VPN

Gabriela Białoskórska, **Mikołaj Knysak**, **Ignacy Tekieli**

January 2020

Spis treści

Wstęp

Jak działa VPN?

Bezpieczne połączenie z Internetem

Całkowita ochrona w Internecie

Komu jest potrzebny VPN?

Kiedy zalecane jest korzystanie z VPN?

W skrócie

WSTĘP

Czym jest VPN?

Skrót VPN (ang. Virtual Private Network) oznacza wirtualną sieć prywatną, czyli usługę szyfrującą dane przesyłane przez Internet w celu ochrony tożsamości użytkownika.

Bezpieczeństwo

VPN przekierowuje połączenie internetowe użytkownika do zdalnego serwera obsługiwanego przez dostawcę VPN. Oznacza to, że serwer ten staje się bezpiecznym punktem startowym przed dostępem do różnorodnych stron internetowych. Definicja VPN obejmuje również systemy firmowe. Taka biznesowa sieć VPN umożliwia pracownikom bezpieczny dostęp do sieci firmy podczas pracy poza biurem.

JAK DZIAŁA VPN?

Jak działa VPN?

W normalnych okolicznościach przy próbie uzyskania dostępu do Internetu użytkownik rozpoczyna od połączenia z dostawcą usług internetowych (ISP, ang. Internet Service Provider). Dostawca usług internetowych następnie przekierowuje użytkownika do wybranej strony internetowej (lub innych zasobów dostępnych w Internecie). Wszystkie dane przesyłane przez Internet przechodzą przez serwery ISP, co oznacza, że dostawca ma do nich dostęp i może je zarejestrować. Firmy te mogą przekazywać nawet historię przeglądania Internetu przez użytkownika reklamodawcom, instytucjom rządowym i innym podmiotom.

Jak działa VPN?

Właśnie wtedy VPN okazuje się bardzo przydatny, ponieważ przekierowuje ruch internetowy do specjalnie skonfigurowanego serwera VPN, ukrywając adres IP użytkownika i szyfrując wszystkie wysyłane i odbierane dane. Zaszyfrowane dane są niemożliwe do odczytania przez podmioty, które je przechwycą.

BEZPIECZNE POŁĄCZENIE Z INTERNETEM

Bezpieczne połączenie z Internetem

Weźmy pod uwagę publiczne sieci Wi-Fi, na przykład w kawiarni lub na lotnisku. Zazwyczaj łączymy się z nimi bez zastanowienia, ale czy wiemy, kto ma dostęp do danych przesyłanych przez łącza tego typu? Czy mamy pewność, że jest to bezpieczny hotspot? Czy mógłby być udostępniony przez cyberprzestępcę próbującego przechwycić Twoje dane osobowe? Dotyczy to haseł, danych konta bankowego, numerów kart kredytowych i wszystkich innych prywatnych danych przesyłanych w trakcie każdego połączenia z Internetem.

Bezpieczne połączenie z Internetem

Po włączeniu usługi VPN, wszystkie dane są przesyłane przez zaszyfrowany tunel, który uniemożliwia dostęp do danych osobowych osobom niepowołanym. Oznacza to, że nawet gdyby cyberprzestępca przechwycił dane użytkownika, nie będzie w stanie ich odszyfrować.

CAŁKOWITA OCHRONA W INTERNECIE

Całkowita ochrona w Internecie

Połączenie z Internetem nie jest w pełni bezpieczne jeżeli nie korzystasz z VPN'a. Niepowołane osoby lub urządzenia mogą uzyskać dostęp do danych użytkownika, zapisując je a następnie wykorzystujące w nieupoważniony sposób. Obejmuje to dostawcę usług internetowych, pracodawcę, router Wi-Fi w kawiarni i każdy pośredniczący serwer, a nawet niepowołaną osobę dysponującą odpowiednimi urządzeniami. Podmioty i serwisy mogą wykorzystać adres IP użytkownika związany z lokalizacją do ustalania różnych cen lub do wyświetlania natarczywych reklam.

Całkowita ochrona w Internecie

Połączenie VPN zabezpiecza użytkownika poprzez szyfrowanie danych i ochronę adresu IP. Dostawca usług internetowych nie wie, do których stron użytkownik uzyskuje dostęp, ponieważ cały ruch danych jest przekierowany przez serwer VPN. Oznacza to, że gromadzenie metadanych użytkownika i informacji o historii przeglądanych stron nie jest już możliwe. Najlepsze jest to, że ISP nie może udostępniać Twoich danych nikomu innemu.

KOMU JEST POTRZEBNY VPN?

Komu jest potrzebny VPN?

