Fernzugang zum Verwaltungsnetz

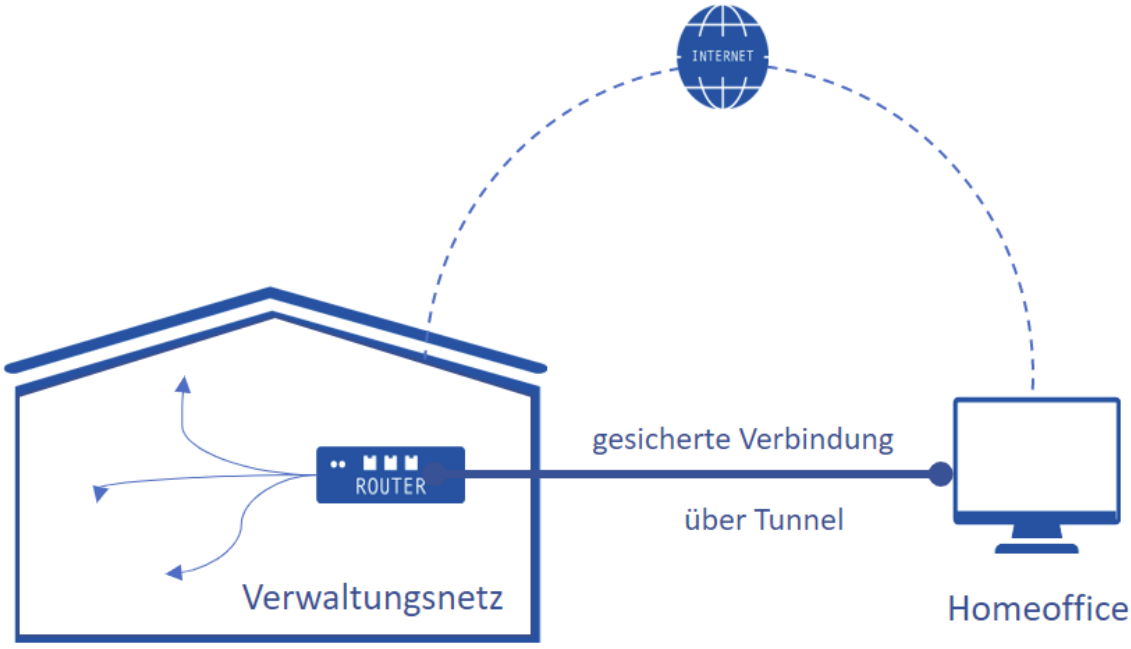
VPN-Zugang

VPN-Technik bietet den sicheren Remote-Zugriff auf IT-Systeme.
Bei der Verarbeitung personenbezogener Daten sind besondere Anforderungen an das Thema Datenschutz zu stellen. Vertraulichkeit, Authentizität und Datenintegrität müssen bei der Kommunikation berücksichtigt werden. VPN-Technologien bieten den geforderten Schutz, müssen aber wohl überlegt ausgewählt, eingerichtet und eingesetzt werden. Die Komplexität der Einrichtung erfordert weitreichende Fachexpertise.

VPN-Szenarien

Im Schulumfeld sind insbesondere zwei Szenarien denkbar: Client-to-Site-VPN und Site-to-Site-VPN.

Ein **Client-to-Site-VPN** ermöglicht die sichere Anbindung eines einzelnen Rechners an ein Netzwerk. Eine VPN-Client-Software wird in diesem Fall auf dem Endgerät der Lehrkraft betrieben, der VPN-Server läuft auf einem Router oder einem dedizierten Gateway im Schulnetz.



Einsatzbeispiele:

