VPN-Überblick: Standorte vernetzen, Geoblocking und Zensur umgehen, Privatsphäre schützen

Verschlüsselte Wendungen

Virtual Private Networks gibt es heute für deutlich mehr Zwecke, als der Name vermuten lässt. In diesem Streifzug lesen Sie, wie diese vielfältige Softwaregattung entstand und dass sie neben soliden Ökosystemen auch sumpfige hervorbrachte. Außerdem geht es um Praxis zu einem mächtigen Mauerblümchen.
Virtual Private Networks gibt es heute für deutlich mehr Zwecke, als der Name vermuten lässt. In diesem Streifzug lesen Sie, wie diese vielfältige Softwaregattung entstand und dass sie neben soliden Ökosystemen auch sumpfige hervorbrachte. Außerdem geht es um Praxis zu einem mächtigen Mauerblümchen.

Von Dušan Živadinović

kompakt

- Viele VPN-Anwendungen haben den spröden Charm der Kommandozeile abgelegt und lassen sich komfortabel bedienen.
- Manche neuen VPN-Funktionen spiegeln gut wider, dass Anwendern der freie Internet-Zugang wichtig ist.
- Für den Privatsphärenschutz setzen Entwickler Techniken ein, die sich bei digitalen Wahlmaschinen bewährt haben.

Ursprünglich hat man Virtual Private Networks (VPN) entwickelt, um entfernte Standorte miteinander zu vernetzen (Site-to-Site), später auch, um ferne Benutzer an Firmen- oder Heimnetze anzukoppeln (Road-Warrior, auch End-to-Site-VPNs genannt), und für diverse andere Zwecke. Zu den wichtigsten davon gehören VPN-Varianten für das Anonymisieren und das Umgehen von Geoblocking und Internet-Sperren (Tor) sowie den Privatsphärenschutz.

Mit Virtual Private Networks waren anfangs nur Routing- und Bridging-Programme zur Standortvernetzung gemeint. Zu Beginn der Internet-Ära koppelte man entfernte Netze sogar noch ohne jeglichen Kryptoschutz. Das änderte sich, nachdem klar wurde, dass über solche Verbindungen auch Daten fließen, die besser vertraulich bleiben.

Fortan blieb die Wahrung der Vertraulichkeit eine der wichtigsten Antriebsfedern und brachte immer neue kryptografische Absicherungen der Nutzdaten gegen unerwünschte Mitleser hervor. Unzureichend gehärtete VPN-Varianten, die ihre vertrauliche Fracht nicht vor Angreifern schützen konnten, verschwanden wieder von der Bildfläche. Ein Beispiel ist das von Microsoft entwickelte Point-to-Point Tunneling Protocol (PPTP), das zwar sehr einfach zu konfigurieren war, sich aber mit überschaubarem Aufwand knacken ließ (siehe ct.de/y9y1). PPTP hat in modernen Installationen nichts zu suchen.

Neben PPTP kamen diverse Spielarten von SSL-VPNs auf und erlangten große Verbreitung. Sie verschlüsseln Nutzdaten mittels Transport Layer Security (früher Secure Socket Layer, SSL, genannt). Bis heute sehr verbreitet sind Implementierungen, die ohne Clientsoftware funktionieren, weil sie sich besonders für den spontanen Aufbau gesicherter Verbindungen eignen (Tunnel), also etwa zwischen Webbrowsern und Webservern. Viele tunneln aber nur den Verkehr bestimmter Anwendungen (z. B. Mailclient und -server, verschlüsselnde DNS-Clients und -Resolver), bieten also keine Infrastrukturvernetzung etwa für Dateifreigaben, weshalb ihre Einordnung zu VPNs umstritten ist.

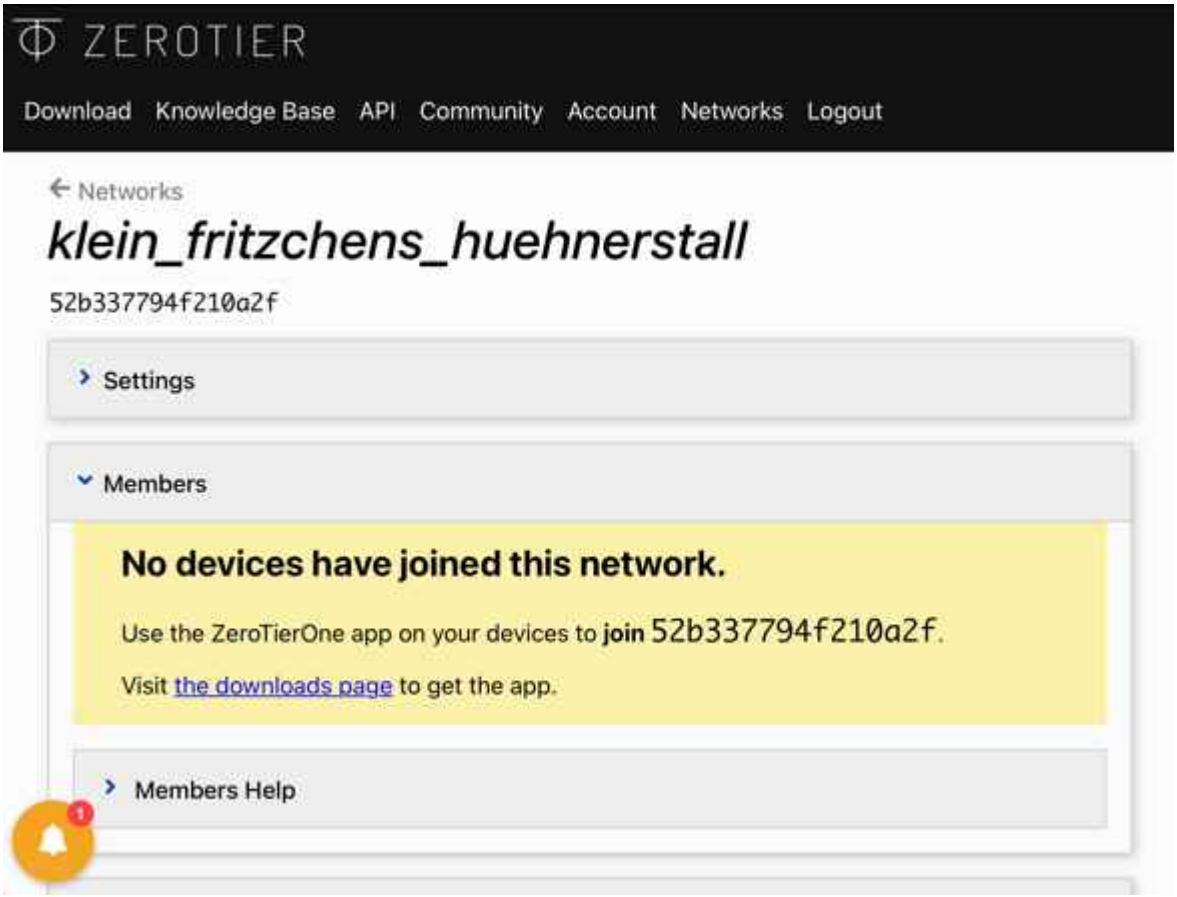
Die bekannteste SSL-VPN-Spielart inklusive Netzwerkzugriff, also mit Kapseln kompletter IP-Pakete, ist bis heute das quelloffene OpenVPN. Jahrelang galt es als das am weitesten verbreitete VPN überhaupt. Daneben gibt es diverse weniger bedeutende SSL-VPNs etwa von Router-Herstellern wie Netgear. Neben OpenVPN galten lange Zeit nur das komplizierte, aber bis heute sichere IPsec und Varianten wie IPsec/L2TP als zuverlässige Alternative zur Netzwerkkopplung.

Auf der Beliebtheitsskala rangiert vor OpenVPN inzwischen das 2019 erschienene, ebenfalls quelloffene WireGuard, das auch schneller ist als OpenVPN & Co. Anders als OpenVPN und andere VPN-Verfahren klammert WireGuard die Benutzerverwaltung komplett aus und regelt nur die Vernetzung und das Chiffrieren von Nutzdaten mittels kryptografischer Schlüsselpaare. Wer sich für Implementierungsdetails interessiert, findet bei der Internet Engineering Task Force (IETF) eine Zusammenfassung für gängige VPNs, darunter TLS, IPsec und WireGuard (ct.de/y9y1). Beispiele für interessante, aber wenig verbreitete VPN-Varianten sind Nebula, SoftEther, Tinc, Twingate oder auch tinyfecVPN (dank spezieller Fehlerkorrektur empfehlenswert für gestörte Leitungen).

Netzwerkkopplung mit Komfort

Wer einfach nur von unterwegs auf einen Server im Heimnetz zugreifen will, den stellen die üblichen VPN-Anwendungen vor zu hohe Hürden. An diesem Punkt kommen VPN-Dienste ins Spiel, die man mittels vereinfachter Programme im Handumdrehen verwenden kann. Zu den ersten Vertretern gehört das kostenpflichtige LogMeIn Hamachi, das sich nach dem Start über die Firewall des Heimrouters hinweg bei der Infrastruktur des Anbieters anmeldet. Anschließend können Hamachi-Clients laut dem Hersteller direkt miteinander kommunizieren (automatisches NAT-Traversal), also ohne den Umweg über Hamachi-Server. Bisher hat der Hersteller den Quellcode aber nicht veröffentlicht, sodass man weder die Sicherheit noch die Funktionsweise prüfen kann.

Zu den komfortablen, aber quelloffenen und geprüften VPNs gehören der WireGuard-Abkömmling Tailscale und ZeroTier. Mit ZeroTier verknüpft man Netzwerkgeräte über einen virtuellen Managed Switch, den ZeroTier anbietet (den man mit Abstrichen aber auch selbst betreiben kann) und der einfach per Web-Interface konfiguriert wird.



Als ZeroTier-Admin koppelt man PCs oder Smartphones innerhalb von Minuten in ein virtuelles Netzwerk. Wer den Dienst ausprobieren möchte, kann gratis eine Handvoll Netzwerke aufsetzen und Clients nach Belieben hinzufügen und entfernen. Fortgeschrittene können ZeroTier-Gateways einrichten, die zwischen einem virtuellen Netz und einem physischen vermitteln.

Auf Linux, macOS, Windows, Android und iOS klappt das Einrichten mit geringem Aufwand, für den Verbindungsaufbau der Clients muss der UDP-Port 9993 geöffnet sein (alternativ UPnP für die beteiligten Hosts im Router einschalten). Das Web-Interface bietet zahlreiche Optionen, die sich an fortgeschrittene Admins richten. Beispielsweise kann man Subnetze beinahe nach Belieben wählen, öffentliche oder private Netze bilden, Netzwerkteilnehmern mehr als eine IP-Adresse und spezielle DNS-Resolver zuweisen oder Clients per Hand aus dem Netz kicken. ZeroTier ist quelloffen und von Fachleuten geprüft und für sicher befunden.

Stille VPNs

VPN-Funktionen verstecken sich manchmal an ungewöhnlichen Stellen. Das ist beispielsweise der Fall bei hybriden Internet-Anschlüssen. Dabei fasst ein Router im Zusammenspiel mit einem Hub im Rechenzentrum per VPN mehrere Internet-Leitungen zu einem Bündel zusammen, was die summierte Datenrate erhöht und die Ausfallsicherheit verbessert. Die Deutsche Telekom bietet solche Anschlüsse unter dem Namen „Magenta zu Hause Hybrid“ an. Dabei wird je ein DSL- und ein Mobilfunk-Zugang gebündelt. Der Router-Hersteller Viprinet bündelt beliebige Internet-Zugänge, ob DSL, Glasfaser, Kabel oder Mobilfunk.

Eine berüchtigte Gruppe unter den VPN-Anwendungen bilden Programme für das Peer-to-Peer-File-Sharing. Dabei versteckt die Sicherungsschicht die Nutzdaten. Manche Anwender verbreiten über diese Softwareklasse, die Napster begründet hat, illegal Medien und Programme. Das Piraten-Image haftet zwar weiter an, aber über Anwendungen wie BitTorrent werden etwa Linux-Distributionen weltweit kostengünstig verteilt und Unternehmen wie Microsoft nutzen die Technik, um Updates oder Spiele-Elemente zu verbreiten (z. B. beim Online-Rollenspiel Skyforge).