Nawet jeśli użytkownik nie ma nic do ukrycia, świadomość bycia obserwowanym i śledzonym powoduje dyskomfort. Głównym powodem, dla którego internauci wybierają usługi VPN, jest prywatność online i ogólne bezpieczeństwo.

Komu jest potrzebny VPN?

Podczas przeglądania Internetu przy użyciu usługi VPN komunikacja jest szyfrowana, więc dostawca usług internetowych, rząd, hakerzy i inne osoby trzecie nie są w stanie zobaczyć, które witryny były odwiedzane oraz nie mogą zakłócać aktywności online.

Komu jest potrzebny VPN?

Kolejną wielką zaletą korzystania z VPN jest to, że z jego pomocą można uzyskać dostęp do globalnego Internetu, gdziekolwiek się znajdujesz. VPN pozwala łączyć się z setkami zdalnych serwerów w różnych lokalizacjach, omijając cenzurę.

KIEDY ZALECANE JEST KORZYSTANIE Z VPN?

Częste korzystanie z publicznych sieci Wi-Fi

Usługa VPN jest bardzo przydatna podczas korzystania z publicznych sieci Wi-Fi, nawet jeżeli są one zabezpieczone hasłem. Połączenie z publicznymi hotspotami może wiązać się z licznymi zagrożeniami dla bezpieczeństwa danych. Istnieje wiele metod stosowanych przez hakerów do przechwytywania danych przesyłanych przez Internet, służących do kradzieży haseł, plików i zdjęć.

Częste podróże

Wybierasz się do obcego kraju? VPN umożliwia dostęp do usług, które mogą być niedostępne w danym kraju — np. w Chinach rząd blokuje dostęp do serwisów takich jak Facebook. Podczas wyjazdów do sąsiednich państw użytkownicy często tracą dostęp do niektórych serwisów przekazu strumieniowego, na które posiadają abonament.

Ukrycie aktywności przed podmiotami zewnętrznymi

Korzystanie z VPN jest przydatne również przy korzystaniu z Internetu we własnym domu. Załóżmy, że chcemy kupić prezent dla kilkuletniego bratanka, ale nie chcemy dostawać tysiąca reklam zabawek dla dzieci przez następnych sześć miesięcy.

W SKRÓCIE

W skrócie

Dostęp do Internetu przez VPN przypomina wysyłanie pocztą paczki w pudełku. Nikt nie może się dowiedzieć, co znajduje się w pudełku, do momentu jego otwarcia, czyli, w tym wypadku, do odszyfrowania danych.

W skrócie

Z chwilą połączenia się z usługą VPN, tworzony jest zaszyfrowany „tunel” przez Internet. Chroni on dane przesyłane pomiędzy użytkownikiem a miejscem docelowym, obejmujące wszystkie informacje, w tym dane internetowego konta bankowego.

W skrócie

Tunel ten powstaje początkowo poprzez uwierzytelnienie klienta VPN, np. komputera, smartfona lub tabletu, przez serwer VPN. Następnie serwer stosuje protokół szyfrowania do wszystkich danych przechodzących tam i z powrotem, między użytkownikiem a miejscem docelowym w sieci.

W skrócie

Należy pamiętać, że dane wysyłane i odbierane przez Internet są najpierw dzielone na tzw. pakiety. W celu ochrony każdego pakietu danych, VPN opakowuje każdy z nich w pakiet zewnętrzny, który następnie jest szyfrowany w ramach procesu zwanego hermetyzacją. Ten dodatkowy pakiet chroni dane podczas przesyłu, stanowiąc kluczowy element tunelu VPN. Po przesłaniu danych do serwera VPN zewnętrzny pakiet zostaje usunięty w wyniku procesu odszyfrowania danych.

W skrócie

Należy również pamiętać, że przy korzystaniu z VPN pakiety danych trafiają do Internetu z innym adresem IP dostarczonym przez dostawcę VPN. Przy łączeniu się z różnymi serwerami zdalnymi, za każdym razem użytkownik będzie widoczny w Internecie jako inna osoba. Jeżeli użytkownik połączy się z serwerem w innym kraju, będzie mieć dostęp do Internetu tak, jakby się w tym kraju znajdował.

Jak zainstalować i używać VPN?

Mimo że stosowanie VPN jest coraz częstsze, dla wielu użytkowników Internetu rozwiązania VPN to nadal czarna magia. To prawda, że niektóre systemy zabezpieczeń cyfrowych mogą być bardzo skomplikowane, lecz wiodący dostawcy serwisów VPN opracowują łatwe w użyciu i intuicyjne aplikacje.