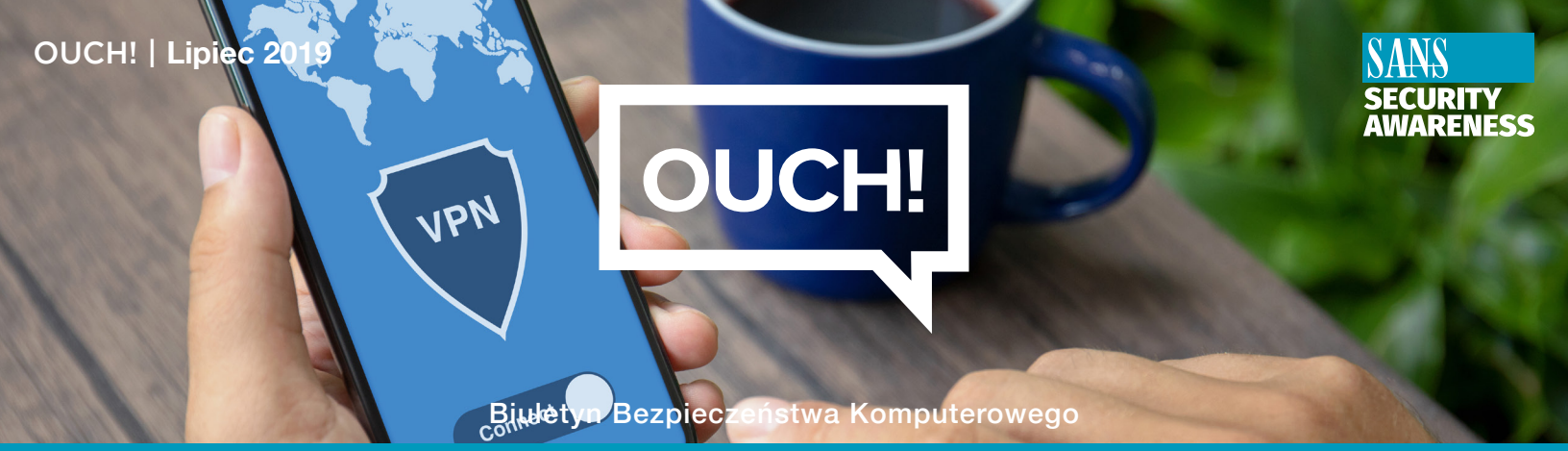


Biuletyn Bezpieczeństwa Komputerowego

# Wirtualne Sieci Prywatne (VPN)

## Wstęp

Niemal każdemu zdarza się skorzystać z publicznego Wi-Fi, kiedy będąc poza domem w restauracji, kawiarni czy podczas podróży w hotelu lub na lotnisku potrzebujemy skorzystać z dostępu do internetu. Ale czy publiczne sieci są bezpieczne i kto obserwuje lub rejestruje co robimy online? Prawdopodobnie nie ufamy nawet swojemu domowemu dostawcy internetu (ISP) i chcemy być pewni, że nie będzie wiedział co robimy w sieci. Można ochronić swoją prywatność i informację o czynnościach online dzięki Wirtualnej Sieci Prywatnej (VPN – Virtual Private Network). VPN to technologia która tworzy prywatny, szyfrowany tunel dla naszych działań online, czyniąc je o wiele trudniejszym dla innych do obserwowania lub monitorowania tego co robimy w internecie. Ponadto VPN ukrywa lokalizację użytkownika, utrudniając zidentyfikowanie naszego położenie stronom internetowym, które odwiedzamy.

