Virtual Private Networks

Dr. Markus a Campo, Dr. Norbert Pohlmann

Virtual Private Networks

2., aktualisierte Auflage

Bibliografische Information Der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.ddb.de> abrufbar.

ISBN 3-8266-0882-8
2., aktualisierte Auflage 2003

Printed in Germany

ein Geschäftsbereich der verlag moderne industrie Buch AG & CO. KG/Landsberg

Redaktion und Lektorat: Norbert Schwob, Aachen
Grafiken: Sabine Schmidt, Aachen
Satz: reemers publishing services gmbh, Krefeld
Druck: Media-Print, Paderborn

Über die Autoren

Markus a Campo studierte Elektrotechnik mit dem Schwerpunkt Technische Informatik an der RWTH Aachen. Von 1985 bis 1991 arbeitete er am Rogowski-Institut der RWTH im Bereich der Entwicklung neuartiger Robotersteuerungen. Er promovierte dort über ein System zur Echtzeit-Kollisionsvermeidung. Während seiner anschließenden mehrjährigen Anstellung in einem großen Industrieunternehmen beschäftigte er sich mit den Problemen der Kommunikation in verteilten Systemen zur Produktionsautomatisierung.

Seit 1997 arbeitet Markus a Campo freiberuflich auf dem Gebiet der Netzwerksicherheit. Er gilt als allgemein anerkannter Spezialist, der die relevanten Angriffs-, Abwehr- und Analysetools kennt und anwendet. Im Auftrag von Unternehmen untersucht er deren Netzwerke, evaluiert das Sicherheitsniveau und offenbart bestehende Sicherheitslücken. Anschließend erarbeitet er Konzepte, um die Netzwerk-Infrastruktur abzusichern.

Markus a Campo ist Hauptautor des Loseblattwerks »Organisationshandbuch Netzwerksicherheit« (INTEREST-Verlag, Herausgeber: Norbert Pohlmann) und Chefredakteur des dazugehörenden Security-Newsletters. Außerdem veröffentlicht er Beiträge in Fachzeitschriften zum Thema IT-Sicherheit und arbeitet als Buchautor sowie Schulungsreferent. Seine Themen sind: Netzwerksicherheit im Allgemeinen, Security Audits, Firewall-Systeme, Intrusion Detection-Systeme und Virtual Private Networks.

Dr.-Ing. Markus a Campo mail@ m-acampo.de
Försterstraße 25 www.m-acampo.de
52072 Aachen

Norbert Pohlmann studierte Elektrotechnik mit dem Schwerpunkt Informatik. Von 1997 bis 2001 arbeitete er an seiner Dissertation zum Thema »Möglichkeiten und Grenzen von Firewall-Systemen«. Er war von 1985 bis 1988 Forschungsingenieur und später Leiter des Labors für Telematik an der Fachhochschule Aachen, in dem viele Forschungs- und Entwicklungsprojekte durchgeführt wurden, die sich mit der Einbindung von Sicherheitsmechanismen in IT-Systemen beschäftigten.

1988 gründete Norbert Pohlmann zusammen mit Professor Dr. Christoph Ruland das Unternehmen KryptoKom, Gesellschaft für kryptographische Informationssicherheit und Kommunikationstechnologie mbH, in Aachen. Das international

tätige Systemhaus (Hardware, Software, Dienstleistungen, Consulting) expandierte rasch, wurde in vielen Bereichen der IT-Sicherheit Marktführer im deutschsprachigen Raum und beschäftigte 1998 mehr als hundert Mitarbeiter. Am 1. Juli 1999 fusionierte die KryptoKom GmbH mit der Utimaco Safeware AG in Oberursel; Norbert Pohlmann ist seit dem 1. Oktober 1999 Vorstandsmitglied der Utimaco Safeware AG.

Als Experte für Sicherheit in der IT-Sicherheit befasst sich Norbert Pohlmann bereits seit 1985 aktiv mit Kryptographie und ihren Anwendungsgebieten. Als Gründungsmitglied, seit 1994 Vorstandsmitglied und seit April 1998 Vorstandsvorsitzender von TeleTrusT e. V. hat er sich die Etablierung von vertrauenswürdigen IT-Systemen zur Aufgabe gemacht.

