Porady

VPN do użytku prywatnego – czy warto?

Paweł Wałuszko 30.12.2019

Ostatnimi czasy YouTube obrodził w reklamy pokazujące korzyści z używania technologii VPN dla osób prywatnych. Reklamodawcy zarzekają się, że VPN pozytywnie wpływa na bezpieczeństwo, szyfrując ruch, pozwala uniknąć śledzenia przez dostawcę Internetu (ISP) lub chroni przepływ danych podczas korzystania z niezabezpieczonego WiFi (np. miejskiego).

Jest jeszcze jedna zaleta, szczególnie często promowana w reklamach, to możliwość dotarcia do treści zablokowanych w danym położeniu geograficznym. Używając usług VPN, teoretycznie zyskujemy możliwość oglądania na Netflixie programów, które nie są dostępne w Polsce.

Oferta brzmi dobrze, ale czy w praktyce też jest tak kolorowo?

Jak działa VPN

Zanim zaczniemy dementować mity o VPN, przyjrzyjmy się bliżej mechanice działania tej technologii.

Za każdym razem, gdy wpisujesz adres URL lub korzystasz z przeglądarki, Twoje urządzenie automatycznie łączy się z licznymi serwerami dostawcy (ISP). Najczęściej są to serwery DNS, które „tłumaczą” adres strony internetowej (URL) na adres IP. Dla przykładu, wpisując w pasek wyszukiwarki „google.pl”, połączysz się z adresem 216.58.211.99.

Każde wysyłanie prośby o połączenie z danym adresem daje dostawcy możliwość sprawdzenia jakie strony odwiedzasz. Dość często dane te są gromadzone oraz używane w celach statystycznych, oraz marketingowych. Przykładowo, gdy wpiszesz niepoprawny adres URL, usługodawca może wyświetlić Ci komunikat, że taka strona nie istnieje oraz reklamę w jej miejsce.

Używając technologii VPN, łączysz się z Internetem odrobinę inaczej, mimo że samo przeglądanie stron wygląda niemal identycznie. Po pierwsze, po podłączeniu się do sieci WiFi, Twoje urządzenie nawiązuje szyfrowane połączenie z wybranym serwerem VPN. Od momentu połączenia z serwerem usługodawcy, wszelka komunikacja pomiędzy urządzeniem a Internetem odbywa się tylko i wyłącznie poprzez ten kanał.

Zważywszy na fakt, że komunikacja pomiędzy urządzeniem a serwerem VPN jest w pełni szyfrowana i “tunelowana” przez to łącze, Twoje zapytania do serwerów również DNS wychodzą z serwera usługodawcy, co w efekcie maskuje Twój ruch przed oczami dostawcy Internetu. Co więcej, przeciętny usługodawca posiada wielu użytkowników jednocześnie. Oznacza to, że jeden serwer VPN łączy się ze stronami internetowymi w imieniu wielu urządzeń klientów końcowych, co daje efekt pewnej anonimizacji ruchu.

Dostawca Internetu może stwierdzić tylko fakt, że nawiązałeś połączenie z serwerem VPN. Nie jest w stanie określić, jakie strony odwiedzasz lub do czego wykorzystujesz łącze po połączeniu z VPN-em. Z punktu widzenia ochrony prywatności, usługa VPN do celów prywatnych może wydawać się świetnym rozwiązaniem.

Uproszczony schemat przepływu danych przy wyświetlaniu strony internetowej bez usługi VPN

Uproszczony schemat przepływu danych pomiędzy stroną internetową a użytkownikiem przy użyciu VPN

Druga strona medalu

Zaleta „tunelowej” technologii VPN, niestety, może być również jej wadą.

Po pierwsze, warto mieć na uwadze, że wszelka komunikacja pomiędzy urządzeniem a Internetem jest kierowana do jednego punktu wyjściowego. Używając VPN, ukrywasz swój ruch przed dostawcą, ale w zamian, dajesz do niego dostęp firmie dostarczającej VPN.

Po drugie, nie zapominaj, że VPN jest pośrednikiem w Twoim połączeniu z Internetem. Jeżeli pośrednik jest nierzetelny lub został zhackowany, narażasz się na niebezpieczeństwo kradzieży danych osobowych lub inne problemy związane ze śledzeniem ruchu. Powinieneś mieć to szczególnie na uwadze, gdy korzystasz np. z bankowości internetowej.

Po trzecie, dostęp do serwera VPN położonego w innym kraju, niekoniecznie gwarantuje dostęp do zablokowanego contentu. Biorąc pod uwagę fakt, że wielu użytkowników korzysta z jednego serwera, firmy takie jak Hulu i Netflix mogą blokować dostęp do swoich serwisów z adresów IP serwerów VPN. Nic dziwnego — korzystanie z serwera zlokalizowanego w innym kraju niż użytkownik, jest jawnym obchodzeniem ich restrykcji.

VPN: Fakty i mity

Wokół technologii VPN narosło wiele mitów. Czas się z nimi rozprawić! Poniżej znajdziesz wyjaśnienie co do prawdziwości popularnych poglądów na temat VPN.

Jeżeli Twoim celem jest ukrycie ruchu przed dostawcą (ISP), VPN Ci w tym pomoże
Fakt. Warto jest jednak pamiętać, że ukrywanie ruchu przed ISP nie jest równoznaczne ze zwiększeniem prywatności w internecie. Nadal możemy być śledzeni np. przez firmy zarabiające na reklamach.

VPN gwarantuje prywatność w internecie
Mit. Po pierwsze, punkt końcowy (serwer) VPN ma możliwość wglądu do adresów stron, które odwiedzasz. Po drugie, prywatność w internecie zależy od wielu czynników, m.in. przeglądarki, z której korzystasz, systemu operacyjnego, plików cookies lub nawet sekwencji stron, które odwiedzasz.

Używając VPN, użytkownik zyskuje dostęp do contentu, który jest zablokowany w jego kraju
Z reguły tak. Niemniej, administratorzy serwisów mogą rozpoznać serwery VPN odwiedzające ich strony i zablokować połączenia wychodzące od tych serwerów.

VPN zabezpiecza komputer podczas korzystania z niezabezpieczonej sieci WiFi
Niekoniecznie. Większość stron internetowych korzysta z protokołu HTTPS, który sam w sobie jest szyfrowany. Używanie VPN w tym wypadku niewiele zmieni. VPN natomiast przyjść z pomocą, gdy połączysz się z siecią, która jest stworzona przez hakerów z myślą o przechwytywaniu danych (tak zwany „honeypot”).

VPN przyspieszy Internet
Mit. Niezależnie od tego, jak szybkie połączenie z Internetem posiada dostawca VPN, szybkość Internetu jest podyktowana jakością Twojego łącza. VPN może wręcz negatywnie wpływać na szybkość Internetu, ponieważ każde połączenie jest kierowane do jednego punktu wyjściowego, które jest współdzielone z wieloma użytkownikami.

VPN ukryje moją tożsamość przed władzami
Najprawdopodobniej nie. Każda legalna firma VPN działa jako podmiot gospodarczy w ramach pewnego rodzaju jurysdykcji. Jako podmiot prawny, firmy te są zobowiązane do przekazywania danych władzom w pewnych sytuacjach – np. na podstawie nakazu sądowego.

Warto jest wspomnieć, że niektóre firmy VPN mogą być zarejestrowane w krajach, w których obowiązują luźne przepisy dotyczące własności intelektualnej, lub w krajach, które wyrywkowo traktują prośby o współpracę pochodzące z krajów Unii Europejskiej. Choć z pewnego punktu widzenia taka lokalizacja dostawcy VPN może wydawać się zaletą, prowadzenie interesów z

podmiotem gospodarczym zarejestrowanym poza naszą jurysdykcją może okazać się hazardem.

Na co zwrócić uwagę przy wyborze usługodawcy VPN?

Jeżeli zdecydowałeś się na zakup usługi VPN, zwróć uwagę na kilka kluczowych aspektów oferty, które opiszę poniżej. Pozwoli Ci to wybrać najlepszego usługodawcę i uchroni przed niemiłą niespodzianką.

Po pierwsze, sprawdź rzetelność usługodawcy

Biorąc pod uwagę fakt, że cały ruch pomiędzy urządzeniem a Internetem będzie odbywał się przez jedno łącze, warto upewnić się, że usługodawca nie będzie gromadził, śledził lub analizował tegoż ruchu. W tym celu należy zapoznać się z polityką prywatności, regulaminem oraz sprawdzić opinie o usługodawcy. Pamiętaj też, że usługodawcy z innych krajów mogą mieć mniej lub bardziej restrykcyjne standardy ochrony prywatności, niż te obowiązujące w Polsce.

Po drugie, sprawdź szybkość łącza serwerów

Ponieważ Twoja komunikacja z Internetem będzie przekierowywana przez specyficzne serwery, warto sprawdzić, jak szybkie jest ich połączenie z Internetem oraz ilu użytkowników korzysta z tego samego serwera jednocześnie. Niestety może okazać się, że serwery są przeładowane i skrajnie spowolnią połączenie z Internetem.

Po trzecie, sprawdź lokalizację serwerów oraz ich ilość

Niektóre serwery VPN znajdują się na terenie kraju, inne poza jego granicami. Jeżeli zależy Ci na dostępie do treści z zagranicy, upewnij się, że usługodawca posiada kilka serwerów w preferowanym przez Ciebie kraju. Może okazać się na przykład, że na jeden serwer w USA przypadają setki użytkowników, co spowoduje, że zostanie on zablokowany przez niektórych dostawców. Nie zapominaj, że dla administratorów stron internetowych ruch z serwerów VPN może wyglądać niewiarygodnie lub przypominać atak, przez co część usług może być prewencyjnie zablokowanych.

Podsumowanie

VPN do tej pory w świecie informatycznym funkcjonowało głównie w kontekście biznesowym. Wiele firm korzysta z tej technologii od lat, oferując pracownikom możliwość bezpiecznej pracy zdalnej. Natomiast nowością na rynku jest wykorzystywanie jej przez użytkowników prywatnych w celu obchodzenia cenzury, geoblokad lub utrzymywania wyższego poziomu prywatności.

Jeśli jednak zdecydujesz się na używanie VPN, dokładnie przeanalizuj wady i zalety tego rozwiązania, a przede wszystkim znajdź dostawcę, który spełni Twoje wymagania.

Oceń artykuł:

30.12.2019

Paweł Wałuszko

Business Development Manager i Ekspert ds. Bezpieczeństwa. Doświadczony menedżer w branży IT, który swoje doświadczenie zdobywał m.in. w Dolinie Krzemowej; entuzjasta oprogramowania open - source.