IMMER SICHER VERBUNDEN: EIN SICHERER ZUGRIFF AUFS INTERNET GELINGT MIT EINEM VPN

Die Notwendigkeit von überall her sicher auf Informationen zugreifen zu können, die normalerweise nur aus dem Firmennetzwerk heraus verfügbar sind, stellt eine Herausforderung dar. Meistens handelt es sich dabei um sensible Informationen, die sicher von A nach B transportiert werden sollen, ohne dass jemand Drittes mitlesen kann.
Wie ein VPN dabei hilft diese Daten sicher verschlüsselt zu übertragen, zeigen wir hier.

DIGITAL SICHER NRW
Kompetenzzentrum für Cybersicherheit in der Wirtschaft

Beauftragt vom Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen

DIGITAL SICHER NRW

ANTWORTEN AUF DIE WICHTIGSTEN FRAGEN

WAS IST EIN VPN?

Ein virtuelles privates Netzwerk (VPN) leitet den Internetverkehr eines Endgeräts über eine sichere Zwischenstation (VPN Zugangspunkt) um und verschlüsselt diesen Verkehr.
Es ist eine Art sicherer Tunnel durch ein unsicheres Internet.
So wird ein Ausspähen, Mitlesen oder Manipulieren unmöglich gemacht.

WARUM IST EINE SICHERE VERBINDUNG NÖTIG?

Heutzutage ist es oft notwendig, von überall und beinahe von jedem Gerät aus auf Daten zugreifen zu können.
Um diesen Zugriff digital sicher zu gestalten, macht es Sinn, die Verbindung zu einem Netzwerk über eine verschlüsseltes und somit abgesichertes VPN aufzubauen. So werden die Daten auch beim Versand oder Empfang vor den Augen unbefugter Dritter geschützt.

WANN SOLLTE EINE VERBINDUNG MIT EINEM VPN GENUTZT WERDEN?

Ein VPN sollte genutzt werden, um Verbindungen abzusichern. Öffentliche Zugangspunkte (z.B. „Hotspots“), bei denen sich die Vertrauenswürdigkeit selten bewerteten lässt, sollten daher nur in Kombination mit einer VPN-Verbindung genutzt werden. Das gilt insbesondere für Cafés, Bahnhöfe, Flughäfen oder Hotels.

ANTWORTEN AUF DIE WICHTIGSTEN FRAGEN

WIE KANN EIN EIGENES VPN EINGERICHTET WERDEN?

Ein eigenes VPN kann software- oder hardwarebasiert eingerichtet werden:

- Softwarebasiert:
  - das Betriebssystem bietet eigene Möglichkeiten an
  - VPN-Software von externen Anbietern oder Open Source Software wie *OpenVPN* kann genutzt werden
- Hardwarebasiert:
  - spezielle VPN-Gateways sorgen für ein erhöhtes Sicherheitslevel und maximale Leistung.

WORAUF SOLLTE BEI DER EINRICHTUNG EINES VPN GEACHTET WERDEN?

Wichtig bei der Einrichtung eines VPN ist, dass die Authentifizierung beim Zugriff auf das virtuelle private Netzwerk nicht nur durch ein einzelnes Kennwort, sondern besser durch eine Zwei-Faktor-Authentifizierung erfolgt.

Die Einrichtung eines VPN kann im Firmenumfeld sehr schnell an Komplexität gewinnen. Im Zweifelsfall sollte daher bei der Planung und Einrichtung professionelle Unterstützung eingeholt werden.

VPN – UNTERWEGS UND IM HOME-OFFICE

Um auch im Home-Office oder bei der Arbeit unterwegs in Bahn, Hotel oder Café sicher auf Firmenressourcen zugreifen zu können, ist die Nutzung eines VPN unabdingbar.

Wie Sie Ihr eigenes Unternehmens-VPN einrichten, zeigen wir Ihnen Schritt für Schritt in unserer Videoanleitung, die Sie über den QR-Code erreichen!

Erklärvideos VPN

DIGITAL SICHER NRW
Kompetenzzentrum für Cybersicherheit in der Wirtschaft

Beauftragt vom Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen