

Czym są wycieki DNS i jak ich uniknąć?

03.04.2023

W dzisiejszym cyfrowym świecie ochrona prywatności i trzymanie działań online z dala od wścibskich oczu mają kluczowe znaczenie. Postęp technologiczny umożliwił gromadzenie i sprzedaż danych (takich jak historia przeglądania, informacje osobowe, wiadomości e-mail) oraz korzystanie z aplikacji bez wiedzy i zgody użytkownika.

Chociaż skuteczny antywirus i dostęp do sieci VPN mogą wydawać się niezawodnym sposobem zapobiegania wydostawaniu się krytycznych danych z twojego połączenia, to czasami nawet one dopuszczają wyciek danych. Przykładem są wycieki DNS, które mogą zagrozić Twojej prywatności. Niestety wielu użytkowników nadal nie rozumie zagrożeń związanych z DNS, dlatego zespół Bitdefender postanowił wyjaśnić, czym są wycieki DNS i jak się ich wystrzegać.

Czym są wycieki DNS?

DNS, skrót od Domain Name System, to system, który jest kamieniem

węgielnym nowoczesnej infrastruktury internetowej. Jego znaczenie wynika z możliwości mapowania czytelnych dla człowieka nazw domen (np. example.com) na adresy IP, co pozwala użytkownikom na dostęp do treści online bez zapamiętywania adresów IP.

Błędna konfiguracja może niestety prowadzić do wycieków, sprawiając, że żądania DNS będą widoczne dla hakerów, a nawet dla własnego dostawcy usług internetowych.

Sieci VPN mogą chronić Twoje połączenie przed naruszeniami prywatności, przekierowując ruch przez prywatny tunel i szyfrując go. Godna zaufania sieć VPN powinna obejmować cały ruch, w tym żądania DNS.

Wyciek DNS ma miejsce zawsze, gdy Twoje żądania DNS są wysyłane do serwerów DNS Twojego dostawcy usług internetowych pomimo korzystania z VPN. Takie sytuacje mogą szybko sprawić, że sieci VPN staną się zbędne z powodu ujawniania prywatnych informacji.

Dlaczego wycieki DNS są niebezpieczne?

„Wycieki DNS są szczególnie niebezpieczne, ponieważ umożliwiają stronom trzecim dostęp do Twoich poufnych informacji, których zwykle nie mogą zobaczyć bez Twojej zgody, m.in. Twojego adresu IP, lokalizacji fizycznej, przeglądanych stron i wyszukiwań w Internecie. Chociaż głównym zagrożeniem związanym z wyciekami jest możliwość ujawnienia Twojej aktywności w sieci niepowołanym osobom, musisz

pamiętać, że uzyskane dane mogą zostać wykorzystane w bardziej destrukcyjny sposób. Wiedząc, które dokładnie witryny odwiedzasz, cyberprzestępcy będą mogli opracować plan skomplikowanych kampanii phishingowych lub ataków typu man-in-the-middle” – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Twój dostawca usług internetowych lub osoba korzystająca z tej samej sieci Wi-Fi może przeanalizować żądania DNS, które wyciekły z Twojego urządzenia, aby dowiedzieć się, jakie strony internetowe odwiedziłeś lub z jakimi usługami online się łączyłeś. Dlatego powinieneś regularnie monitorować szczelność swojego DNS.

Jak sprawdzić szczelność DNS?

Najprostszym sposobem, aby sprawdzić, czy nie masz wycieków DNS jest połączenie się z siecią VPN i serwerem, a następnie odwiedzenie strony internetowej, która umożliwia przetestowanie szczelności DNS, np. BrowserLeaks i przeprowadzenie testu adresu IP.

Wyniki serwera DNS nie powinny ujawniać żadnych informacji o Twojej prawdziwej tożsamości. Jeśli podczas testu okaże się, że istnieją wycieki DNS, warto rozważyć zmianę dostawcy dostępu do sieci VPN.

Zespół Bitdefender przypomina, że nawet dedykowane usługi wykrywania nieszczelności nie są niezawodne. Czasami test może

generować fałszywe wyniki. Aby upewnić się, że Twoja sieć VPN nie powoduje wycieku żądań DNS, wyczyść pliki cookie i pamięć podręczną przeglądarki, a następnie ponownie uruchom test. Warto także skorzystać z innego wykrywacza nieszczelności i porównać wyniki.

Nawet niewielkie wycieki danych mogą ujawnić Twoją prawdziwą tożsamość niepożądanym stronom. Wybór dostawcy, na którym możesz polegać, zapewni Ci anonimowość cyfrową, a co za tym idzie bezpieczeństwo tożsamości i prywatność Twojej aktywności online.

Źródło: <https://bitdefender.pl/czym-sa-wycieki-dns-i-jak-ich-uniknac/>

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.

Data udostępnienia: 03.04.2023

Z pozdrowieniami Piotr Rozmiarek

E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender

Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz

Czym są wycieki DNS i jak ich uniknąć?

Bitdefender

EDR i XDR.