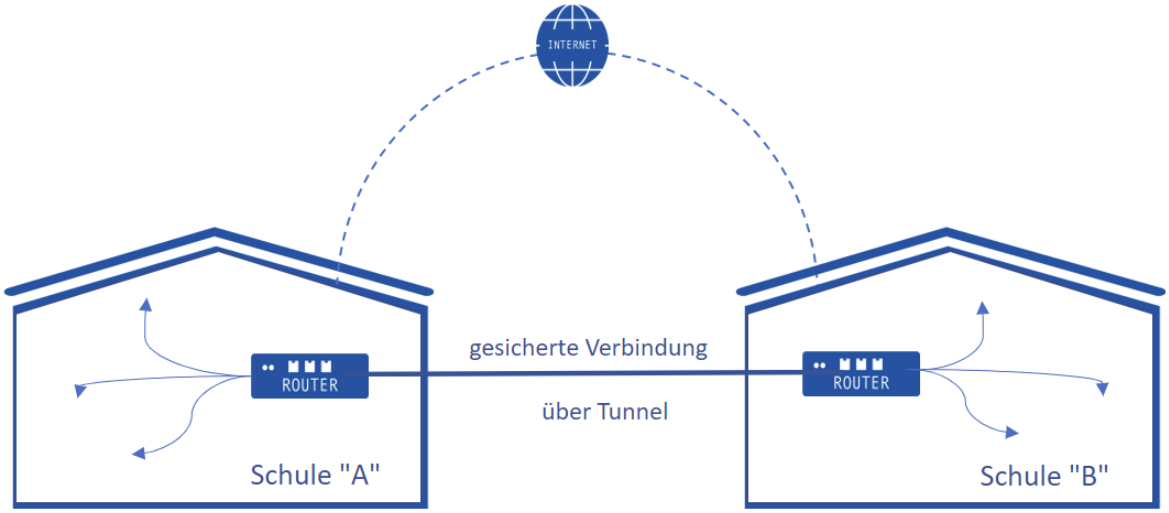
- Zugriff auf Server im Schulverwaltungsnetz durch die Schulleitung
- Datenkommunikation mit schulinternen Systemen durch Lehrkräfte
- Erledigung administrativer Aufgaben durch die Systembetreuung

Stand: 09.06.2022

In jedem Fall muss der VPN-Client technisch korrekt installiert und eingesetzt werden. Die Installation sollte dokumentiert und die Funktionalität überprüft werden.
Benutzerfragen zur Bedienung und Datensicherheit werden durch eine Einführung oder Schulung beantwortet.

Site-to-Site-VPN

Bei einem **Site-to-Site**-Szenario bauen zwei VPN-Systeme (bspw. Router) eine gesicherte Verbindung zueinander auf. Die Kommunikation zwischen den beiden Netzen läuft über einen verschlüsselten VPN-Tunnel. Mehrere Standorte einer Schule können auf diese Weise mit der zentralen IT-Infrastruktur verbunden werden.



VPN-Protokoll

Alle am VPN beteiligten Komponenten, der VPN-Client und der VPN-Server, müssen die gleiche Sprache, d.h. das gleiche Protokoll, sprechen.

Die Auswahl eines geeigneten VPN-Protokolls ist von verschiedenen Faktoren abhängig:

- VPN-Szenario und Einsatz
- Kompatibilität zum Client-Betriebssystem
- Skalierbarkeit
- Infrastruktur
- Expertise bei Einrichtung und Wartung
- IP-Adressen (ext. /int., IPv4/IPv6)
- Sicherheit (z.B. Unterstützung von Zweifaktorauthentifizierung, falls erforderlich)

Ein weit verbreiteter Standard ist IPsec[1]. Viele Hersteller von Internetzugangsroutern haben das VPN-Protokoll IPsec implementiert und ermöglichen so den Betrieb des Routers als VPN-Gateway. Die Anzahl der gleichzeitigen VPN-Tunnel ist von der Leistungsfähig des Routers und ggf. der erworbenen Lizenz abhängig.
Mit IPsec lassen sich sowohl Client-to-Site als auch Site-to-Site-Szenarien realisieren.

Neben IPsec gibt es verschiedene andere, teilweise proprietäre, VPN-Technologien am Markt. Verbreitet sind auch Lösungen wie OpenVPN, Wireguard oder HTTPS- bzw. SSL-basierte Verfahren.

Das ausgewählte Verfahren muss Mechanismen für eine gesicherte Datenübertragung bereithalten. Die Authentifizierung erfolgt über ein separat geführtes Benutzerverzeichnis – z.B. auf dem Router – oder über die Anbindung eines Authentifizierungsdienstes bzw. -servers. Eine weitere Möglichkeit ist der Einsatz von Zertifikaten.

Entsprechend der Router- und Firewall-Konfiguration dürfen die VPN-Nutzer nur auf ausgewählte Bereiche im Schulnetz zugreifen.

Sicherheit

Im Falle des Zugriffs vom Heimarbeitsplatz auf das Schulnetz wird das schulische Endgerät ein Teil des Schulnetzes. Damit ist er genauso zu behandeln wie ein Schul- bzw. Verwaltungs-PC. Das gilt sowohl für Firewall-Einstellungen wie auch für die Richtlinien bzgl. Anti-Viren-Schutz.
Ein besonders hoher Schutzbedarf ergibt für den Zugriff auf das Verwaltungsnetz. Nur ausgewählte Personen (SL, Mitarbeiter der SL etc.) mit berechtigtem Interesse können auf dieses Netzwerk zugreifen.

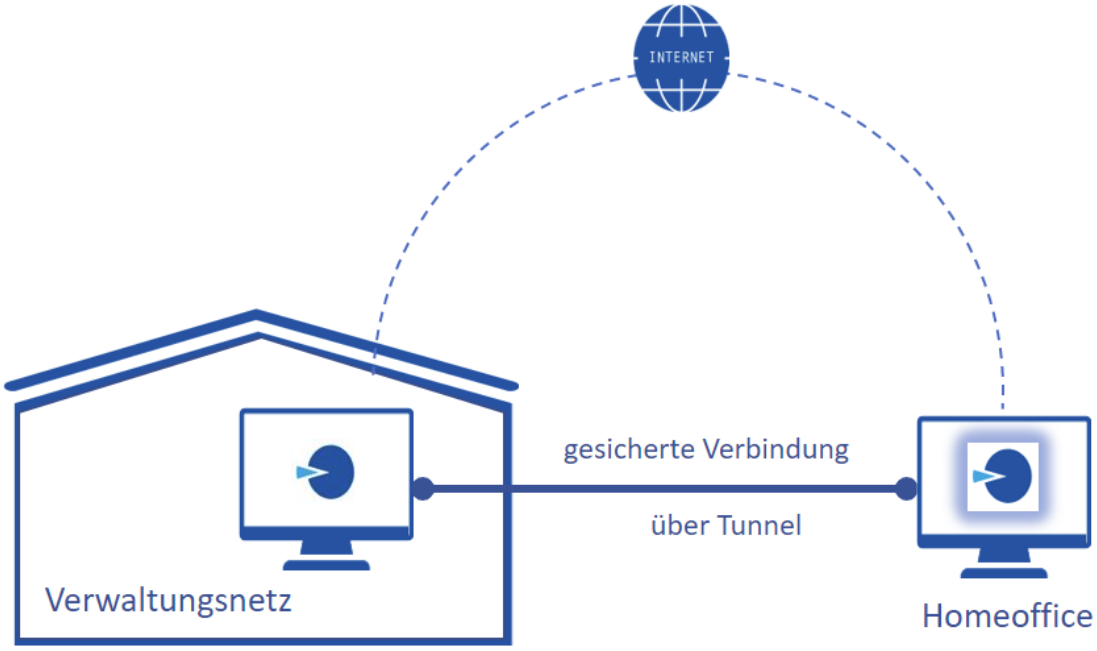
Bei einem Zugriff per VPN ist sicherzustellen, dass der gesamte Datenfluss über die VPN-Verbindung erfolgt. In diesem Fall ist die allgemeine Internetnutzung nur über das Gateway mit Firewall der Schule gestattet. Der gleichzeitige Zugriff auf das Verwaltungsnetz und das offene Internet (Split-Tunnel) sollte über die VPN-Client-Konfiguration eingeschränkt werden.

Der Schlüssel zur VPN-Nutzung wird in vielen Fällen in der VPN-Software gespeichert. Im Falle eines Verlustes des Endgerätes (Notebook, Tablet, Smartphone) besitzt der Finder damit die Möglichkeit des Netzzugriffs. Eine Zwei-Faktor-Authentifizierung erhöht die Sicherheit und bietet einen erweiterten Schutz.

[1] IPsec wird hier beispielhaft für ein mögliches und geeignetes VPN-Protokoll verwendet

Virtuelle Desktop Infrastruktur (VDI)

Zugriff auf ausgewählte Anwendungen (z. B. Termialservices; Virtual Desktop Infrastructure)



Als Sonderform von VPN kann der Zugriff auf bestimmte Anwendungen betrachtet werden. Bei dieser Technik werden über eine gesicherte Verbindung die Bedienung einzelner Anwendungen eines extra bereitgestellten Terminalservers im Zielnetzwerk über einen Terminaldienst ermöglicht. Über die Verbindung werden nur Eingaben zur Bedienung einerseits und die grafische Darstellung/Ausgabe andererseits transportiert. Es ist kein direkter Zugriff auf weitere Ressourcen im Zielnetz auf Netzwerkebene möglich. Da diese Technik die potentielle Gefahr der Daten-Kompromittierung deutlich reduziert, sind auch geringere Anforderungen an die Sicherheit des Endgeräts zu stellen. Eine Festplattenverschlüsselung an den Endgeräten ist hier deshalb nicht zwingend notwendig. Es empfiehlt sich vor allem, wenn dem Anwender nur Zugriff auf ausgewählte Anwendungen ermöglicht werden soll – zur Fernadministration des Netzwerks eignen sich die oben genannten VPN-Techniken wohl mehr.