

Was ein VPN wirklich ist

Es ändert, wer dich sehen kann, nicht ob es jemand kann.

Einfach erklärt: Ein VPN verhindert, dass dein Internetanbieter oder ein Flughafen-WLAN sieht, wohin du dich verbindest. Diese Information verschwindet jedoch nicht, sondern geht an den VPN-Anbieter, der sie nun sieht. Was ohnehin verschlüsselt war, wie E-Mails oder Online-Banking, war es auch vorher schon. Es dient wenigen konkreten Zwecken, wird aber oft so verkauft, als leiste es weit mehr.

Jahrelang hörte ich von VPNs und schenkte ihnen keine Beachtung, genau wie bei Antivirenprogrammen: Ich nutze kein Antivirenprogramm oder so gut wie nie. Ich habe Echtzeitkopien von allem an drei Orten und passe genau auf, was ich herunterlade, welche Links ich anklicke und welche Websites ich besuche. Das ist keine hundertprozentige Sicherheit, aber für mich funktioniert es. Eines Tages sah ich ein VPN-Angebot für etwas mehr als zwei Euro im Monat und schloss es aus Neugier ab. Es funktioniert gut, hat mir aber wenig genützt: etwa um einen Dienst auszuprobieren, der damals nur in den USA verfügbar war. Fühle ich mich sicherer? Nein. Wenn man es mir wieder zu diesem Preis anbietet, verlängere ich vielleicht; wenn nicht, dann nicht. Es ist nur meine Erfahrung, sie beweist nichts. Also fragte ich mich, was ein VPN genau tut. So habe ich es verstanden.

Stell dir vor, du wirfst einen Brief mit deutlich lesbarer Empfängeradresse in den Briefkasten. Der Postbote sieht, an wen du ihn schickst, auch wenn er ihn verschlossen nicht lesen kann. Dieser Postbote ist dein Internetanbieter. Ein VPN steckt deinen Brief in einen zweiten Umschlag, adressiert an einen Zwischenhändler, der ihn öffnet und weitersendet. Dein gewohnter Postbote sieht die eigentliche Adresse nicht mehr. Er sieht nur, dass du diesem Zwischenhändler schreibst.

Wer das Netzwerk kontrolliert, über das du dich verbindest – etwa ein Flughafen-WLAN –, sieht nicht mehr, wohin du surfst. Doch der Zwischenhändler sieht nun das, was zuvor dein Anbieter sah, und manchmal mehr, da dein gesamter Datenverkehr über ihn läuft. Die Überwachung verschwindet nicht: Sie wechselt die Hände. Daher der Name.

Zudem läuft heute fast alles, was du tust – wie E-Mails abrufen oder Online-Banking –, dank des Browser-Schlusses ohnehin verschlüsselt bis zum Zielserver. Das geschieht mit und ohne VPN. Ein VPN fügt nur auf dem ersten Teilstück Schutz hinzu, bis zu seinem eigenen Server. Ab dort verläuft der Weg wie gewohnt.

Deshalb gibt es Dinge, die es dir nicht versprechen kann, auch wenn es manchmal so beworben wird. Wenn du dich bei deinem E-Mail-Dienst oder deiner Bank angemeldet hast, weiß dieser Dienst, dass du es bist – mit oder ohne VPN. Es garantiert auch nicht, dass niemand deinen Datenverkehr einsieht: Es ändert nur, wer hinschaut. Wenn ein Unternehmen erklärt, es «führe keine Protokolle», ist das ein Versprechen, genauso wie wenn ein großer Konzern sagt: «Deine Nachrichten sind verschlüsselt, wir lesen sie nicht». Ein Audit kann das zu einem bestimmten Zeitpunkt bestätigen, bleibt aber etwas, auf dessen Einhaltung du vertrauen musst – keine Unmöglichkeit durch Architektur.

Und der Inhalt eines Gesprächs bleibt unverändert. Wenn deine Messaging-App bereits Ende-zu-Ende verschlüsselt, fügt ein VPN nichts hinzu. Tut sie das nicht, behebt ein VPN das auch nicht: Es schützt den Übertragungsweg, nicht das, was die App oder ihr Server nach dem Eintreffen damit tun.

