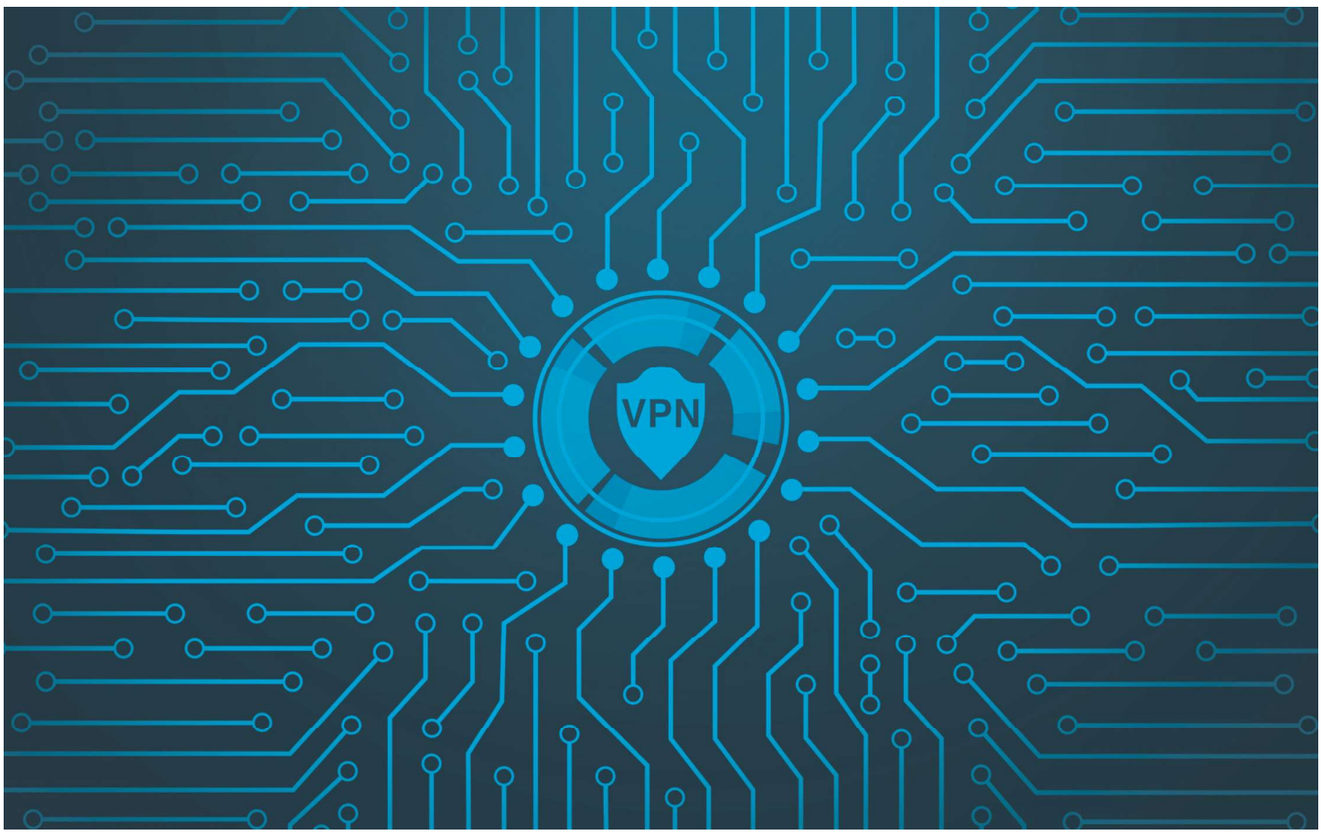


Sicher surfen

Wer seine Endgeräte über ein privates virtuelles Netzwerk (VPN) mit dem Internet verbindet, schützt seine Privatsphäre und verhindert, dass Cyberkriminelle den Datenverkehr mitlesen.

Hier erfahren Sie, wie man VPN nutzt und was es bringt. ● VON BEAT RÜDT

Personalisierte Werbung, die Sie auf dem Streifzug durchs Internet begleitet, Hotelpreise, die bei jedem erneuten Besuch eines Vermittlungsportals ansteigen, und geblockte Inhalte auf Streamingplattformen: Das sind Beispiele dafür, wie Betreiber von Webdiensten die Spuren ausnutzen, die wir im Netz hinterlassen.

Das ist nervig, aber nicht ganz so gefährlich wie ein Internetzugriff über ein ungeschütztes WLAN, während Cyberkriminelle Ihren Datenverkehr mitlesen und wichtige Informationen stehlen.

Beide Probleme können gelöst werden, indem man sicherstellt, dass man seine Identität beim Zugriff aufs Internet verschleiert und die Daten konsequent verschlüsselt.

Dafür gibt es eine Lösung: ein virtuelles privates Netzwerk, kurz VPN. Statt direkt auf Dateien und Dienste zuzugreifen, macht der Datenverkehr den Umweg über dieses verschlüsselte Netzwerk.

Was macht ein VPN?

Normalerweise wird ein Computer direkt über den Internetprovider mit dem Internet verbunden. Wird eine Webseite oder eine andere Webdienstleistung aufgerufen, wird die Anfrage direkt vom Computer an diesen Anbieter gesendet. Dieser Datenverkehr kann auch unverschlüsselt geschehen, womit die übermittelten Daten von Aussenstehenden und vom Internetanbieter theoretisch eingesehen werden können. Der Internetdienstanbieter weiss zudem, von welchem Computer die Anfrage kommt. Das ist sowohl aus Sicherheitsgründen als auch aus Datenschutzgründen heikel.

Hier kommt das VPN ins Spiel: Auf dem Computer wird eine Software installiert, welche die Daten verschlüsselt, noch bevor sie den Rechner verlassen. Diese werden an den Server des VPN-Anbieters übermittelt. Erst von dort wird der gewünschte Internetdienst aufgerufen. Als Absender sieht der Dienstanbieter nur den VPN-Server. Der Computer, von dem die Anfrage kommt, wird hingegen verborgen, Bild 1.

Was nützt VPN im Alltag?

Wenn Sie zum ersten Mal mit eingeschaltetem VPN surfen, werden Sie sofort feststellen, dass Sie keine personalisierte Werbung mehr sehen. Der Grund: Wegen der verschleierten IP-Adresse erkennen die Werbenetzwerke nicht mehr, wer genau zugreift. Das verhindert einerseits personalisierte Werbung, andererseits aber auch, dass die Webseite erkennt, aus welchem Land Sie zugreifen. Wenn Sie internationale Websites aufrufen, sehen Sie nicht mehr zwingend Angebote, die speziell für Schweizerinnen und Schweizer gemacht werden, was Auswirkungen auf die angezeigte Währung und Sprache haben kann – aber auch auf die Preisgestaltung.

Foto: Shutterstock/BERK CAN

SCHUTZ IM OFFENEN WLAN

Wenn Sie öffentliche WLAN-Zugangspunkte nutzen, beispielsweise in einem Restaurant oder im öffentlichen Verkehr, schützt das VPN die Verbindung zu Ihrem Router. Selbst wenn dieser keine oder eine schlecht verschlüsselte Verbindung anbietet, sind die Daten bei der Übertragung dank der Verschlüsselung des VPNs jederzeit gegen fremde Blicke abgesichert.

KEIN GEOBLOCKING

Unter Geoblocking versteht man den Ausschluss von Internetnutzern aus bestimmten Ländern. Diese Technik verwenden diverse Fernsehstationen auf ihrer Webseite, weil sie gewisse Inhalte nur dem heimischen Publikum anbieten dürfen.

Das merkt man zum Beispiel, wenn man im Ausland ist und den neusten Tatort anschauen möchte. Surft man in diesem Fall über einen VPN-Server in der Schweiz, merkt die Webseite nicht mehr, dass man aus dem Ausland auf die Website zugreift.

Derselbe Trick lässt sich nutzen, wenn man bei einem Streamingdienst einen Film oder eine Serie schauen möchte, die zum Beispiel nur in den USA im Programm ist. Nach dem Umstellen des Serverstandorts sehen Sie immer die Filmbibliothek des gewählten Landes.

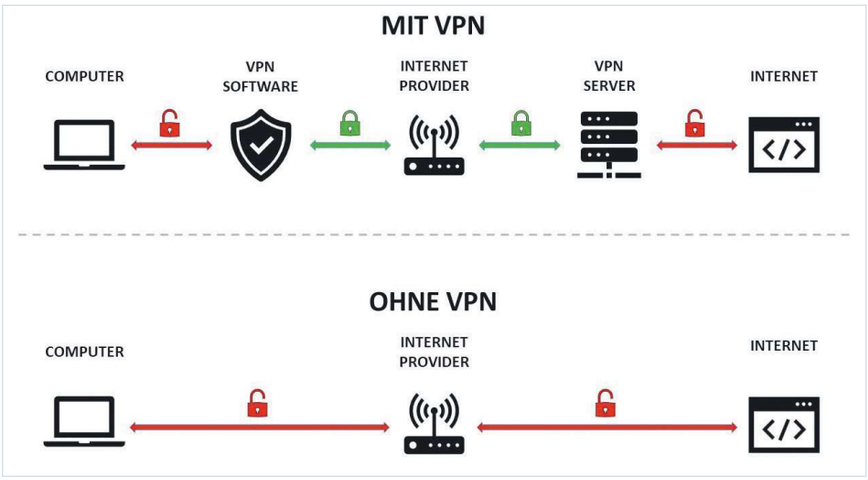


Bild 1: Der VPN-Server schaltet sich zwischen Nutzer und Website

Wie installieren?

Bei den meisten Anbietern erhalten Sie erst Zugriff auf die VPN-Software, nachdem Sie einen Preisplan gewählt und die gewünschte Zahlungsmethode festgelegt haben. Sie haben aber in der Regel 30 Tage Zeit, das Abonnement wieder zu kündigen, und erhalten den Kaufpreis zurückerstattet. Zu den wenigen Ausnahmen zählen windscribe.com sowie protonvpn.com (mehr dazu in der Tabelle auf S. 20). Diese beiden Tools können Sie auch installieren und ausprobieren, ohne die Zahlungsmethode festzulegen.

AUF DEM PC

Registrieren Sie sich beim Anbieter, laden Sie die Software auf Ihren PC herunter und folgen Sie den Installationsschritten. Am Ende des Prozesses wird die VPN-Software gestartet. Alles, was Sie jetzt noch tun müssen: Loggen Sie sich ein, wählen Sie den Standort (respektive das Land) und einen der dort verfügbaren Server aus. Danach starten Sie das VPN mit einem Klick auf den *On*-Schalter, Bild 2. Möchten Sie die VPN-Verbindung wieder trennen, klicken Sie erneut auf den Schalter.

AUF DEM SMARTPHONE

Fürs Smartphone holen Sie sich die Apps direkt im zugehörigen Store (Android oder iOS). Beim ersten Aufstarten müssen Sie noch die VPN-Konfiguration erlauben, Bild 3. Danach melden Sie sich an, wählen einen passenden Server aus, schalten das VPN ein und surfen geschützt los. Auch hier beenden Sie die VPN-Verbindung durch erneutes Drücken des Buttons.

Mögliche Probleme

Die meisten Webseiten und -dienste funktionieren bei eingeschaltetem VPN problemlos. Die Software und die Verschlüsselung verlangsamen aber die Verbindung – auch wenn dies in den meisten Fällen kaum spürbar ist. Einige Anbieter von Webdienstleistungen – insbesondere Streamingplattformen – versuchen, Kundinnen und Kunden zu blockieren, die via VPN zugreifen. Die VPN-Anbieter wiederum finden immer wieder neue Wege, diese Blockaden zu umgehen. Somit ist der Zugriff nicht immer und nicht über alle Anbieter möglich. Zudem sind VPNs nicht in allen Ländern legal oder es sind nur vom Staat betriebene VPNs zugelassen. Dem versuchen die VPN-Anbieter entgegenzuwirken, indem sie ihre Netzwerke so verschleiern, dass sie nicht mehr als VPN erkannt werden. ➜