## Jak to działa?

Wirtualna Sieć Prywatna działa poprzez utworzenie zaszyfrowanego tunelu do dostawcy usługi VPN, którą wybierzemy. Całość naszej sieciowej aktywności przechodzi przez ten tunel, następnie opuszcza sieć naszego dostawcy VPN i kieruje się do zamierzonego wcześniej celu. Dla przykładu jeśli przebywasz w Tampa (Floryda) i łączysz się z serwerem VPN w Monachium to każda strona którą odwiedzisz będzie identyfikować twoją lokalizację jako Monachium. Korzystanie z VPN jest proste. W pierwszej kolejności należy znaleźć dostawcę usługi VPN któremu zaufamy, a następnie należy założyć konto (VPN to z reguły usługa płatna). Gdy już mamy konto, ściągamy i instalujemy oraz konfigurujemy oprogramowanie obsługujące dany VPN. Po zainstalowaniu i konfiguracji możemy połączyć się z internetem jak zawsze. Oprogramowanie dostawcy VPN w cichy sposób utworzy szyfrowany kanał i zacznie chronić naszą prywatność, tak że nawet nie zdążymy się zorientować.

## Wybór dostawcy VPN

Nasza aktywność w internecie będzie bezpieczna i poufna tylko w takim zakresie w jakim jest nasz dostawca VPN. Upewnijmy się wybierając zaufanego dostawcę. Oto najważniejsze elementy na które powinniśmy zwrócić uwagę wybierając dostawcę.

**Logowanie:** Szukajmy usługi, która nie przechowuje logów i skupia się na zachowaniu prywatności. Jeśli nasz dostawca nie przechowuje logów to utrudnia to komukolwiek wyśledzenia historii naszej aktywności online.

**Gdzie znajduje się siedziba przedsiębiorstwa:** Dostawcy VPN zlokalizowani są w różnych krajach, upewnijmy się czy nasz dostawca rezyduje w kraju, które gwarantuje prawo do prywatności. W przypadku dostawców zlokalizowanych w krajach o słabej gwarancji powyższych praw istnieje ryzyko że dostawca zostanie zmuszony do przekazania informacji, które zbierał o tobie.

**Serwery:** Szukajmy usługi VPN która ma zlokalizowane serwery w krajach i miastach, które okażą nam się przydatne. Niektórzy dostawcy VPN mają tysiące serwerów zlokalizowanych na całym świecie. Upewnijmy się że nasz dostawca może dostarczyć nam adresy z konkretnego kraju który nas interesuje.

**Kompatybilność:** Zwróćmy uwagę na usługi które działają na różnych komputerach i urządzeniach mobilnych. Dla przykładu możemy używać laptopa z systemem Windows, tabletu i iPhone'a. Musimy więc znaleźć usługę VPN która zadziała na wszystkich naszych urządzeniach.

**Unikajmy darmowych:** Powinniśmy być ostrożni w stosunku do tzw. "darmowych" VPN-ów. Podejrzane jest to w jaki sposób utrzymują się na rynku, darmowe usługi mogą wiązać się z gromadzeniem i sprzedawaniem informacji o nas.

VPN to fantastyczny sposób na ochronę naszej prywatności w internecie. Niemniej jednak, VPN nie zabezpiecza naszych komputerów, urządzeń i kont internetowych. Dlatego nawet jeśli korzystamy z VPN, przestrzegajmy zawsze następujących zasad bezpieczeństwa: zadbajmy o aktualizację naszych urządzeń, blokujmy ekran oraz stosujmy silne niepowtarzalne hasła dla poszczególnych kont.

## Polski przekład

CERT Polska jest zespołem działającym w strukturach NASK, powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w polskiej sieci Internet. Należy do organizacji FIRST, w ramach której współpracuje z podobnymi zespołami na całym świecie.
WWW: http://www.cert.pl
Twitter: @CERT_Polska
Facebook: http://facebook.com/CERT.Polska

## Redaktor wydania

***Phil Johnsey*** *(@peakreflections) jest specjalistą IT w hrabstwie Palm Beach i zajmuje się bezpieczeństwem, informatyką śledczą i audytem. Może pochwalić się certyfikatami SANS z podstaw bezpieczeństwa oraz informatyki śledczej, ponadto jest członkiem społeczności recenzentów OUCH. Jego pasją jest popularyzacja tematyki bezpieczeństwa w sieci.*

## Źródła

| | |
|---|---|
| Czyniąc hasła prostymi: | https://www.sans.org/u/Sd8 |
| Zabezpieczenie urządzenia mobilnego: | https://www.sans.org/u/Sdd |
| Stop złośliwemu oprogramowaniu: | https://www.sans.org/u/Sdi |