Mehrere Bücher und zahlreiche Fachartikel, Vorträge und Seminare zu Themen der Informationssicherheit dokumentieren seine Fachkompetenz und sein Engagement auf diesem Gebiet. Neben dem hiermit in der zweiten Auflage vorliegenden Fachbuch »Virtual Private Networks« ist im MITP-Verlag die inzwischen fünfte Auflage des Titels »Firewall-Systeme – Sicherheit für Internet und Intranet« verfügbar.

Norbert Pohlmann ist Träger des Preises der Stadt Aachen für Innovation und Technologie 1997 und wurde 1999 von der Zeitschrift 'IT.Services' als »Vordenker der deutschen Computerindustrie« ausgezeichnet.

Norbert Pohlmann ist Mitinitiator und Vorsitzender des Programmkomitees der »Information Security Solutions Europe«-Konferenzen (ISSE). Die erste Konferenz fand im Oktober 1999 statt. Die zweite ISSE wurde im September 2000 in Barcelona und die dritte im September 2001 in London erfolgreich durchgeführt. Die vierte ISSE fand im Oktober 2002 in Paris statt, die fünfte wird im Oktober 2003 in Wien stattfinden.

Dr. Norbert Pohlmann
Utimaco Safeware AG
Germanusstraße 4
52080 Aachen

norbert.pohlmann @ utimaco.de
www.utimaco.com

Inhaltsverzeichnis

Übersicht

Einleitung: Gesellschaftlicher Wandel und IT-Sicherheit

Die Einleitung zeigt anhand von »Meilensteinen« die Entwicklungssprünge von Kryptographie, Informationstechnologie und Informationssicherheit sowie die Vorteile der Internet- und Intranet-Technologie und die daraus folgenden gesellschaftlichen Veränderungen. Die Notwendigkeiten und Chancen von IT-Sicherheit werden erläutert und der VPN-Markt wird dargestellt (VPN: Virtual Private Network).

Notwendigkeiten, Ziele und Anwendungsformen von VPN-Systemen

Nach der Definition des Begriffs »VPN« verdeutlichen Analogien, dass die Sicherheitsmechanismen zur Absicherung von heutigen Geschäftsprozessen den neuen Bedingungen angepasst werden müssen. Die Sicherheitsziele, die mit einem VPN-System realisierbar sind, werden dargestellt, ferner die grundsätzlichen Anwendungsformen: unternehmensweites VPN, sichere Remote-Ankopplung, VPN zwischen verschiedenen Unternehmen und Kombinationen.

Bedrohungen aus dem Netz

Die Motive von Angreifern und die potenziellen Angriffe auf Kommunikationssysteme werden beschrieben und eine Abschätzung über Eintrittswahrscheinlichkeit und mögliche Schäden wird vorgenommen.

Grundlegende Sicherheitsmechanismen

Zuerst werden einige grundlegende Sicherheitsmechanismen beschrieben, mit denen Kryptographiekonzepte für VPN-Systeme aufgebaut werden können. Anschließend erfolgt die Beschreibung der eigentlichen kryptographischen Algorithmen und der zur Verwaltung von Schlüsseln benötigten Infrastruktur.

Konzepte von Virtual Private Networks

In diesem Kapitel werden verschiedene Konzepte beziehungsweise Topologien diskutiert, nach denen VPN-Systeme aufgebaut werden können, die zur Sicherstellung einer vertrauenswürdigen Kommunikation genutzt werden. Außerdem werden Aspekte des Sicherheitsmanagements beschrieben.

VPN-Verfahren

Um die drei Ziele einer vertrauenswürdigen Datenübertragung – Vertraulichkeit, Authentikation und Integrität – mit einem VPN zu realisieren, müssen eine Reihe von Überlegungen durchgeführt werden. Dieses Kapitel hilft beim Verständnis der Protokolle, die den vertrauenswürdigen Transport von Daten und den Austausch der Schlüssel durchführen.

