w przeglądarce internetowej dotyczących np. zainfekowania systemu. W ten sposób oszuści próbują wymusić na użytkowniku natychmiastową reakcję i połączenie się czatem online z konsultantem. Następnie będą nalegać, abyś pozwolił im zainstalować program do zdalnego dostępu, który pozwoli im naprawić Twój komputer. Nie zgadzaj się na to. Jest to próba zainstalowania złośliwego oprogramowania, którym wykradną m.in. dane logowania do serwisów z których korzystasz.

Wyloguj się: Po zakończeniu korzystania z serwisu internetowego należy pamiętać o wylogowaniu się. Powoduje to usunięcie poufnych informacje dotyczących logowania i hasła przed zamknięciem przeglądarki.

Redaktor gościnny

Dean Parsons jest dyrektorem generalnym ICS Defense Force. Posiada ponad 20-letnie doświadczeniem w zakresie cyberobrony IT/ICS. Jest również certyfikowanym instruktorem SANS ICS515 i współautorem / instruktorem ICS418. Uczy aktywnej obrony cybernetycznej, reagowania na incydenty i zarządzania ryzykiem dla przemysłowych systemów kontroli. www.linkedin.com/in/dean-parsons-cybersecurity.

Źródła

Menedżer haseł: https://www.sans.org/newsletters/ouch/password-managers/
Moc aktualizacji: https://www.sans.org/newsletters/ouch/the-power-of-updating/
Ataki socjotechniczne: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Prywatność - chroń swoje cyfrowe życie: https://www.sans.org/newsletters/ouch/privacy/

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz