OUCH! Luty 2023

SANS SECURITY AWARENESS

OUCH!

Biuletyn Bezpieczeństwa Komputerowego

Czy potrzebne są dodatkowe narzędzia zabezpieczające?

Wstęp

W momencie kiedy kupowałeś komputer wiele lat temu, prawdopodobnie musiałeś zainstalować na nim dodatkowe oprogramowanie zabezpieczające, aby zapewnić mu bezpieczeństwo przed cyberatakami. Dzisiejsze nowe komputery i urządzenia mają już wbudowanych wiele funkcji bezpieczeństwa, takie jak automatyczne aktualizacje, zapory sieciowe czy szyfrowanie dysków. Ciekawostką jest, że firma Microsoft domyślnie udostępnia na urządzeniach z systemem operacyjnym Windows funkcję bezpieczeństwa o nazwie Microsoft Defender, która zawiera dodatkowe funkcje, m.in. antywirus. Pod wieloma względami dzisiejsze systemy operacyjne w konfiguracji domyślnej są znacznie bardziej bezpieczne. Niestety w tym momencie to człowiek jest najsłabszym punktem bezpieczeństwa każdego urządzenia. Dlatego właśnie cyberprzestępcy nieustannie obierają sobie za cel ludzi, próbując podstępem skłonić ich do robienia rzeczy, których nie powinni robić, takich jak podawanie haseł, klikanie w niebezpieczne linki lub otwieranie załączników przesłanych wiadomością e-mail.

Jakie narzędzia powinienem rozważyć?

Jeśli chcesz zwiększyć bezpieczeństwo swoich systemów, rozważ zaimplementowanie dodatkowych programów zabezpieczających.

Menedżer haseł: Hasła mogą być długie i skomplikowane, a zwłaszcza problematyczna może być konieczność ich zapamiętywania do setek różnych portali. Menedżer haseł to bezpieczny program, który chroni i przechowuje wszystkie hasła. Aby się do niego dostać, musisz zapamiętać jedynie hasło główne. Ponadto menedżery haseł wyposażone są w funkcje pomagające wymyślać złożone hasła oraz automatycznie wpisywać je do paneli logowania.

Virtual Private Network (VPN): Wirtualne Sieci Prywatne (VPN) skupiają się przede wszystkim na ochronie prywatności poprzez szyfrowanie połączenia z internetem i ukrywanie lokalizacji źródłowej.

Security Suites: to pakiety oprogramowania zabezpieczającego, które zapewniają zbiór dodatkowych funkcji bezpieczeństwa wykraczające poza te, które zapewnia system operacyjny. Na przykład filtrowanie niebezpiecznych stron internetowych, kontrola rodzicielska, a często także VPN. Każdy pakiet posiada inne funkcje, więc warto wypróbować wiele i wybrać ten, który czujesz, że jest dla Ciebie najlepszy.

Wybór dostawcy usług zabezpieczających

W przypadku konieczności zakupu dodatkowych narzędzi lub oprogramowania zabezpieczającego (np. program antywirusowy), istnieje wielu różnych dostawców, którzy oferują wiele tego typu narzędzi. Który z nich wybrać? Oferty dostawców oprogramowania często są do siebie bardzo zbliżone. Kluczem jest zastosowanie rozwiązania od zaufanego dostawcy. Nikt przecież nie chciałby zakupić i zainstalować oprogramowania zainfekowanego szkodliwym oprogramowaniem i dystrybuowanego przez cyberprzestępców.

Dlatego postaw na narzędzia dostarczanych od znanych sprzedawców, o których słyszałeś i którym możesz zaufać. Nigdy nie kupuj narzędzi od firm, o których nic nie wiesz, które są zupełnie nowe, nie mają żadnych opinii lub mają wiele negatywnych komentarzy. Podczas wyboru oprogramowania zwróć również uwagę czy dostawca zapewnia wieloletni dostęp do aktualizacji. Możesz nawet sprawdzić w jakim kraju sprzedawca ma swoją siedzibę. Istnieje wiele stron internetowych, które porównują różnice w funkcjach i kosztach użytkowania wybranych rozwiązań.

Podchodź z dozą ostrożności do darmowych narzędzi. Nigdy nie masz pewności, czy nie pojawią się niespodziewane problemy. Narzędzia te mogą mieć ograniczone funkcje, być trudne w użyciu lub nie być aktualizowane. W niektórych przypadkach darmowe narzędzia mogą być tworzone przez cyberprzestępców i używane do infekowania urządzeń szkodliwym oprogramowaniem.

Pomimo że te narzędzia są pomocne, zacznij najpierw od wbudowanych w urządzeniu funkcji bezpieczeństwa, w tym od włączenia automatycznej aktualizacji. Dzisiejsze systemy operacyjne domyślne są dosyć dobrze zabezpieczone. Pamiętaj, że to Ty jesteś dla siebie najlepszą ochroną. Zachowaj ostrożność w przypadku dziwnych lub podejrzanych połączeń telefonicznych, wiadomości e-maili lub tekstowych. Żadne oprogramowanie zabezpieczające na świecie nie jest w stanie ochronić Cię przed kimś, kto próbuje Cię oszukać lub nabrać na coś, czego nie powinieneś robić.

Redaktor gościnny

Nico "Dutch_OsintGuy" Dekens jest certyfikowanym instruktorem SANS i byłym rządowym analitykiem wywiadu specjalizującym się w Open-Source Intelligence (OSINT).Więcej informacji o Nico: https://www.sans.org/profiles/nico-dekens/
oraz tu https://www.dutchosintguy.com.

Źródła

Menedżer haseł: https://www.sans.org/newsletters/ouch/password-managers/
Moc aktualizacji: https://www.sans.org/newsletters/ouch/the-power-of-updating/
Virtual Private Networks: https://www.privacyguides.org/vpn/
Social Engineering: https://www.youtube.com/watch?v=lc7scxvKQOo
Security Suite Reviews: https://www.pcmag.com/picks/the-best-security-suites

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz