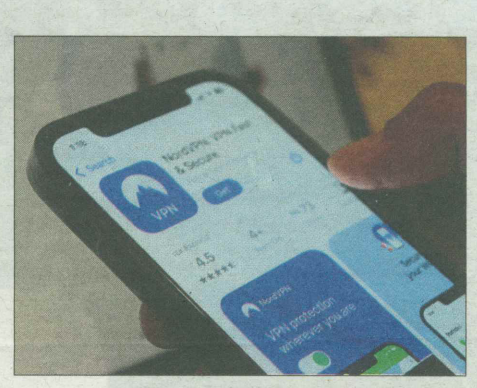
Panorama

VPN: Wie diese drei Buchstaben digitale Grenzen sprengen

Surfen ohne Spuren: VPNs versprechen digitale Freiheit. Doch wie funktioniert diese und wo bewegt man sich in rechtlichen Grauzonen? Wir haben mit einem Experten gesprochen

Von Jeff Karier



Besonders die Nutzung von etablierten, kostenpflichtigen VPNs mit Abo-Modell ist auch für Personen mit kaum technischem Wissen sehr einfach.
Foto: Shutterstock

Die Kataloge an Serien und Filme unterscheiden sich bei den Streaming-Anbietern von Land zu Land. Grund dafür sind regionale Lizenzverträge.
Foto: Shutterstock

Es ist Freitagabend, Netflix ist geladen – und ausgerechnet der Film oder die Serie, auf die man sich die ganze Woche gefreut hat, ist verschwunden. Nicht gelöscht, wohlgemerkt, sondern schlicht „in Ihrem Land nicht verfügbar". Ein Klick weiter zur ZDF-Mediathek, und wieder dasselbe Spiel: „Aus rechtlichen Gründen kann dieser Beitrag nur in Deutschland gezeigt werden."

Was wie digitale Willkür wirkt, folgt knallharten wirtschaftlichen Regeln: Lizenzverträge und Geoblocking teilen das Internet in unsichtbare Ländergrenzen auf. Netflix Frankreich zeigt andere Filme als Netflix Luxemburg, Inhalte deutscher Mediatheken bleiben zum Teil deutschen IP-Adressen vorbehalten.

Die Lösung für frustrierte Streaming-Fans trägt drei Buchstaben: VPN. Virtual Private Networks versprechen nicht nur Zugang zu global gesperrten Inhalten, sondern spielen auch bei Datenschutzbedenken und in autoritären Staaten eine wichtige Rolle. Aktuelle Debatten über Altersverifikationssysteme etwa in Großbritannien sorgen für zusätzliche Aufmerksamkeit gegenüber VPN-Anbieten. Doch was steckt wirklich hinter der Technologie, die digitale Grenzen verschwimmen lässt? Wann macht ihr Einsatz Sinn, und wo beginnt die rechtliche Grauzone?

Was ist ein VPN eigentlich?

Daten, die übers Internet verschickt werden, sind in der Regel verschlüsselt, sodass andere den Inhalt nicht lesen können. „Ähnlich wie ein Brief in einem Umschlag", erklärt Mats Brorsson, Forschungswissenschaftler am Interdisciplinary Centre for Security, Reliability and Trust (SnT) der Universität Luxemburg. „Stellen Sie sich vor, Sie wollen nicht preisgeben, wohin Ihr Brief geht oder wer ihn gesendet hat. Dann stecken Sie ihn in einen zweiten Umschlag und schicken ihn an jemanden, der ihn stellvertretend für Sie weiterleitet."

Genau so funktioniert ein VPN: Es erstellt einen virtuellen, verschlüsselten Kanal zwischen dem eigenen Gerät und einem VPN-Server. „Alle Ihre Internetaktivitäten werden zunächst an diesen Server geschickt, der sie dann an das eigentliche Ziel weiterleitet. Für Websites und Online-Dienste sieht es so aus, als würden die Anfragen vom VPN-Server kommen – nicht von Ihnen."

Verschiedene VPN-Arten – ein System

Ob kostenpflichtige Dienste wie NordVPN oder ExpressVPN oder Unternehmenslösungen wie FortiClient – im Kern funktionieren alle VPNs nach demselben Prinzip. „Sie verwenden möglicherweise unterschiedliche Protokolle für die Kommunikation zwischen Server und Client", so Brorsson, „aber alle verschlüsseln die Kommunikation und haben Authentifizierungsmechanismen."

Der Unterschied liegt hauptsächlich in der Qualität der Verschlüsselung, der Serverinfrastruktur und dem Verwendungszweck. Während Privatnutzer oft auf kommerzielle Anbieter setzen, nutzen Unternehmen spezialisierte Lösungen für den sicheren Zugriff auf interne Netzwerke.

Wie sicher sind VPNs wirklich?

Die gute Nachricht: Moderne VPN-Dienste verwenden militärtaugliche Verschlüsselung. „Die Kommunikation im Internet ist heute bereits größtenteils verschlüsselt", betont der Experte. „VPNs nutzen dieselben hochwertigen Verschlüsselungsstandards." Die Entschlüsselung würde so lange dauern, dass sie praktisch sinnlos wäre.

Allerdings gibt es einen wichtigen Punkt: Vertrauen. „Sie müssen dem VPN-Anbieter vertrauen", warnt Brorsson. Der VPN-Server kann theoretisch sehen, woher der Datenverkehr kommt und wohin er geht – auch wenn er den Inhalt aufgrund der zusätzlichen Verschlüsselung nicht lesen kann.

Kostenlos vs. kostenpflichtig

Bei der Auswahl eines VPN-Dienstes rät der Wissenschaftler eindeutig zu kostenpflichtigen Anbietern: „Ich würde kostenlosen Services nicht vertrauen. Es gibt einen berühmten Spruch: Wenn ein Service kostenlos ist, bezahlt man mit seinen Daten."

Mats Brorsson, Forschungswissenschaftler der Forschungsgruppe „Security and Trust in Service and Data Management" des SnT, welches Teil der Universität Luxemburg ist. Foto: University of Luxembourg

> *Wenn ein Service kostenlos ist, bezahlt man mit seinen Daten.*
> **Mats Brorsson, Forschungswissenschaftler**

Kostenlose VPN-Anbieter müssen irgendwie Geld verdienen – oft durch den Verkauf von Nutzerdaten oder durch Werbung. Etablierte kostenpflichtige Dienste wie ExpressVPN und NordVPN haben hingegen ein Geschäftsmodell, das auf Abonnements basiert.

Besonders solche kostenpflichtigen VPNs sind in der Regel sehr einfach zu nutzen. Zunächst lädt man sich die entsprechende App auf sein Smartphone oder Programm auf den Computer. Auch einige Smart-TVs ermöglichen die Nutzung dieser VPNs. Anschließend muss man sich nur noch anmelden beziehungsweise ein Konto erstellen.

In der App wählt man dann ein Land oder einen Server aus und verbindet sich damit. Ab diesem Moment läuft der Internetverkehr über diesen Server.

Auswirkungen auf die Geschwindigkeit

VPNs haben durchaus Auswirkungen auf die Internetgeschwindigkeit. „Alles muss einen zusätzlichen Umweg über die VPN-Server nehmen", erklärt Brorsson. Das bedeutet höhere Latenz – also längere Antwortzeiten.

Für das Streaming von Filmen oder das normale Surfen ist das meist vernachlässigbar. Nur bei Anwendungen, die sehr schnelle Reaktionszeiten benötigen, könnte der Unterschied merkbar werden. Qualitätseinbußen beim Streaming deuten meist darauf hin, dass der gewählte VPN-Server überlastet ist – ein Problem, das vor allem bei kostenlosen Anbietern auftritt.

Rechtliche Aspekte: Was ist erlaubt?

Die Nutzung von VPNs ist in der EU und Luxemburg grundsätzlich legal. „Alles, was ohne VPN illegal ist, bleibt auch mit VPN illegal", stellt Brorsson klar. „VPNs selbst machen nichts illegal."

Lediglich in autoritären Ländern wie China, Russland oder Iran wird die VPN-Nutzung eingeschränkt, ist untersagt oder es sind nur staatlich genehmigte Anbieter zugelassen. Immerhin findet in solchen Ländern oft eine Überwachung der Internetaktivitäten statt. Durch VPNs entziehen sich jedoch Nutzer dieser Kontrolle, zum Missfallen der Machthaber. So werden VPNs etwa gerne von Oppositionellen oder auch Journalisten genutzt. Um sich selbst zu schützen.

Ein häufiger Anwendungsfall ist das Umgehen von Geoblocking, der geografischen Sperren bei Streaming-Diensten. Netflix und andere Streaming-Dienste versuchen aktiv, VPN-Nutzer zu erkennen und zu blockieren. Sie setzen dabei verschiedene technische Maßnahmen ein, um gegen die Nutzung von VPNs vorzugehen.

Sie erkennen und blockieren bekannte VPN-Server anhand ihrer IP-Adressen. Zusätzlich kommen Methoden wie „deep packet inspection" zum Einsatz, um den verschlüsselten VPN-Traffic zu identifizieren und herauszufiltern. Trotz dieser Maßnahmen reagieren VPN-Anbieter sehr schnell: Sie tauschen gesperrte IPs aus, entwickeln Tarntechnologien, die VPN-Verkehr wie normalen Internet-Traffic aussehen lassen, und bieten spezielle, unauffällige Streaming-Server an. Das führt zu einem ständigen Katz-und-Maus-Spiel zwischen den Diensten und den VPN-Betreibern.

Wie Brorsson hervorhebt, verstoße man mit der Nutzung von VPNs zum Umgehen von Geoblocking möglicherweise gegen die Nutzungsbedingungen der Anbieter. Dies sei aber nicht strafbar. Fälle, bei denen Nutzerkonten wegen der Nutzung von VPNs gesperrt würden, scheine es bislang nicht oder nur äußerst selten zu geben.

Wann und für wen lohnt sich ein VPN?

VPNs sind ein nützliches Werkzeug für mehr Privatsphäre und Sicherheit im Internet, aber nicht für jeden Nutzer in jeder Situation notwendig. Sie bieten zusätzlichen Schutz vor neugierigen Blicken, autoritären Kräften und Ermöglichen den Zugriff auf eine Vielzahl an weiteren Inhalten.

Mit der zunehmenden Digitalisierung und neuen Regulierungsbestrebungen könnten VPNs in Zukunft noch relevanter werden – als Werkzeug für digitale Selbstbestimmung und Privatsphäre im Netz.