Nichts davon macht es nutzlos. Zu verbergen, wohin du dich verbindest – vor einem öffentlichen WLAN, einem Anbieter, der diesen Verlauf verkaufen möchte, oder einem Staat, der einen Dienst blockiert –, ist eine reale Aufgabe, und das erledigt es gut. Das Marketing verspricht allerdings meist mehr, als diese Schicht leisten kann.

Die Frage, die man sich bei einem VPN oder jedem Dienst stellen sollte, der Schutz verspricht, lautet nicht «Ist es verschlüsselt?». Wahrscheinlich ja, zumindest auf einer Teilstrecke. Sie lautet: Wem schenke ich das Vertrauen, das ich einem anderen entzogen habe? Und was bleibt mir, falls es sich als unberechtigt erweist?

Ein VPN ändert, wenn es seine Arbeit gut macht, nur den Zwischenhändler deiner Verbindung. Eine App wie Solo2, deren Nachrichten über keinen Server laufen, nimmt den Zwischenhändler ganz aus dem Gespräch. Sie konkurrieren nicht: Sie lösen unterschiedliche Probleme.

Sie zu verwechseln ist ein weit verbreiteter Weg, sich geschützter zu wiegen, als man tatsächlich ist.

Anmerkung der Redaktion: Wenn diese Cuadernos Unternehmen oder Produkte nennen, geschieht dies nicht, um sie anzuklagen. Diejenigen, die sie entwickeln, leisten Arbeit, die Millionen von Menschen nutzen und schätzen. Was wir aufzeigen, ist struktureller Natur — das Modell, nicht die Marke. Marken erscheinen als Beispiele, weil der Leser sie erkennt.

Quellen und weiterführende Literatur

- Das HTTPS-Protokoll und die Transportverschlüsselung sind offene Standards, öffentlich dokumentiert von der IETF.
- In dieser Reihe beleuchten «Wenn niemand dazwischen ist» und «Du bist nicht anonym» aus anderen Blickwinkeln dieselbe Unterscheidung zwischen Struktur und Versprechen.

[← Zurück Du bist nicht anonym](#)

Aktuelle Lektüre

- [Reflexion · 29. Juni 2026 Du bist nicht anonym](#)
- [Reflexion · 27. Mai 2026 Was eine Unterschrift nicht in Ordnung bringen kann](#)
- [Analyse · 26. Mai 2026 Echte vs. scheinbare Privatsphäre: Die Fragen, die man sich stellen sollte](#)

Nimm diesen Artikel mit, wohin du ihn brauchst.

[↓ Markdown](#) [↓ Klartext](#) [↓ PDF](#)

Die Datei wird auf dein Gerät heruntergeladen. Von dort aus kannst du sie speichern, in Solo2 importieren oder teilen, wo immer du möchtest. Cuadernos entscheidet nicht über den Zielort für dich.

Siegellack-Siegel · SHA-256 2e9d93de70b4dd5f25b0b2ede8f03d02bd3ba950d2857d65b7e1be3421cbc75a
[Funktionen](#) [Preise](#) [Installieren](#) [Neuigkeiten](#) [Blog](#) [Pro](#) [Hilfe](#) [Über uns](#) [Kontakt](#)
[Transparenz](#) [Verifikation](#) [Datenschutz](#) [AGB](#) [Cookies](#)

Cuadernos Lacre · Eine Publikation von [Menzuri Gestión S.L.](#) ·
geschrieben von R.Eugenio · herausgegeben vom Team von [Solo2](#).

Diese Website verwendet keine Cookies. Alles, was dein Browser lädt, ist von uns geschrieben oder überwacht und auf unseren europäischen Servern gehostet: das anonyme Besuchsanalysetool (Umami, selbst gehostet) und das Minimum an JavaScript, das für die Sprachauswahl und deine Einstellung für helles/dunkles Design erforderlich ist, die auf deinem eigenen Gerät gespeichert wird. Keine Ressourcen von Drittanbietern, keine Tracker, kein Profiling, keine Datenweitergabe. Wenn du uns folgen möchtest: [RSS](#).