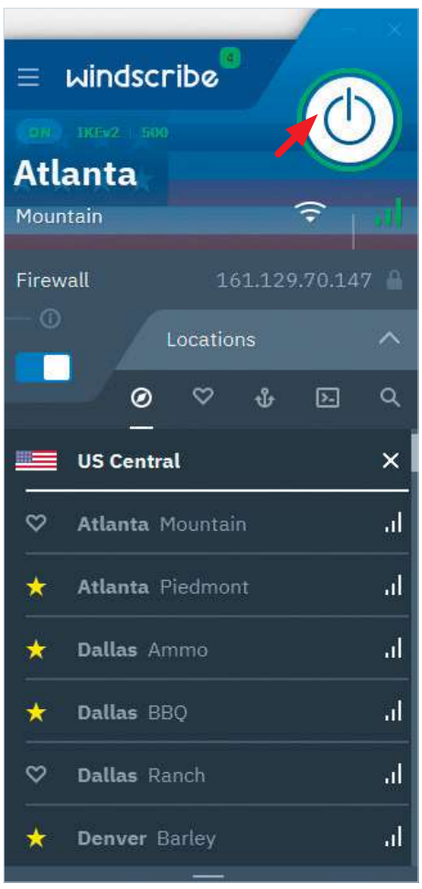


Bild 2: Mit nur einem Klick auf den Schalter oben aktivieren Sie das VPN

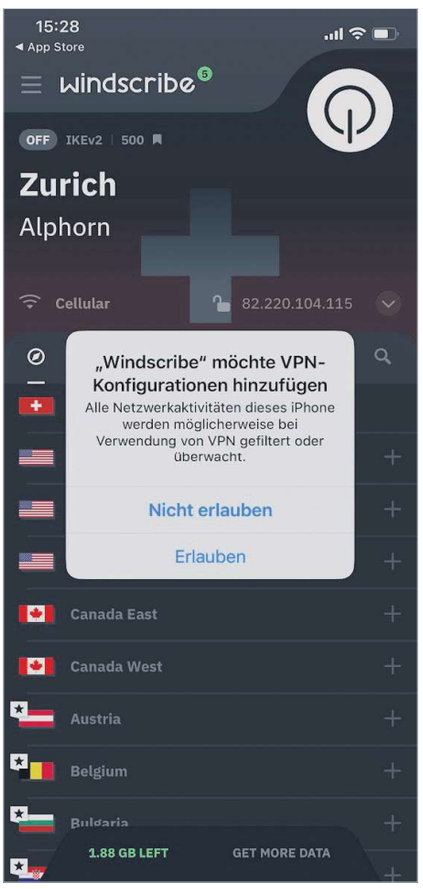


Bild 3: Per Smartphone-App gehts genauso einfach wie am PC

Kaufratgeber

Damit eine VPN-Software ihren Zweck erfüllt, muss die Verschlüsselung sicher sein. Die meisten Anbieter setzen auf den Advanced Encryption Sandard (kurz AES; fortschrittlicher Verschlüsselungsstandard). Das ist ein Verschlüsselungsverfahren, bei dem der Schlüssel zum Ver- und Entschlüsseln der Daten identisch ist.

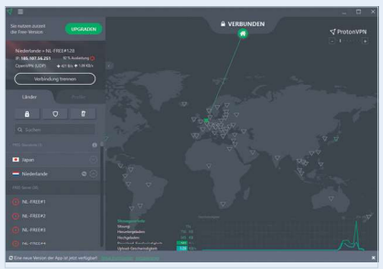
Eine Schlüssellänge von 256 Bit ermöglicht den grösstmöglichen Schutz. Bis heute ist keine Angriffsmethode bekannt, mit der nach diesem Verfahren verschlüsselte Daten geknackt werden können.

Ausserdem lohnt es sich, einen Blick auf die Anzahl Server zu werfen, die ein Anbieter betreibt. Theoretisch gilt hier: je mehr, desto besser. Denn bei grösserer Anzahl dürfte das Volumen der gleichzeitigen Nutzerinnen und Nutzer sinken, ausserdem stehen mehr Standorte zur Verfügung, sodass man nicht immer über den gleichen Server auf die Dienste zugreift. Oft bieten nicht alle Server die exakt gleichen Möglichkeiten an. So versuchen etwa Streamingdienste, VPN-Server zu blockieren, weil sie den Standort der Kundinnen und Kunden nicht mehr ermitteln können. VPN-Dienstleister wehren sich dagegen, indem sie neue Zugangspunkte eröffnen.

Wenn Sie VPN-Server in einem bestimmten, nicht europäischen oder nordamerikanischen Land nutzen möchten, lohnt sich ein Blick auf die Standortliste des Anbieters, um sicherzugehen, dass er dort tatsächlich über einen Serverstandort verfügt.

Achten Sie ausserdem darauf, wie viele Geräte mit einem Account betrieben werden dürfen. Die Angebote reichen von unbegrenzt bis zu einer bestimmten Anzahl (fünf bis zehn). Wenn Sie neben Computer, Smartphone und Tablet noch Smart-TVs und Router per VPN nutzen möchten, kann dies relevant sein.

TIPP: Gratis-VPN



Proton bietet ein kostenloses VPN

Die meisten VPN-Anbieter locken Unentschlossene mit einem 30-Tage-Rückgaberecht oder einem ersten Gratismonat. Nicht so das Schweizer Unternehmen Proton: Hier gibt es eine eingeschränkte Version des VPN, das gänzlich gratis genutzt werden kann. Die Software wird unter dem Link protonvpn.com angeboten und kann auf einem Computer oder Smartphone installiert werden.

Gegenüber der Bezahlversion gibt es einige Einschränkungen. Es stehen nur wenige Server in Japan, in den Niederlanden und in den USA zur Verfügung. Ausserdem ist die Surfgeschwindigkeit auf «mittel» reduziert und es kann nur ein Gerät genutzt werden. Zusatzdienste wie Werbeblocker oder Unterstützung für Streaming sind in der Gratisversion ebenfalls deaktiviert.

Nichtsdestotrotz ermöglicht Proton die Installation einer VPN-Software, die es Ihnen erlaubt, den Service für eine beliebige Zeit kostenlos zu testen und erste Erfahrungen zu sammeln.

Die grössten VPN-Anbieter im Vergleich

Anbieter https://	Anzahl Server	Anzahl Länder	Verschlüsselung	Plattformen	Preis/ Monat
Atlas VPN atlasvpn.com	750	48	256-Bit-AES	Windows, macOS, Android, iOS, Linux	$ 2.05
CyberGhost VPN cyberghostvpn.com	> 100	91	256-Bit-AES	Windows, macOS, Android, iOS, Linux	ab Fr. 2.11
Express VPN expressvpn.com	160	94	256-Bit-AES	Windows, macOS, Android, iOS, Linux	ab $ 6.67
IP Vanishj ipvanish.com	> 2000	75	256-Bit-AES	Windows, macOS, Android, iOS, Linux	$ 3.33
Nord VPN nordvpn.com	5500	59	256-Bit-AES	Windows, macOS, Android, iOS, Linux	Fr. 5.39
Private Internet Access privateinternetaccess.com	keine Angaben	84	256-Bit-AES	Windows, macOS, Android, iOS, Linux	ab Fr. 2.25
Private VPN privatevpn.com	200	63	256-Bit-AES	Windows, macOS, Android, iOS, Linux	€ 1.97
Proton VPN protonvpn.com	1750	64	256-Bit-AES	Windows, macOS, Android, iOS, Linux	€ 4.99 (gibts auch gratis)
Surfshark surfshark.com	3200	99	256-Bit-AES	Windows, macOS, Android, iOS, Linux	€ 2.21
Windscribe windscribe.com	500	69	256-Bit-AES	Windows, macOS, Android, iOS, Linux	$ 5.75 (gibts auch gratis)

Stand: November 2022

ZUSATZDIENSTLEISTUNGEN

In den meisten Fällen sind in einem Abonnement auch noch Zusatzdienstleistungen und -funktionen inbegriffen. Oft macht die Menge der Zusatzdienstleistungen nebst der Vertragsdauer den Unterschied in der Preisgestaltung aus. Mögliche Zusatzleistungen sind:

- **Werbeblocker:** Ist VPN eingeschaltet, wird die Werbung auf Webseiten blockiert.
- **Tracker-Blocker:** Mit Trackern versuchen Werbetreibende, Besucher wiederzuerkennen. Der Blocker verhindert, dass die entsprechende Scripte aufgerufen werden.
- **Webseiten-Blocker:** Der Dienstleister verfügt über eine Datenbank mit potenziell gefährlichen Webseiten. Wird eine aufgerufen, sperrt das VPN den Zugang.
- **No-Logs:** Der VPN-Anbieter verzichtet darauf, den Datenverkehr zu protokollieren. So ist es auch für ihn im Nachhinein unmöglich festzustellen, wer zu welcher Zeit auf einen Dienst zugegriffen hat.
- **Kill Switch:** Mit diesem Panik-Schalter kann die Internetverbindung mit einem Klick komplett getrennt werden. Es fliessen keine Daten mehr vom und zum Computer.
- **Cloud-Speicher:** Zusätzlich zum VPN wird ein verschlüsselter Cloud-Speicher angeboten, auf dem wichtige Dateien sicher abgelegt werden können.
- **Passwortspeicher:** Ein geräteübergreifender Passwortmanager speichert alle Passwörter verschlüsselt ab.
- **Datenleckscanner:** Passwörter und Kreditkartendaten werden mit öffentlichen Datenleckverzeichnissen abgeglichen. Sind Sie von einem Datendiebstahl oder einer Panne betroffen, werden Sie gewarnt.
- **Zusätzliche Gerätetypen:** Während praktisch alle Anbieter PCs und Smartphones mit den gängigsten Betriebssystemen schützen, gilt dies nicht zwingend für Spielkonsolen, Smart-TVs oder Router. Achten Sie darauf, ob all Ihre Geräte im Portfolio sind.