Blitz-VPNs: Einfach, schnell & sicher

Was Peer-to-Peer-VPNs leisten, wie Pretty Good Phone Privacy Smartphones schützt

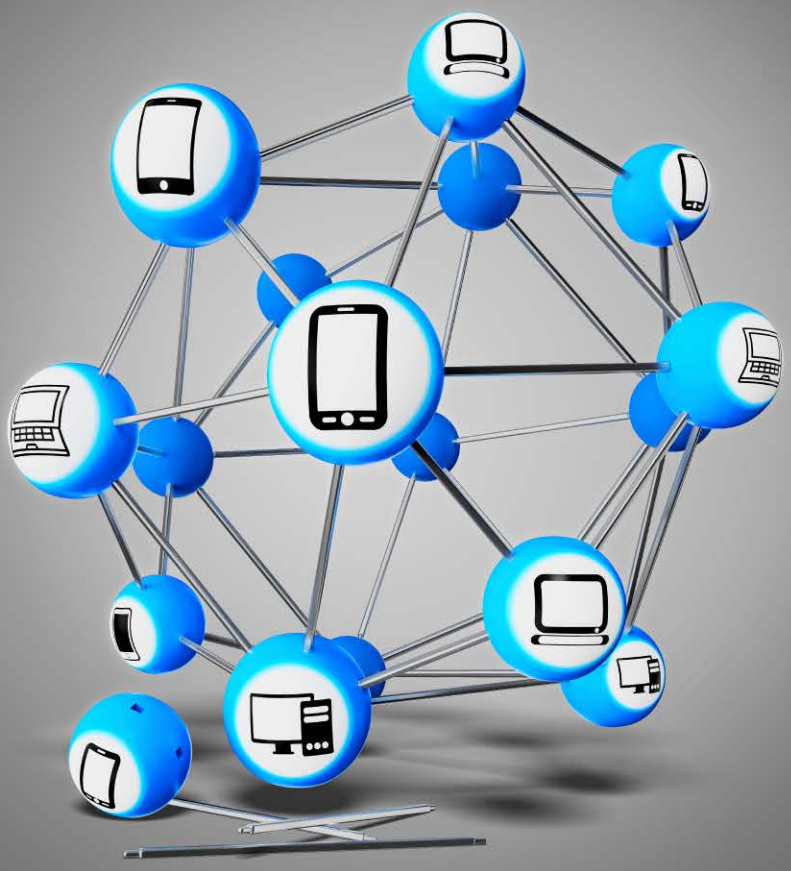

Bild: Andreas Martini

Die VPN-Technik zur Gerätevernetzung hat viele Gesichter. Wir stellen VPN-Anwendungen vor, die mit eleganten Client-Direktverbindungen kleine Arbeitsgruppen ansprechen. Zusätzlich werfen wir ein Schlaglicht auf ein erstaunliches Werkzeug zur digitalen Selbstverteidigung auf Smartphones.

Von Dušan Živadinović

Das Kürzel „VPN“ steht auf vielen Dingen, doch was genau drin ist, muss man erst herausfinden. In diesem Schwerpunkt geht es um den Smartphone-Schutz Pretty Good Phone Privacy sowie um die vier VPN-Anwendungen Nebula, Twingate, Tailscale und ZeroTier. Damit binden Admins von Heimnetzen und kleinen bis mittleren Arbeitsgruppen ferne Standorte und Geräte zum Beispiel für Freigaben und für die Fernwartung an. Anders als bei konventionellen VPNs wie IPsec oder WireGuard steht dabei kein zentraler VPN-Server als Drehscheibe im Mittelpunkt. Stattdessen kommunizieren die Clients direkt miteinander, Peer-to-Peer.

Mit Pretty Good Phone Privacy, das augenzwinkernd an die PGP-Verschlüsselung für E-Mails erinnert, zieht das US-Start-up Invisv viel Aufmerksamkeit auf sich. Die Firma wirbt mit den Namen der Sicherheits- und Datenschutzexperten Bruce Schneier und Jon Callas als Berater und verspricht eine Tarnkappe für Smartphones, die sogar vor den Augen von Mobilfunknetzbetreibern schützt. Mehr dazu ab dem Abschnitt „Spurlos funken“.

Die Peer-to-Peer-VPNs gehen auf gestiegene Schutzanforderungen und auf eine Modernisierung der Architektur zurück. In herkömmlichen VPNs bildet der Server den zentralen Umschlagpunkt und somit einen Engpass: Ein langsamer Internetanschluss des Servers bremst die Clients ebenso aus wie eine Serverüberlastung. Der Peer-to-Peer-Ansatz löst den Umschlagpunkt auf, Clients kommunizieren direkt miteinander. Zu dieser VPN-Klasse gehören etwa Tinc, yggdrasil und auch manche Selbstbauanleitung (siehe ct.de/yvtt).

Zugleich haben einige Hersteller die zentrale Verwaltung in ein Webinterface verpflanzt (Dashboard) und mit Konzepten von Software-defined Networks erweitert. Damit gelingt die Verteilung von kryptografischen Schlüsseln und Konfigurationen nebenbei ganz einfach per Mausklick. Manchen gelten sie daher als kleines Admin-Glück.

Ein Beispiel ist ZeroTier, mit dem man Server, PCs, NAS-Geräte und Smartphones vernetzt. Das geht so schnell, dass man von Blitz-VPNs sprechen kann. Mehr dazu lesen Sie ab den Seiten 20 und 28.

Burgverbesserung

Andere Hersteller haben das Peer-to-Peer-Konzept mit zusätzlichen Schutzmaßnahmen für Unternehmen aufgebohrt. Manche sprechen mit kostenlosen Einstiegsangeboten und durchdachten Bedienoberflächen inzwischen auch kleine Arbeitsgruppen und Privatnutzer an, zum Beispiel um Familienmitglieder zu vernetzen.

Viele Sicherheitskonzepte gehen davon aus, dass es genügt, interne Infrastrukturen ähnlich einer Burg mit Firewalls abzuschotten. Und da Mitarbeiter auch mal von draußen ins Firmennetz müssen, richtet man hinter der Firewall VPN-Server ein, zu denen ähnlich einer Zugbrücke ein einziger, gut geschützter Zugang führt. Das interne Netz gilt als sichere Umgebung für Unternehmensanwendungen.

Doch längst halten manche Fachleute den Ansatz für überholt. Google ist überzeugt, dass auch das interne Netzwerk voller Gefahren steckt. Beispielsweise können Phishing-Mails zum Herunterladen von Schadsoftware verleiten, was selbst Firewalls mit Deep Packet Inspection nicht verhindern können.

Zwei Fluchtbewegungen

Hinzu kommt, dass Admins von konventionellen VPNs zwei Fluchtbewegungen absichern müssen: Viele Mitarbeiter bleiben im Homeoffice und viele Applikationen wandern vom abgeschotteten Firmenserver in die Cloud. So sind immer mehr Mitarbeiter und Betriebsmittel übers Internet verstreut. Ein traditionelles VPN ist daher schwer zu verwalten und wenn Angreifern ein Einbruch gelingt, ist oft das ganze Netz gefährdet.

Nach neueren Konzepten ist keinem Netzwerkgerät und keinem Nutzer zu trauen, jeglicher Zugriff auf Firmenressourcen muss authentifiziert, autorisiert und verschlüsselt werden (Zero Trust). Zusätzlich schränkt man den Zugriff auf die für die Arbeit erforderlichen Ressourcen und Applikationen ein (Least Privilege). So schrumpft die Angriffsfläche und es spielt keine Rolle, wo sich Mitarbeiter physisch aufhalten.

Zu dieser VPN-Klasse gehören Tailscale, Twingate und Nebula, die wir ab Seite 20 vorstellen. Tailscale entwickelt keine eigene Verschlüsselung, sondern greift auf das moderne WireGuard zurück. Das gilt auch für das taufrische NetBird, an dem das Saarbrücker CISPA Helmholtz Center für Informationssicherheit mitwirkt. Wir widmen NetBird einen genaueren Blick, sobald die Entwickler mobile Clients freigeben.

Spurlos funken

VPNs können andererseits auch im Mobilfunk die Privatsphäre schützen. Kritiker sehen diese Privatsphäre längst ausgehöhlt und halten Smartphones mit GPS für digitale Plaudertaschen.

Eine durchgehende digitale Selbstverteidigung fällt da schwer. Selbst Apples Private Relay und Google One VPN schützen nur die Kommunikation vor Mitlesern und verbergen die IP-Adresse der Nutzer. Dafür setzen beide zusätzlich zum Tunnel die Kryptografietechnik RSA Blind Signatures ein und entkoppeln so die Nutzdaten von der Kundenauthentifizierung, sodass sich keine Benutzerprofile erstellen lassen. Der Verschleierer Invisv setzt dem ganzen noch eins drauf und entkoppelt mit eigenen eSIMs die Identität des Mobilfunknutzers von der SIM-Karte (genauer: IMSI). Leider ist PGPP in Deutschland nicht zu bekommen. Warum, und wie die Technik funktioniert, lesen Sie ab Seite 26. *(dz@ct.de)* **ct**

Peer-to-Peer-VPNs: ct.de/yvtt