

VPN allgemein

Kurz und knapp bietet die Verwendung von VPN Nutzenden an der TU Braunschweig folgende Vorteile:

- Sämtlicher Verkehr aus dem möglicherweise unsicheren lokalen Netz wird zunächst verschlüsselt zur TU Braunschweig übertragen. Der Verkehr selbst, so wie eigene Aktivitäten im Netz vor Ort sind vor dem Ausspähen durch Dritte geschützt.
- Man erhält Zugriff auf Dienste, die sonst nur aus dem Netz der TU Braunschweig möglich sind.
- Es werden die DNS-Server der TU Braunschweig genutzt, auf denen Sicherheitsmechanismen implementiert sind, die u. a. den Zugriff auf kompromittierte Ziele blockieren.

Genauer steht VPN steht für "Virtual Private Network", auf Deutsch virtuelles privates Netzwerk. Es handelt sich zunächst allgemein um eine Technologie, die es ermöglicht, eine sichere Verbindung zwischen einem Nutzer (oder einem lokalen Netzwerk) und einem entfernten Netzwerk herzustellen. Dabei wird außerdem der **Datenverkehr zwischen Client und Server verschlüsselt**, um Privatsphäre und die Sicherheit der übertragenen Daten zu gewährleisten. Oft wird diese Verbindung auch als "VPN-Tunnel" bezeichnet. Eine Einwahl per VPN aus einem mobilen Netzwerk, bei der sämtlicher Verkehr zunächst verschlüsselt zur Heimateinrichtung übertragen wird, beugt der Ausspähung der übertragenen Daten und eigenen Aktivitäten durch Dritte vor, die lediglich beobachten können, dass sämtlicher Verkehr zu einem einzigen entfernten Ziel übermittelt wird.

Für den VPN-Tunnel können verschiedene Protokolle zur gegenseitigen Authentifizierung der Tunnel-Endpunkte und Verschlüsselung des Datenverkehrs eingesetzt werden. An der TU Braunschweig wird IKEv2 für die Authentifizierung und den Austausch der Verschlüsselungsparameter eingesetzt, während der Tunnel selbst über Port 443 per SSL verschlüsselt wird. Letzteres erlaubt den Aufbau eines Tunnels aus nahezu allen Netzwerken, in denen speziellere Protokolle (z.B. IPSec) blockiert werden. Auf Client-Seite setzen wir hier insbesondere auf die **Software "Cisco Secure Connect"**, die in gleicher bzw. sehr ähnlicher Weise für alle gängigen Betriebssysteme bereit steht.

Neben der Verschlüsselung des Verkehrs führt der Aufbau eines VPN-Tunnels zur Heimateinrichtung außerdem dazu, dass man innerhalb des Tunnels über eine **IP-Adresse kommuniziert, die zur Heimateinrichtung gehört**, und ggf. so von den Vorteilen und Berechtigungen profitiert, die man ansonsten nur nutzen könnte, wenn man sich im Heimatnetz befindet. An der TU-Braunschweig bezieht sich dies insbesondere auf einige Dienste, die sonst nur innerhalb des TU-Netzwerks erreichbar sind bzw. Dienste externer Anbieter, die diese wiederum für

den Adressbereich der TU freigegeben haben. Letzteres betrifft vor allem Bibliotheksrecherchen in den Portalen verschiedener Verlage für wissenschaftliche Veröffentlichungen.

Ein weiterer Vorteil, der in Zeiten immer häufiger und professioneller werdender Phishing-Attacken von zunehmender Bedeutung wird, ist, dass **für Verbindungen durch den VPN-Tunnel die DNS-Server der TU Braunschweig für die Namensauflösung zuständig sind**. Bei der Herstellung einer VPN-Verbindung mit dem **Profil "Tunnel-all-Traffic"** profitieren Nutzende deswegen auch mobil bzw. im HomeOffice von den darauf implementierten Sicherheitsmechanismen, die z.B. den Zugriff auf bekanntermaßen kompromittierte Ziele blocken.

Es kann jeweils immer nur eine Verbindung pro Benutzer aufgebaut werden.

Revision #9

Created 18 January 2024 11:02:18 by Tina Strauf

Updated 22 October 2024 11:26:36 by Ralf Geffers