

# 1 Einleitung

Der folgenden Aussage wird sicher niemand widersprechen:

*Das Internet hat sich heute zu einem der wichtigsten Wirtschaftsfaktoren auf unserem Planeten entwickelt und beeinflusst unser Leben in so vielen Bereichen, wie wir es uns vor 10 Jahren noch gar nicht vorstellen konnten.*

Wissenschaft, Forschung, Industrie und Privatanwender sind über ein weit gefächertes Netz miteinander verbunden und tauschen Wissen, Bilder und hohe Geldbeträge aus. Doch drehen wir die Zeit ein bisschen zurück und betrachten die Geschichte dieses Netzwerks: Seine Anfänge hat das Internet im so genannten ARPANET [1], das seinen Betrieb 1969 aufnahm. Ursprüngliche Aufgabe des ARPANETS war es, vier US-amerikanische Universitäten, die im Auftrag des Pentagons forschten, über ein Netzwerk zu verbinden. Die Macher dieses Projektes setzten mit ihrem dezentralen Ansatz eine Revolution in Gang, die zusammen mit dem nahezu gleichzeitigen Erscheinen des Betriebssystems Unix und der Programmiersprache C einen gewaltigen Entwicklungsprozess startete. Denn mit Unix als verbreiteter Plattform und C als durchaus portabler Programmiersprache konnten die für das ARPANET entwickelten Anwendungen schnell und effizient von einem System auf andere übertragen werden. Darüber hinaus war der freie und kostenlose Zugang zu Spezifikationen ein wesentlicher Faktor bei der weiteren Entwicklung.

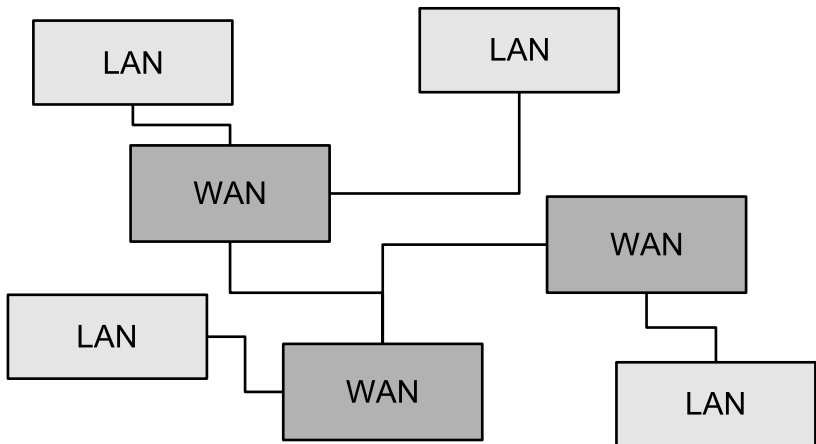
Knapp vier Jahre später waren bereits zahlreiche weitere Einrichtungen an das Netz angeschlossen. Es existierten schon grundlegende Protokolle, die als Basis für Anwendungen dienten, aber vom *Internet* war damals immer noch nicht die Rede. Ein Meilenstein war der Entwurf von TCP (*Transmission Control Protocol*) im Jahre 1973 von Vint Cerf und Bob Kahn mit dem Anspruch, das Arpanet und andere Netze miteinander verbinden zu können. Hieraus entstand der Gedanke des Internets – ein Begriff der nichts anderes ist als die Abkürzung des englischen Begriffes

*In diesem Zusammenhang ist übrigens anzumerken, dass der häufig zitierte (angebliche) Auftrag des ARPANET, im Falle eines Atomkriegs die Kommunikation sicherzustellen, nichts als ein Mythos ist.*

*Interconnection Network*, also ein großes Netzwerk, das aus kleineren zusammengesetzt ist.

TCP wurde in den folgenden Jahren noch mehrmals modifiziert; 1978 wurden die Bestandteile funktional getrennt: Es entstanden TCP/IP und UDP/IP (beziehungsweise allgemein auch nur als TCP und UDP (*User Datagram Protocol*) bezeichnet. TCP und UDP arbeiten beide auf der Basis des *Internet Protocol*, welches der gemeinsame Nenner für die Weiterleitung von Daten im Internet ist.

**Abbildung 1.1**  
Verbindungen  
zwischen Wide-Area-  
Netzwerken und  
Local-Area-  
Netzwerken bilden  
das Rückgrat des  
Internets.



Annähernd zwei Jahrzehnte nach dem Entwurf von TCP kam mit der Entwicklung des WWW oder *World Wide Web* der Durchbruch des Internets für den privaten Anwender. Mittlerweile ist WWW eine gemeinhin anerkannte Technologie zum Informationsaustausch, zur Präsentation, als Marktplatz für Supermarktketten, eine Plattform für Auktionshäuser und für viele andere Anbieter. Der Durchbruch des Internets als »Medium für alle« war eng verbunden mit einer besonderen Applikation – dem Webbrowser, der einen einfachen Weg für alle Altersgruppen und soziale Schichten bietet, sich die angebotene Informationsvielfalt im Internet zu erschließen. Immer mehr Anwendungsgebiete vereinen Anwender aus den unterschiedlichsten Berufen und Interessengebieten, was zur Folge hat, dass über das Internet mehr und mehr sensible Informationen und Daten transportiert werden.

Wie so oft gilt aber auch im Internet: Wo es Geld zu verdienen gibt, sind nicht nur gutmütige Gestalten unterwegs. Themen wie Angriffe auf Webserver, Viren und Würmer sind in aller Munde und belegen, dass das Internet nicht unbedingt ein sicheres Pflaster ist (mal abgesehen von den wirtschaftlichen Schäden, die

durch solche Gefahren und Angriffe entstehen). Darüber hinaus sind zahlreiche Möglichkeiten vorhanden, Datenverkehr mitzulesen und nach interessanten Informationen zu durchsuchen. Wundert es daher, dass in solch einem Umfeld Methoden erschaffen wurden, die den unbefugten Zugriff auf Daten nahezu unmöglich machen sollen?

## 1.1 VPNs von der Antike bis heute

Der Schutz von sensiblen Daten wäre heute ohne die Hilfsmittel der Kryptografie undenkbar. Die Kryptografie hat in der Geschichte der Menschheit eine lange Tradition. So ist heute bekannt, dass bereits die Ägypter verschlüsselte Botschaften in Hieroglyphen darstellten. Bei den Hebräern wurden Zeichenersetzungsverfahren verwendet und Gaius Julius Cäsar benutzte das nach ihm benannte *Caesar-Chiffre* zum (mehr oder weniger) sicheren Nachrichtenaustausch mit seinen Legionen. Im Mittelalter wurden mehr und mehr Geheimsprachen und Schriften eingesetzt, um diplomatische Post zu verschlüsseln. Und natürlich kann in diesem Zusammenhang auch nicht der obligatorische Verweis auf die *Enigma* fehlen, die im Zweiten Weltkrieg eine sichere Nachrichtenübermittlung gewährleisten sollte.

## 1.2 Eine sich ändernde Welt benötigt sichere Kommunikation

Während früher die Nachrichtengröße eher gering war und daher eine Nachricht mit vertretbarem Aufwand manuell ver- und entschlüsselt werden konnte, ist das Datenvolumen heute in der Regel viel größer und hat oft durchaus zeitkritische Randbedingungen. Konsequenterweise werden für solche komplexen Berechnungen »on the fly« leistungsstarke Computer oder sogar spezialisierte Geräte eingesetzt. Diese performanten Geräte sind erforderlich, da die Verbindung von Rechnern und Netzen an verschiedenen Standorten eine (nicht nur in der Industrie) bewährte Methode ist, strukturiert zu expandieren und die Kommunikationswege kurz und administrierbar zu halten. Zusätzlich hat sich eine Kultur etabliert, bei der die gemeinsame Nutzung von Dateien und der dezentrale Zugriff auf alle Arten von Informationen möglich ist.

Um die Kosten gering zu halten, soll in der Regel bei solchen Verbindungen auf bestehende Netze zurückgegriffen werden. So

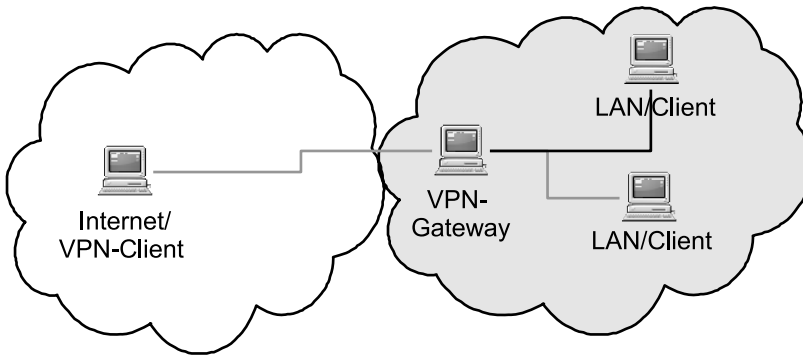
werden öffentliche Netze verwendet, um mit deren Infrastruktur eine weltweite Expansion zu ermöglichen oder aber auch um den immer beliebter werdenden Trend der Heimarbeit zu unterstützen. Das darüber realisierte Netzwerk ist der Nabel, ohne den Mitarbeiter und sogar ganze Unternehmensteile nicht miteinander arbeiten können.

Mit der Einführung von virtuellen privaten Netzen (VPNs) werden solch sensible Verbindungen geschützt. VPNs verbinden nicht nur einzelne Rechner über *VPN-Gateways* mit Servern, sondern auch ganze Netzwerke mit anderen Netzwerken. Jedoch wird die Sicherheit von IP-basierten Netzen immer wieder durch neue Meldungen über Würmer, Viren, *Denial-of-Service-(DoS-)*Attacken und virtuellen Einbrüchen widerlegt. Für VPNs bedeutet das, dass sie Kriterien des Datenschutzes, der Validierung der Verbindung bis hin zur Verifikation einzelner Datenpakete erfüllen müssen. Die Bedrohung durch Würmer und Viren hat vor allem durch eine vorherrschende Monokultur bei dem Einsatz von Betriebssystemen zugenommen. Durch die (welt-)weite Verbreitung von Microsoft Windows fällt es Autoren von Schädlingen leicht, mit einem kompromittierenden Programm ganze Netzwerke in ihre Gewalt zu bringen. Diesem sportlichen Ehrgeiz folgt als weitere Disziplin die Zerstörung von Serviceverfügbarkeit. Dabei kann es sich um die mutwillige Unterbrechung von bestehenden Verbindungen handeln, es kann aber auch heißen, dass ein Rechner oder Softwareservice erst gar nicht nutzbar ist. Bekannte Beispiele gibt es immer wieder: So hat im Mai 2004 der Computerwurm *Sasser* weltweit Millionen Rechner infiziert und als Symptom den Computer neu gebootet.

Der Einbruch in Rechner und Rechnernetze ist für die Aggressoren eine lukrative Arbeit, denn durch die professionelle Bereitstellung und Vermarktung von Zugangsdaten und Rechenleistung innerhalb dieser Szene wird jedes System interessant, das Teil eines öffentlichen Netzes ist. Dieser nachgewiesene Umstand veranlasst Programmierer aus allen Ländern die Grenze der Legalität zu überschreiten: angefangen beim Diebstahl von Kreditkartendaten, Zugangsdaten für E-Mail-Konten bis hin zu firmeninternen Dokumenten.

Um dem Ruf nach dem Schutz privater Daten bei der Übertragung durch öffentliche Netze nachzukommen, haben verschiedene Hersteller und Organisationen Lösungen entwickelt, die in der Lage waren, das Vertrauen der Anwender zu erhalten oder zurückzugewinnen. Von den zahlreichen technischen Lösungen sind die folgenden am meisten verbreitet:

*Um hier etwas  
klarzustellen: Es gibt  
natürlich auch  
Schädlinge für andere  
Betriebssysteme!*



**Abbildung 1.2**  
VPN-Gateways sind der gesicherte Netzübergang aus dem Internet in ein lokales Netzwerk.

- ❑ **L2TP** Das *Layer 2 Tunneling Protocol* ist ein Tunnelprotokoll, welches, wie der Name verrät, auf OSI-Schicht 2 arbeitet. Mit Hilfe einer Tunnel-ID ist es möglich, mehrere Verbindungen nebeneinander zu identifizieren und aufzubauen. L2TP sieht grundsätzlich keine Verschlüsselung vor und sollte deshalb nicht verwendet werden. Authentifizierungsmethoden sind PAP (Password Authentication Protocol) und CHAP (Challenge Handshake Authentication Protocol).
- ❑ **PPTP** Das *Point-to-Point Tunneling Protocol* trat in den letzten Jahren als weit verbreiteter Vorgänger zu L2TP auf. Da es bei dieser TCP-basierten Verbindung jedoch einige kritische Sicherheitslücken gab, lieferten Hersteller immer wieder bereinigte Versionen aus. Die große Schwachstelle, dass die Verschlüsselungstiefe von der Länge des Passworts abhängt, konnte jedoch nie geschlossen werden.
- ❑ **IPsec**, eine Abkürzung für *IP security*, hat es sich zur Aufgabe gemacht, das unsichere Internetprotokoll (IP) zu schützen und die zu transportierenden Daten zu validieren. Dazu bietet es verschiedene Arten der Authentifizierung von Benutzern und Clients. Aufgrund der offenen Standardisierung hat sich IPsec in den vergangenen Jahren zum Marktführer bei VPNs entwickelt und wird auch von zahlreichen Herstellern im Security-Umfeld unterstützt. Allerdings beinhaltet IPsec auch eine gewisse Komplexität, weswegen es bei unbedarften Anwendern häufig zu Problemen führen kann.
- ❑ **SSL-VPNs** sind der aktuelle Trend bei den Herstellern von VPN-Produkten. Es lässt sich am Markt sehr gut beobachten, dass mittlerweile auch die klassischen Hersteller von IPsec-Geräten in dieser Kategorie Geräte im Portfolio haben. SSL-VPNs verwenden das TLS/SSL-Protokoll, um Da-

ten zu verschlüsseln. Die Verbindungen sind im ISO/OSI-Referenzmodell über der Transportschicht und unterhalb der Anwendungsschicht angesiedelt. SSL-VPNs arbeiten üblicherweise mit TCP-Port 443 (wie der allseits bekannte Zugriff über `https`) und können unterschiedliche Ausprägungen besitzen: Vom Portal über Proxy-basierten Access bis hin zum transparenten Tunnel ist so ziemlich alles zu finden.

- ❑ OpenVPN ist ein sehr verbreiteter Vertreter der SSL-VPNs und kann wahlweise über UDP oder TCP eingesetzt werden. Für die SSL-Verschlüsselung wird die OpenSSL-Bibliothek verwendet. Durch die Lizenzierung als OpenSource-Software und die Verfügbarkeit auf unterschiedlichen Betriebssystemen findet OpenVPN mit allen Vorteilen einer SSL-basierten VPN-Lösung immer mehr Akzeptanz und Einsatzgebiete. Zur Authentifizierung bieten sich *Preshared Keys* oder *Zertifikate* an.
- ❑ CIPE Mit dem Anspruch, einen einfach zu verwendenden VPN-Ansatz zu implementieren, ist *Crypto IP Encapsulation* eine Technologie, die meist komplett im Betriebssystemkern eingebettet ist. Anwendungen, die auf ein VPN zugreifen, senden und empfangen Daten über eine virtuelle CIPE-Schnittstelle. Hinter dieser Schnittstelle werden die Daten in UDP-Paketen über ein bestehendes Netzwerk verschickt. CIPE hat den Vorteil, in NAT-Umgebungen eingesetzt werden zu können.

NAT: Network Address  
Translation

Um die genannten Technologien (im Allgemeinen) und natürlich OpenVPN (im Speziellen) einschätzen zu können, sind die folgenden Kapitel des Buches in drei Teile untergliedert:

- ❑ *Teil I* umschließt die Kapitel 2 bis 4 und betrachtet allgemeine Gesichtspunkte, die beim Thema VPN von Interesse sind.
- ❑ In *Teil II* geht es um die grundlegenden Bausteine bei OpenVPN und wie sie miteinander verwoben sind. Dieser Teil umfasst die Kapitel 5 bis 9.
- ❑ Der abschließende *Teil III* stellt weiter gehende Funktionen und Möglichkeiten vor und zeigt anhand zahlreicher Beispiele die Einsatzmöglichkeiten auf.