Virtuelle Private Netzwerke

... mit Sicherheit durchs Internet

Hubert Pitner

Das *World Wide Web* (WWW) hat mit weltweiter E-Mail, der Zugriffsmöglichkeit auf WEB Seiten, E-Commerce, Chat und anderen Anwendungen das Leben von uns allen wesentlich verändert. Bei der Entwicklung der Technologien für das Internet hatten die Programmierer jedoch immer nur die **Datensicherheit** im Auge – um den **Datenschutz** muss sich jeder Anwender selbst kümmern.

Wenige wissen es und auch von ihnen wird nur hinter vorgehaltener Hand darüber gesprochen: Sämtliche Daten im Internet sind „öffentlich" mit geeigneten Sniffer- (=schnupper) Programmen kann der gesamte Datenverkehr im Internet beobachtet und protokolliert werden. Das stellt kein Problem dar, solange es sich um öffentlich zugängliche Daten (wie z.B. den Besuch von Webseiten) handelt. Wesentlich kritischer wird die Sache schon bei E-Mails, E-Commerce, persönlichen Kenndaten wie PIN-Codes, Wertkartendaten und ähnlichem. Eine Möglichkeit seine Privatsphäre zu sichern besteht darin, einen „Tunnel" durch das Internet zu bauen; wie das funktioniert, soll hier besprochen werden.

Was ist ein VPN (Virtuelles Privates Netzwerk)

Über jedes existierende Netzwerk (z.B. ein LAN im Intranet, dem Internet etc.) kann als weitere Schicht ein virtuelles Netzwerk gelegt werden. Der Trick besteht nun darin, dass sämtliche Daten des Virtuellen Privaten Netzwerkes mit einem Schlüssel gesichert werden, dessen Code nur den rechtmäßigen Benutzern des VPN zugänglich ist; es wird durch Verschlüsselung gleichsam ein gesicherter „Tunnel" durch das existierende Netzwerk gebaut. An den Endpunkten des Tunnels können einzelne Rechner oder sogar ganze LANs angeschlossen werden. Die Endpunkte dieser Verbindung bestehen dann aus speziellen VPN-Servern oder VPN-Gateways, die miteinander über die im öffentlichen Netz benutzten Protokolle kommunizieren. VPN Server verschlüsseln die „getunnelte" Verbindung auf der Protokollebene; damit ist selbst bei Benutzerfehlern eine Verschlüsselung sichergestellt.

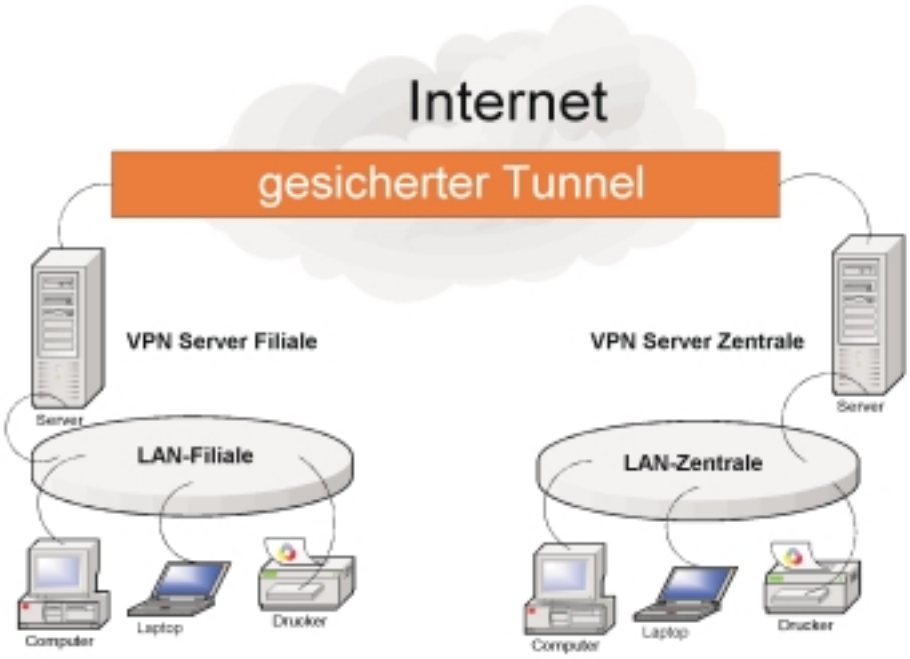
Einsatz von VPN

VPN werden überall dort eingesetzt, wo Daten verschlüsselt zwischen zwei oder mehreren Standorten z.B. einer Firma, Universitäten oder auch privaten Anwendern schnell, sicher und kostengünstig übertragen werden müssen. Neben diesen meist festen Installationen besteht die Möglichkeit, dass sich Außendienstmitarbeiter gesichert und verschlüsselt das Netz ihrer Firma einloggen können. In Fällen, wo es auf besonders hohe Sicherheitsstandards ankommt, reicht die übliche Sicherung durch Passwörter oft nicht aus. Abhilfe gegenüber dieser Sicherheitslücke schafft hier die Authentifizierung mit Hilfe digitaler Zertifikate.

Wie funktionieren VPN?

Tunneling

Tunneling ist die VPN-Technologie die es ermöglicht, Datenpakete aus einem LAN über ein beliebiges Netzwerk (z.B. das Internet) verschlüsselt in ein anderes LAN oder zu einem anderen Rechner zu senden. Die VPN-Software übernimmt auf der einen Seite des Tunnels von einem LAN die unverschlüsselten Datenpakete, verschlüsselt diese (ähnlich wie das auch z.B. bei PGP (*pretty good privacy*) gemacht wird) und schickt die verschlüsselten Datenpakete durch den „Tunnel" über das Netzwerk. Am Ende des Tunnels übernimmt ein zweiter VPN-Server die Datenpakete und entschlüsselt diese, mit dem ihm bekannten Schlüssel. Die einzelnen Rechner in den beiden LANs arbeiten so zusammen, als ob sie sich in ein und demselben Netzwerk befinden würden.



Welches Tunneling Protokoll soll ich wählen ?

Die Protokolle arbeiten üblicher Weise auf den Layern 2 und 3 des OSI-Referenz-Modells und sind somit in der Lage, Zugriffskontrollmechanismen bereit zu stellen, die eine Sicherung des Datenverkehrs über ein VPN ermöglichen.

Das Point to Point Protokoll (PPP)

Üblicher Weise gelangt man heute mit Hilfe von PPP über eine Wählleitung in das Internet. PPP arbeitet nicht verschlüsselt. Es dient jedoch als Transportmittel für die VPN-Protokolle PPTP und L2E.

Das Point to Point Tunneling Protokoll (PPTP)

Dieses Protokoll ist eine Erweiterung des PPP. PPTP kapselt PPP-Pakete in IP-Pakete; auf diese Art können Protokolle wie IP, IPX, NETBEUI etc. über das Internet getunnelt werden. Die Authentifizierung erfolgt hier üblicher Weise über das *Password Authentification Protocol* (PAP).

Layer 2 Forwarding (L2F)

L2F wurde von Cisco entwickelt; es unterstützt verschiedene Protokolle und mehrere voneinander unabhängige parallele Tunnels. L2F verpackt zum Transport die Datenpakete in das PPP-Format.

Andere Verschlüsselungsverfahren, die sich in ihrer Komplexität unterscheiden, jedoch dem gleichen Zweck dienen, sind das *Layer 2 Tunneling Protocol* (L2TP), *IP Security* (IPSec), *RADIUS* und *SOCKS v5*.

Schlussfolgerung

VPN benutzen das Internet oder andere verfügbare Datennetze, um eine gesicherte Verbindung zu Filialen, Außendienstmitarbeitern oder Kunden aufzubauen. So können auf einfache und kostengünstige Weise Netzwerke aufgebaut und bestehende LANs erweitert werden. Das weltweite Internet ermöglicht, dass nahezu jeder Standort und auch mobile Benutzer rasch in das VPN eingebunden werden können.

hubert.pitner@tgm.ac.at