Virtual Private Network (VPN) ist eine weit verbreitete Methode, um externen Rechnern einen sicheren Zugriff in Ihr Firmennetz zu gewähren. Dabei sind jedoch situationsabhängig einige Dinge zu beachten. Diese Checkliste soll Ihnen bei den Vorüberlegungen zu Einführung und Erweiterung einer VPN-Infrastruktur eine Hilfestellung geben.

Sind VPN-Zugänge über private Endgeräte in Ihrem Unternehmen überhaupt erlaubt/erwünscht?
Zuerst sollten Sie sich Gedanken dazu machen, welchen Geräten Sie überhaupt einen VPN-Zugriff erlauben möchten. Beinhaltet dies nur unternehmenseigene Hardware oder auch private Hardware (BYOD)?

Erfüllt Ihre eingesetzte Firewall die nötigen Voraussetzungen?
VPN ist aufgrund der Verschlüsselung und der Authentifizierung ein sehr ressourcenintensiver Dienst, dementsprechend sollte Ihre Firewall über ausreichend Leistungsreserven verfügen. Stellen Sie außerdem sicher, dass verfügbaren User-Lizenzen für Ihren Bedarf ausreichen.

Ist die Qualität der Internetverbindung ausreichend?
Prüfen Sie, ob die Internetanbindung den Anforderungen von VPN und den geplanten Aufgaben gewachsen ist. Dies beinhaltet nicht nur Ihren Unternehmensanschluss sondern speziell auch die private Leitung Ihrer Mitarbeiter. Gerade in Privathaushalten ist der Upload oft deutlich geringer als der Download bemessen und die Antwortzeiten erschweren flüssiges Arbeiten.

Muss auf mehrere Standorte zugegriffen werden?
Wenn Ihr Unternehmen über mehrere Standorte verfügt, ist eine zentrale Einwahl zumindest für die Anwender die praktischere Lösung. Wenn dies gewünscht und umsetzbar ist, gelten jedoch besondere Anforderungen an das Routing und die nötigen Sicherheitsvorkehrungen.

Entspricht die vorhandene (VPN-)Infrastruktur einem aktuellen Stand?
Bei der Erweiterung einer vorhandenen VPN-Lösung sollten Sie sich natürlich auch Gedanken dazu machen, ob diese noch dem Stand der Technik entspricht und ob eine Erweiterung möglich und sinnvoll ist. Ggf. kann ein Austausch vorhandener Komponenten die Stabilität und Sicherheit Ihrer gesamten VPN-Lösung steigern. Außerdem sollten Sie natürlich prüfen, ob VPN für alle Ihre eingesetzten Systeme die richtige Wahl ist, oder ob Sie nicht manche Systeme anders verfügbar machen möchten z.B. über einen Application Delivery Controller.

Wie soll die Sicherheit gewährleistet werden?
Generell sind bei der VPN-Nutzung erweiterte Sicherheitsvorkehrungen geboten. Unter anderem empfiehlt sich eine Multi-Faktor-Authentifizierung, denn leider sind mittlerweile vermehrt Angriffe auf VPN-Infrastrukturen und entsprechende Phishingwellen zu verzeichnen.

Sie haben weitere Fragen zu VPN oder möchten sich zu einer für Sie passenden Lösung beraten lassen? Kommen Sie einfach auf uns zu. **Hier gehts zum Kontaktformular!**

Deutschland
INNEO Solutions GmbH
Rindelbacher Straße 42, 73479 Ellwangen
Tel. +49 (0) 7961 890-0, Fax +49 (0) 7961 890-177

www.inneo.de
shop.inneo.de