Umgehung per Tunnel

Mit Aufkommen der Videostreamingangebote teilten vor allem US-amerikanische Medienhäuser den Weltmarkt in Regionen auf, um ihre Kommerzialisierungsideen durchzusetzen. Dafür werten deren Server den Standort der Nutzer aus: Wer aus einem noch nicht bedienten Gebiet anfragt, bekommt nichts zu sehen (Geoblocking). Filterkriterien sind beispielsweise die IP-Adressen der Nutzer und der Standort des befragten DNS-Resolvers, der den Anwendern beim Verbindungsaufbau die IP-Adresse der Streamingserver mitteilt. So bleiben etwa die Tore von HBO geschlossen, wenn man sich aus Europa anmeldet.

Mit VPN-Anwendungen täuscht man legitime Standorte vor, indem man den fernen Tunnelendpunkt in ein Land legt, das der Streaminganbieter versorgen will, also etwa in die USA. Ein derartiges VPN kann man mit etwas Know-how selbst basteln, indem man den VPN-Server in einer Cloud installiert, vorausgesetzt, man kann dessen Standort wählen. Solche Angebote kosten bei Amazon oder DigitalOcean monatlich wenige Euro. Zusätzlich muss das Betriebssystem des Nutzers einen Resolver aus dem Zielland befragen, sodass man auch diesen auf dem Cloudserver einrichtet oder einen offenen Resolver ausfindig macht, der im Zielland steht.

Privatsphärenschutz

Für jedes ferne Tunnelende braucht man aber einen separaten Server, sodass es schnell teuer wird, wenn man mehrere Endpunkte braucht. Deshalb, und auch weil die VPN-Konfiguration nicht jedermanns Sache ist, kamen vor einigen Jahren VPN-Anbieter auf den Markt, die genau dieses Anwendungsfeld mit eigenen Clients abdecken. Darüber kann man vor jedem Verbindungsaufbau einen von meist vielen Tunnelendpunkten per Menü auswählen.

Zusätzlich versprechen die Diensteanbieter, die Privatsphäre zu schützen, denn ohne VPN können Angreifer oder Spione Metadaten wie Ziel-Domains, Quell- und Ziel-IP-Adressen und unverschlüsselten Verkehr zum Beispiel an WLAN-Hotspots abfischen. Staatliche Sicherheitsorgane können solche Daten auch an Internet-Austauschknoten abgreifen.

Ein VPN schützt die Meta- und Nutzdaten kryptografisch, solange die Daten vom Nutzer zum Tunnelendpunkt unterwegs sind. Die VPN-Clients leiten daher sämtlichen Verkehr über den Tunnel zum VPN-Anbieter, der sie mit seiner eigenen Quell-IP-Adresse zum Ziel ins Internet gibt. Außerhalb des Tunnels erscheint nur die IP-Adresse des VPN-Anbieters. Deshalb lassen sich viele Metadaten nicht mehr korrekt zuordnen, weshalb sie für Angreifer und fremde Sicherheitsorgane wertlos sind.

Das gilt aber nicht für den Betreiber des VPNs, denn er kann den austretenden Verkehr den Nutzern prinzipiell anhand von Tunnel-IDs zuordnen. Deshalb erfordert es großes Vertrauen, ein VPN-Angebot zu buchen. Viele kommerzielle VPN-Anbieter sichern in den AGB zu, die Benutzeraktivitäten nicht zu protokollieren. Aber Kunden können das nicht prüfen. Tatsächlich deutet einiges darauf hin, dass manche Anbieter nur vorgeben, die Privatsphäre zu schützen, sie aber eigentlich sogar aushöhlen.

Sumpfiges Ökosystem

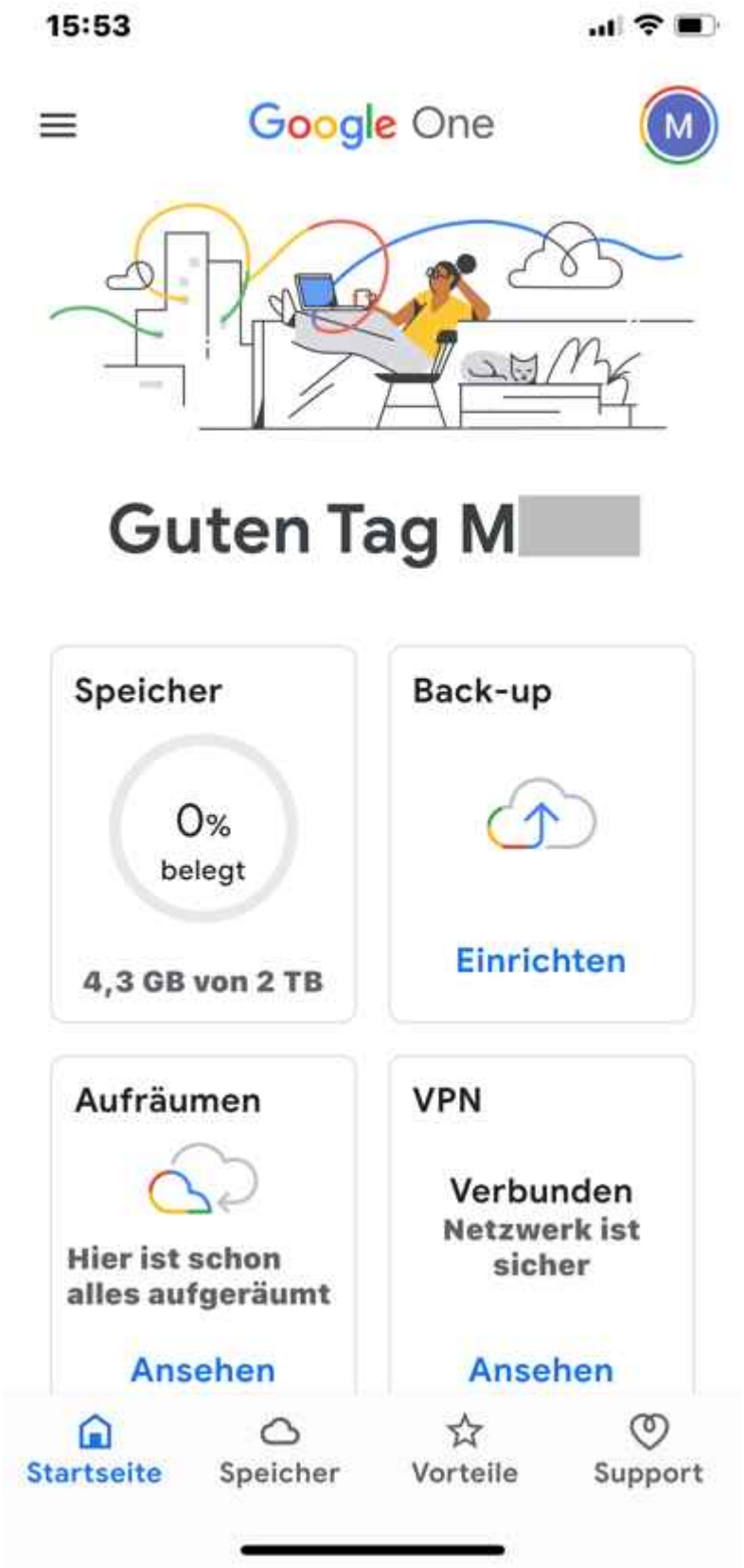
Beispielsweise deckte die Technologieforscherin und Redakteurin Katie Kasunic bereits im Juni 2020 auf, dass 40 VPN-Anbieter nach außen vorgeben, miteinander zu konkurrieren, tatsächlich aber der Kontrolle von nur sieben Unternehmen in Pakistan und China unterstehen. Beispielsweise kontrollierte zum Prüfzeitpunkt die in Singapur ansässige Firma Innovative Connecting insgesamt acht VPN-Anwendungen für Mobilgeräte, deren in China stationiertes Team entwickelte manche der Apps selbst und kontrollierte andere über stillschweigend aufgekaufte Tochterfirmen.

Solche Verflechtungen wecken Zweifel an der Vertrauenswürdigkeit von VPN-Anbietern. Auch erinnern die Firmenkonglomerate daran, dass in China vor einigen Jahren ungewöhnlich viele Tor-Exit-Punkte stationiert wurden. Das weckt den Verdacht, dass der oder die Betreiber am VPN- und Tor-Verkehr interessiert sind. Ein Exit-Node kann mitlesen und weiß lediglich nicht, wer die Daten anfordert. Es ist aber sichtbar, ob Tor-Nutzer zum Beispiel Webseiten abrufen, die einem autoritären Regime unliebsam sind. Auch der Opera-Browser, den manche Nutzer wegen seines eingebauten VPN-Verfahrens schätzen, segelt unter einer fragwürdigen Flagge: Dahinter steht ein Konsortium namens Golden Brick Silk Road Equity Investment Fund, das neben seinem Hauptsitz in China ein Büro in Russland unterhält.

Anscheinend haben also manche restriktiven Regierungen den Spieß umgedreht und nutzen VPNs offensiv zum Bespitzeln ihrer Nutzer. Dabei finanzieren die Bespitzelten durch den Kauf ihre Überwachung unwissentlich selbst.

Großer Entflechtungstrick

Unabhängig von ihrer Redlichkeit haben VPN-Anbieter ein strukturelles Problem: Kundendatenbanken und Verkehrsprotokolle können leicht miteinander verknüpft werden, um auszukundschaften, welche Ziele die VPN-Nutzer im Internet ansteuern. Selbst wenn ein Anbieter keine Log-Funktion eingerichtet hat, könnte er auf staatliche Weisung dazu gezwungen werden, womit die Privatsphäre der User perdu wäre.



Google hat eine eigene VPN-Anwendung für den Privatsphärenschutz entwickelt. Kundendaten und Kundenverkehr sind mittels moderner Kryptografietechniken entflochten.

An dieser Stelle greifen neue Angebote von Apple und Google. Beide entflechten die Authentifizierung der Anwender von den

Verkehrsdaten, sodass sich Benutzernamen und Einwahlzeitpunkte nicht mit IP-Adressen und durchgeleitetem VPN-Verkehr verknüpfen lassen. Dafür setzen beide Konzerne auf RSA Blind Signatures.

Die Technik erlangte in digitalen Wahlmaschinen einige Bekanntheit, weil sich damit digitale Wahlzettel so beglaubigen lassen, dass man die Inhalte keinem Wähler zuordnen kann. Eine Variante der Methode spezifizieren Apple, Cloudflare und Fastly unter dem Dach der Internet Engineering Task Force (siehe ct.de/y9y1).

Google verwendet RSA Blind Signatures beim kostenpflichtigen Dienst „Google One“. Der ist ab monatlich 10 Euro für macOS-, Windows-, Android- und iOS-Clients erhältlich; mit aktuellen Geräten der Pixel-7-Reihe soll der Dienst ab Dezember kostenlos sein. Der Client lenkt den gesamten Verkehr des Smartphones automatisch zum nächstgelegenen Tunnelendpunkt von Google, eignet sich also nicht zur Umgehung von Geoblocking.

Netzwerkverkehr einschließlich DNS, IP-Adressen und Verbindungszeiten werden Google zufolge nicht protokolliert, was den Dienst attraktiv erscheinen lässt. Wie bei anderen VPNs können auch hier Dritte im Datenstrom schnüffeln, sobald er den Tunnel verlassen hat, sodass man darauf achten muss, keine unverschlüsselten Anwendungen zu verwenden.

Die VPN-Varianten für Windows und macOS sind noch sehr frisch. Auf Android und iOS haben wir den Dienst ausgiebig getestet und dabei fielen nur wenige Fehlversuche auf. Der VPN-Client baut den Tunnel (vermutlich für Stromsparzwecke) häufig ab und bei Bedarf wieder auf und meldet jeden Statuswechsel. Wer das lästig findet, kann das Meldungsfeuer abschalten. Doch ob Sie ausgerechnet der Datenkrake Google auch noch fürs VPN vertrauen sollten, sei dahingestellt.

Apples Privatsphärenschutz Private Relay gibt es als Dreingabe zu einem iCloud+-Abo ab 0,99 Euro monatlich. Der Dienst setzt

iOS, iPadOS oder macOS voraus, ist aber ab Werk löchrig: Apple schützt mit Private Relay nicht den gesamten Verkehr des Nutzers, sondern nur den der eigenen Internet-Anwendungen. Dazu gehören DNS-Anfragen und der Verkehr des Safari-Browsers. Statt eines herkömmlichen VPN-Tunnels setzt Apple zwei verkettete Proxies ein (Multi-hop Masque proxy), die unterschiedlichen Betreibern gehören.

Der erste Proxy bekommt verschlüsselte Pakete und weiß daher nicht, welche Domain der Client ansteuern will. Nur der zweite kann sie entschlüsseln und leitet sie zum Ziel weiter, aber er weiß nicht, von welcher Quell-IP-Adresse die Pakete stammen. Deshalb weiß auch ein Webseiten-Betreiber nicht, welche IP-Adresse ein Besucher tatsächlich nutzt. Den ersten Proxy betreibt Apple selbst. Der zweite stammt aus einem Pool, den die CDN-Anbieter Akamai, Cloudflare und Fastly beisteuern. Aus diesem Pool stammen die IP-Adressen, die beim Surfen im Internet sichtbar werden (Test via ct.de/ip). Schaltet man einen VPN-Dienst ein, endet die Umleitung über die Proxies und der Verkehr läuft über den neuen Tunnel.

Wenn Private Relay eine DNS-Anfrage nicht auflösen kann, delegiert es die Aufgabe an den im Betriebssystem konfigurierten Resolver. Auf speziell konstruierten Webseiten wie astrill.com/dns-leak-test sickert so die IP-Adresse des Resolvers durch. Falls das einer ist, der auf Ihren Aufenthaltsort schließen lässt (etwa, weil sie zu Hause einen eigenen betreiben), richten Sie besser den anonymisierenden DNSCrypt-Proxy auf dem Mac ein (siehe ct.de/y46t); der ist auch für Windows und Linux empfehlenswert.

Trotz der Proxy-Kette wirkte Apples Dienst im Test schnell, Verzögerungen im Webseitenaufbau fielen gegenüber dem Betrieb ohne Private Relay nicht auf. Das dürfte daran liegen, dass die Proxies in CDNs stehen, die ohnehin viele nachgefragte Inhalte ausliefern. Im rund sechsmonatigem Test fiel Private Relay nur wenige Male aus und das auch nur vorübergehend. Einige wenige Webseiten, darunter HUK24.de, haben die Proxy-

IP-Adressen fälschlich dem europäischen Ausland zugeordnet und die Anmeldung abgelehnt. Nach Rückmeldungen der Nutzer beseitigten sie das Problem.

Verschleiernde VPNs

Große Firewalls können Datenpakete von gängigen VPNs einschließlich Google One leicht identifizieren und sperren. Auf dieser Grundlage setzen manche Staaten Internet-Zensur durch. Dem stellt eine große Entwicklergruppe das Tor-VPN entgegen. Es verschlüsselt und anonymisiert den Datenverkehr und verschleiert den VPN-Charakter, sodass die Datenpakete beispielsweise wie harmloser HTTP-Verkehr aussehen.

Tor ist hinlänglich bekannt und auch über dessen Snowflake-Erweiterung für Browser, die Tor-Clients zum Weg ins unzensierte Internet verhilft, haben wir berichtet (ct.de/y9y1). Aber da die Datenpakete über mehrere Vermittler ins Internet gelangen, sind sie viel länger unterwegs. Die Tor-Vermittler und der Endpunkt werden zufällig ausgewählt, sodass sich kaum rückverfolgen lässt, von wem eine Internet-Sitzung gestartet wurde. Aber manche restriktiven Regierungen betreiben eigene Tor-Endpunkte und können so mitlesen, welche Seiten im Web aufgerufen werden und Tor-Verkehr manipulieren.

An dieser Stelle kommt das VPN-Mauerblümchen Shadowsocks ins Spiel, das mutmaßlich einer Tastatur in China entstammt. Nachdem der Entwickler 2015 die Arbeit daran aufgeben musste, führten das Projekt andere fort und entwickelten Varianten. Unter diesen sticht das von Googles Jigsaw-Gruppe geführte Projekt Outline hervor. Shadowsocks und Outline standen jahrelang im Schatten von Tor, rückten aber kürzlich durch Netzsperren im Iran in den Blickpunkt.

Shadowsocks

Mit Shadowsocks kann man den Tunnelendpunkt selbst bestimmen, also sicherstellen, dass man keinen unerwünschten Tor-Endpunkt

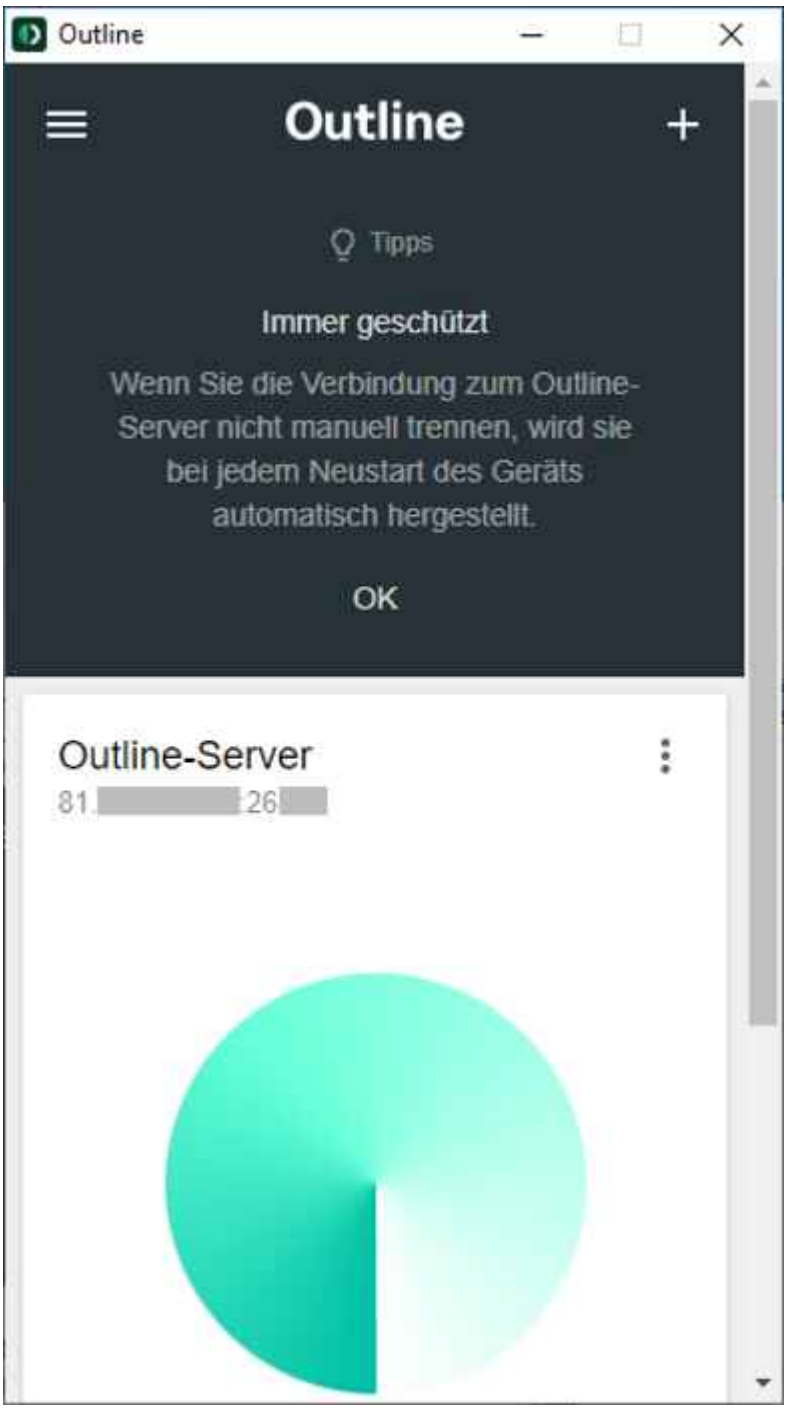
nutzt. Das scheint zwar die Anonymisierung auszuhebeln, weil man für den Server-Betrieb Cloud-Instanzen etwa bei Hetzner anmietet und dabei natürlich Personalien hinterlässt.

Aber manche Betreiber stellen ihre Shadowsocks-Server Nutzern aus dem Iran oder China auf Zuruf incognito und gratis zur Verfügung. Um dann unzensiert zu surfen, braucht man nur den Shadowsocks-Client und den zum Server passenden Schlüssel, der keinen Bezug zum Nutzer hat. Server lassen sich so konfigurieren, dass sie für alle Nutzer denselben Zugangsschlüssel verwenden. Unterm Strich können Betreiber selbst dann die Identität der Anwender nicht preisgeben, wenn ihr Server in fremde Hände fällt.

Mit Shadowsocks verbindet sich ein Client mit einem fernen SOCKS5-Proxy. Die Technik ähnelt dem Ansatz von SSH-Tunneln und wird auch bei Tor genutzt. Ist die Verbindung aufgebaut, leitet der Proxy den zu ihm gelangenden TCP- und UDP-Verkehr ins Internet.

Im Outline-Pelz

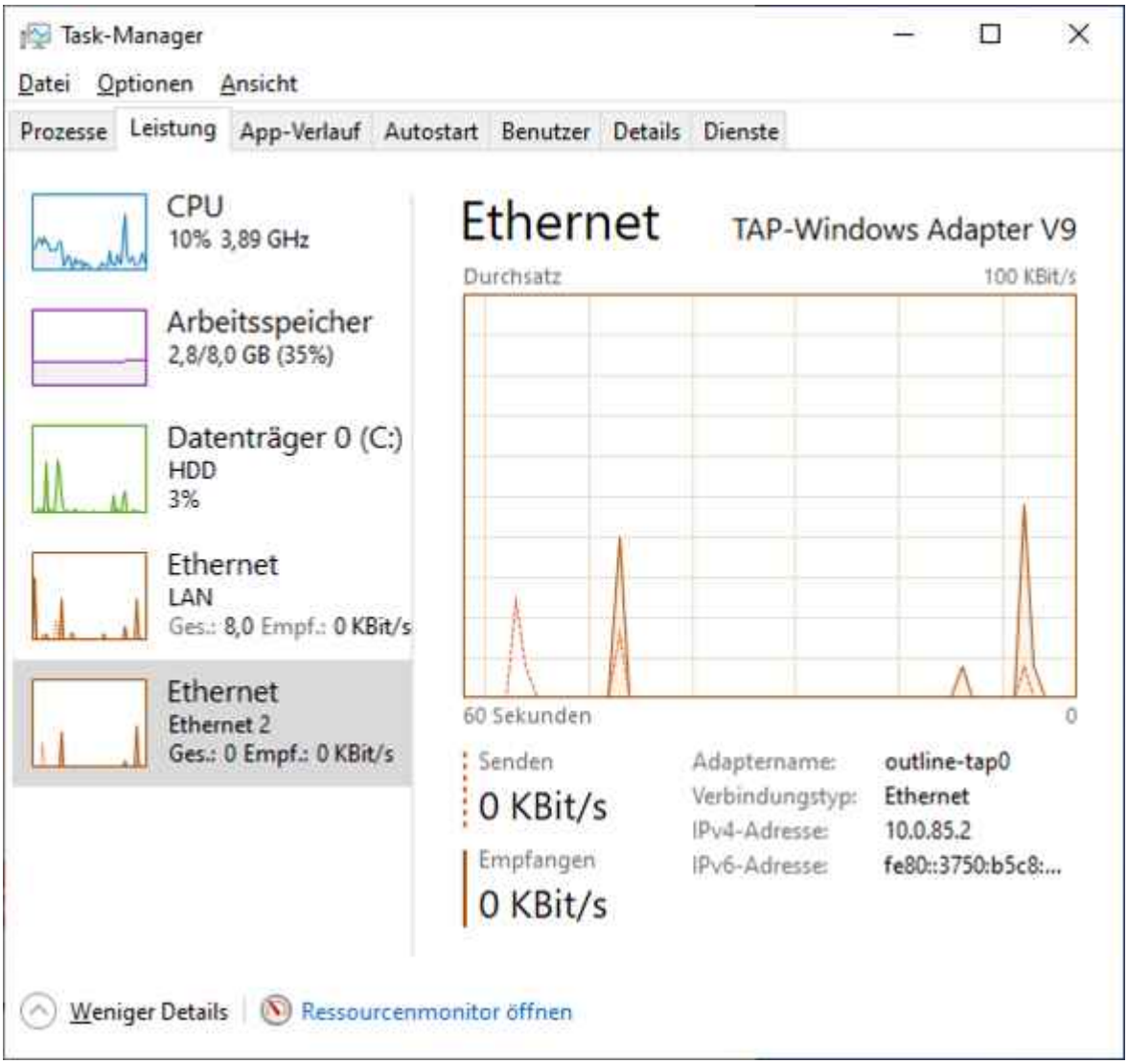
Die Jigsaw-Entwickler haben um Shadowsocks herum unter dem Namen Outline drei Anwendungen mit sehr übersichtlichen grafischen Oberflächen gebaut: Client, Server und Server-Manager. Alle drei sind für Linux, macOS und Windows erhältlich, die Clients auch für Android und iOS.



Von Googles Entwicklergruppe Jigsaw stammt auch die Shadowsocks-Variante Outline. Beide, Shadowsocks und Outline, verschleiern die Nutzdaten, um Firewallsperren zu entgehen.
Den Server installiert man mit dem Outline Manager typischerweise auf Cloud-Instanzen innerhalb von Minuten. Drei vereinfachte Installationen für DigitalOcean, Google und Amazon LightSail bietet der Manager gleich auf seiner Startseite an. Aber für das Einrichten auf anderen Linux-Servern oder im Firmennetz braucht man ebenso wenig Vorkenntnisse, denn die Installationsskripte erledigen den Großteil selbst.

Die Jigsaw-Entwickler bieten Outline hauptsächlich für Nachrichtenagenturen und Journalisten an, die aus Ländern mit Internet-Sperren berichten. Outline ist wie Shadowsocks quelloffen und gilt als sicher und vertrauenswürdig; es wurde 2017 und 2018 von Spezialisten auf Herz und Nieren geprüft. Allerdings lässt es sich einem Bericht zufolge trotz Verschleierungstechniken mit etwas Aufwand identifizieren (siehe ct.de/y9y1).

Deshalb lässt sich der Zugriff auf Outline-Server sperren. Das erfolgt allerdings per Hand und krude anhand von Ziel-IP-Adressen, weshalb sich Outline-Sperrungen nur dann häufen, wenn sich die politische Lage zuspitzt. Als Gegenmaßnahmen empfehlen die Outline-Entwickler den Betrieb mit mehreren IP-Adressen unter demselben Domainnamen (ct.de/y9y1).



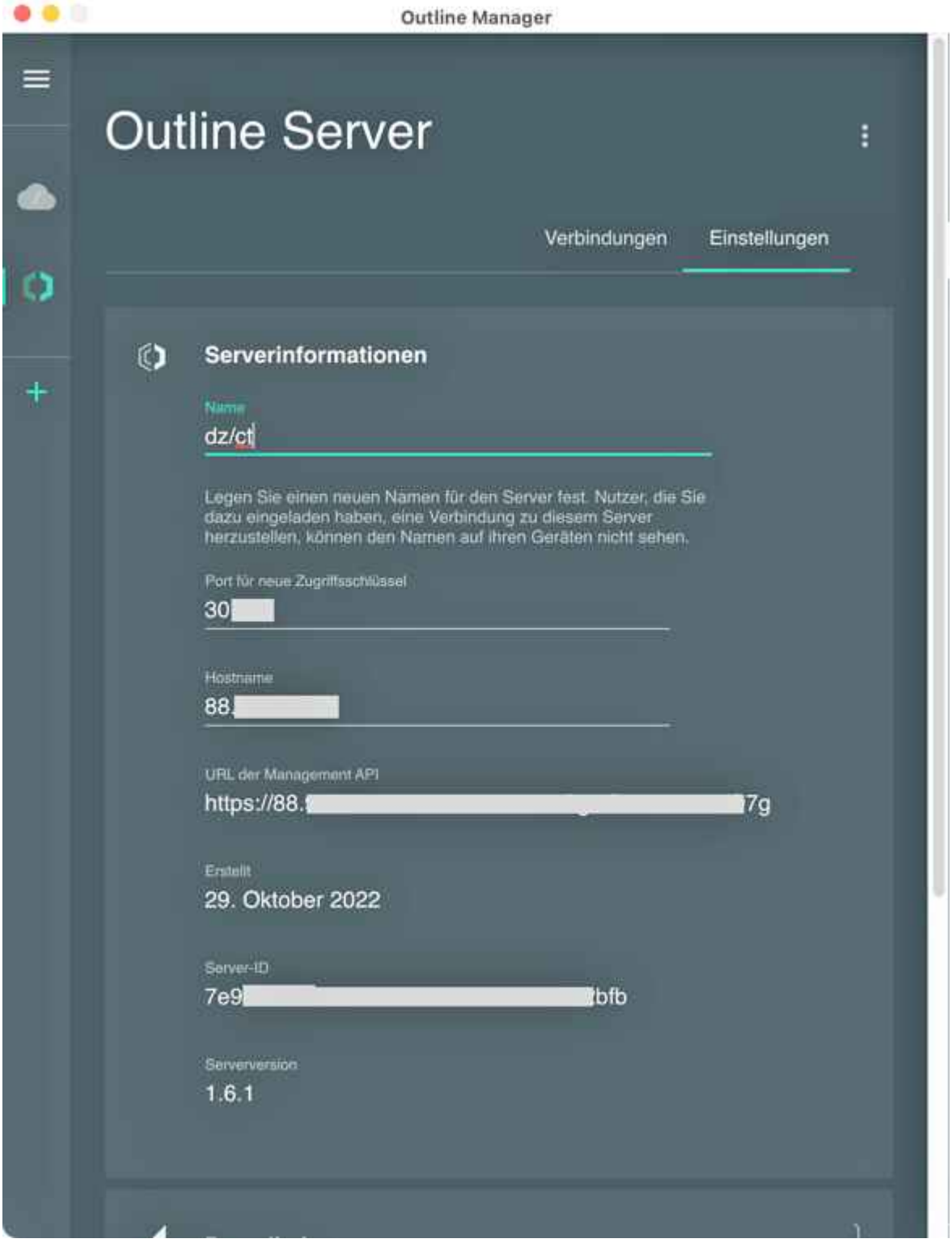
Der Outline-Client installiert auf Windows ein virtuelles TAP-

Interface und lenkt darüber allen ausgehenden Internet-Verkehr in den Tunnel zum Outline-Server.

Outline Manager und Server

Ausgehend vom Outline Manager haben wir den Outline-Server auf zwei Debian-VMs installiert, es klappte auf beiden im Nu und reibungslos. Dabei nimmt ein Bash-Skript dem Admin sehr vieles ab; es verlangt nur einige wenige Angaben. Am Ende fällt ein URL heraus, den man in den Outline-Manager kopiert und ein Zugangsschlüssel mitsamt Server-URL, die man an die Nutzer verteilt.

Darüber hinaus bietet der Manager nur wenige weitere Funktionen. Man kann für Clients Obergrenzen für das Übertragungsvolumen festlegen und Verwaltungsdaten wie IP-Adresse oder Server-ID ablesen – das wars auch schon. Infos und diverse Statistiken liefert das Monitoring-Tool Prometheus, das man auf dem Outline-Server über die lokale IP-Adresse 127.0.0.1 und die TCP-Ports 9090, 9091 und 9092 anzapft. Außerdem bietet Google einen Metrics-Server auf Grundlage der Google App Engine; er setzt Googles Cloud SDK voraus (ct.de/y9y1).



Das Einrichten des Outline-Servers startet man auf Linux, macOS oder Windows mit dem Outline Manager. Anschließend läuft auf dem Zielserver ein Bash-Skript und richtet dort einen Docker-Container mit Shadowsocks ein – was alles ohne besondere Netzwerkkenntnisse klappt.

Prinzipiell sollte der Server auch auf anderen Betriebssystemen laufen, denn er steckt in einem Docker-Container auf Basis der Alpine-Distribution 3.11.6 (siehe

Docker-Plattform Quay, ct.de/y9y1). Das Installationsskript des Outline Managers sieht aber nur Linux-Plattformen (x86_64) als Zielserver vor.

Um zu prüfen, was das Skript tut, lädt man es einfach aus dem GitHub-Projekt von Jigsaw (siehe ct.de/y9y1) auf einen PC und liest es in einem Editor. Unter anderem installiert es Docker, falls das fehlt, und richtet den Container mitsamt dem Zugriffsschlüssel ein.

Insgesamt liefen beide Server-Instanzen im mehrwöchigen Testbetrieb reibungslos. Zwar haben die Entwickler den Container seit zwei Jahren nicht aktualisiert, sodass die automatische Test-Routine von Quay viele und auch kritische Sicherheitslücken meldet. Sie betreffen aber nur den Befehl curl 7.67.0 (Release-Datum 6.11.2019), den man im Serverbetrieb nicht nutzt. Wer die Lücken trotzdem eliminieren will, findet die erforderlichen Update-Befehle im Quay-Repository (siehe ct.de/y9y1).

Outline Client

Der Outline Client ist ebenfalls flink installiert. Hat man ihm eine passende URL spendiert, baut er die Verbindung zum Server umgehend auf und signalisiert das im Menü. Fortan läuft jeglicher Internet-Verkehr durch den Tunnel. Auf Macs kann man das beispielsweise mit dem Befehl netstat -rn | grep 'default' auslesen. Dabei wird sichtbar: Der gesamte Verkehr wird an ein virtuelles TUN-Interface geleitet (z. B. utun10).

Mit ifconfig utun10 kann man die (lokale) Ziel-IP-Adresse auslesen (inet 169.254.19.0) und route -n get <domain> zeigt, über welchen Weg ein bestimmtes Ziel angesprochen wird:

route -n get ct.de

gibt zum Beispiel Folgendes aus:

route to: 193.99.144.80

```
destination: default
interface: utun10
```

Wer im Container herumspaziert, findet bald, dass die Jigsaw-Entwickler zur DNS-Auflösung der VPN-Clients die DNS-Resolver von Google konfiguriert haben. So schenkt man Google die Surf-Ziele der VPN-Nutzer. Google sichert immerhin zu, dass es DNS-Anfragen anonymisiert und spätestens nach 48 Stunden löscht. Wer trotzdem andere Resolver will, muss den Container editieren und etwa 9.9.9.9 eintragen (Resolver des gemeinnützigen Anbieters Quad9).

Fazit

VPN-Funktionen bilden heute für sehr viele Anwendungen die Kommunikationsgrundlage, obwohl die Technik ursprünglich nur zur Vernetzung von Standorten gedacht war. Manche Anwendungen verändern sich (Peer-to-Peer für Filesharing) und manche greifen Methoden aus teils scheinbar fernen Bereichen auf, etwa die Nutzdatenverschleierung bei Shadowsocks oder die RSA Blind Signatures beim Privatsphärenschutz von Apple und Google.

Das liegt in der Natur der Sache, denn die VPN-Entwicklung unterliegt einem starken Optimierungsdruck. Auf weitere Innovationen kann man ebenso gespannt sein wie darauf, ob und welche weiteren VPN-Anbieter diese aufgreifen. *(dz@ct.de)*

VPN-Infos: ct.de/y9y1