Praktischer Einsatz von Virtual Private Networks (VPNs)

In diesem Kapitel wird zunächst anhand von Praxisbeispielen vorgestellt, wie verschiedene Unternehmen beziehungsweise Organisationen mit sehr unterschiedlichen Anforderungen Virtual Private Networks aufgebaut haben, um eine vertrauenswürdige Kommunikation gewährleisten zu können. Im Anschluss werden praktische Hinweise zur Implementierung von VPN-Systemen gegeben und die prinzipielle Vorgehensweise bei der Konfiguration am Beispiel zweier gängiger VPN-Lösungen wird erläutert.

VPNs für E- und M-Business

Öffentliche Netze wie das Internet und die Mobilfunknetze haben eine zentrale Bedeutung im Leben jedes Einzelnen gewonnen. Die Stichworte »E-Business« und »M-Business« stehen für die neue Flexibilität bei der Abwicklung von Geschäften wie Einkäufen, Reisebuchungen und Bankgeschäften. »E-Business« bezeichnet ganz allgemein die Abwicklung von geschäftlichen Transaktionen über öffentliche Netzwerke, »M-Business« ihre Abwicklung über das Mobilfunknetz. Das Kapitel beschreibt, wie in Zukunft mithilfe von VPNs auch für diese Anwendungen sichere Verbindungen geschaffen werden können.

VPN-Sicherheitspolitik und weitere Sicherheitsmaßnahmen

In diesem Kapitel wird erläutert, welche Aspekte bei der Erarbeitung einer VPN-Sicherheitspolitik berücksichtigt werden müssen und welche infrastrukturellen, organisatorischen und personellen Sicherheitsmaßnahmen ein VPN-System ergänzen müssen, damit ein hohes Maß an Gesamtsicherheit erreicht werden kann.

VPN: Eine Investition für die Zukunft

In diesem Kapitel werden die Kosten eines VPN-Systems aus unterschiedlichen Blickwinkeln betrachtet. Da ein VPN-System eine Investition für die Zukunft ist, sollten die Kosten-Nutzen-Aspekte schon bei der Planung besonders berücksichtigt werden.

Evaluierung und Zertifizierung von VPNs

Vor der Anschaffung eines VPNs stellt sich Kunden und Benutzern die Frage, welche Sicherheitskriterien wirklich erfüllt werden. Mit dem Mittel der Evaluation kann überprüft werden, ob angegebene Sicherheitsfunktionalitäten tatsächlich vorhanden sind und ihre Funktion korrekt erfüllen. Ziel der Evaluierung ist, dem Anwender des Sicherheitssystems das Vertrauen zu geben, dass das VPN-System ordnungsgemäß und wunschgemäß arbeitet.

VPN-Systeme versus Firewall-Systeme

Der Sicherheitsmechanismus Verschlüsselung bei VPN-Systemen wirkt nur gegen die unerlaubte Einsicht der Informationen während der Kommunikation per Internet. Zusätzlich muss noch mithilfe von Firewall-Systemen das zweite Hauptrisiko beim Anschluss an das Internet, der unerlaubte Zugriff auf die eigenen Rechnersysteme, verhindert werden. Das Kapitel beschreibt neben der Grundidee von Firewall-Systemen deren verschiedene Elemente: Wie können damit technische Sicherheitsmechanismen realisiert werden und welche konkreten Möglichkeiten bestehen, Sicherheit zu gewährleisten?

Weiterführende Aufgabenstellungen

In diesem Kapitel werden einige weiterführende Aufgabenstellungen behandelt, die mit dem Betrieb von VPN-Systemen verbunden sind. Dazu gehören die Verfügbarkeit der Netzwerkdienste, Konzepte von Redundanzsystemen, mögliche Realisierungsformen von VPN-Gateways (im Router integriert oder als separate Sicherheitskomponenten), Hilfsmechanismen für die Verwaltung großer VPN-Netzwerke sowie ein Ausblick auf die zukünftige Entwicklung bei VPN-Systemen.

Anhang

- Recht im Internet
- Computerkriminalität – Fakten und Zahlen
- TCP/IP-Technologie für Internet und Intranet
- eine Liste der auf dem Markt vertretenen VPN-Anbieter
- wichtige Adressen und Web-Links
- Literaturverzeichnis
- Glossar mit Abkürzungen
- die Legende für die Symbole, die im Buch verwendet werden
- Stichwortverzeichnis

Vorwort

Der gegenwärtige Wandel zur Informations- und Wissensgesellschaft verändert unser Leben – und damit auch das Wirtschaftsleben – tief greifend. Die »elektronische Geschäftswelt« bietet uns neue Chancen, denen jedoch, ähnlich wie in der »traditionellen Geschäftswelt«, bestimmte Risiken gegenüberstehen.

In der »traditionellen Geschäftswelt« haben wir im Laufe der Zeit gelernt, diese Risiken einzuschätzen und uns angemessen dagegen zu schützen: Schutzmechanismen wie Pförtner, Safes und gepanzerte Werttransporter, aber auch Ausweise, Briefumschläge und die eigenhändige Unterschrift gewährleisten zwar keine hundertprozentige Sicherheit, aber sie helfen, das Risiko auf ein kalkulierbares Maß zu begrenzen.

Entsprechende Mechanismen benötigen wir auch in der »elektronischen Geschäftswelt«. Damit wir die Möglichkeiten, die uns die Kommunikation über das Internet bietet, erfolgreich nutzen können, müssen die grundlegenden Sicherheitsanforderungen – *Vertraulichkeit, Authentizität, Integrität* und *Nachweisbarkeit* von Datenübertragungen – erfüllt werden.

Diese Notwendigkeit wird um so deutlicher, wenn wir den immer weiter steigenden Wert elektronischer Informationen in Betracht ziehen. Immer mehr Daten, die erhebliche finanzielle Werte darstellen, werden durch Netze übertragen oder auf Rechnersystemen gespeichert. Dazu gehören Entwicklungsunterlagen, Kundendaten, Logistikinformationen oder auch Strategiekonzepte, die möglicherweise Börsenwerte beeinflussen können. Die Bits und Bytes solcher Informationen können leicht mehrere Millionen Euro wert sein.

Hinzu kommt, dass die gegenwärtige, national begrenzte Gesetzgebung im weltweiten Internet keinen angemessenen Schutz bieten kann. Es wird sicher noch Jahre dauern, bis internationale Gesetze – z. B. im Rahmen der G8-Bemühungen – erlassen werden. Bis dahin müssen Unternehmen und Organisationen sich mit geeigneten IT-Sicherheitsmaßnahmen selbst gegen die Gefahren der »elektronischen Welt« schützen.

Ein Beispiel für solche Sicherheitsmaßnahmen sind *Virtual Private Networks (VPNs)*, mit denen unsichere Netze wie das Internet als vertrauenswürdige Kommunikationswege genutzt werden können – ähnlich wie auch das Straßennetz von gesicherten Geldtransportern befahren wird.

Unter dem Begriff »VPN« werden Hard- und Software-Lösungen zusammengefasst, die sich in ihren Einsatzgebieten und ihrer technischen Realisierung deutlich unterscheiden. Dieses Fachbuch soll zur Klärung des Begriffs beitragen und stellt die grundlegenden Konzepte von VPN-Systemen dar. Als praxisorientierter Leitfaden erläutert es verschiedene Einsatzmöglichkeiten von VPNs und bietet den Lesern Hilfestellungen zur Wirtschaftlichkeitsberechnung, zur Definition einer VPN-Sicherheitspolitik sowie zu Beschaffung, Instandhaltung und Betrieb von VPN-Systemen.

Für die zweite Auflage wurde das Buch erneut durchgesehen und an verschiedenen Stellen aktualisiert oder ergänzt.

Unser Dank gilt den VPN-Spezialisten der Compumatica secure networks GmbH. Unsere Leser sind weiterhin gerne eingeladen, Fragen zu stellen und Anregungen zu geben. Sie erreichen uns dazu per E-Mail unter:

Dr.-Ing. Markus a Campo: mail@m-acampo.de

Dr. Norbert Pohlmann: norbert.pohlmann@utimaco.de

Kapitel 1

Einleitung: Gesellschaftlicher Wandel und IT-Sicherheit

Dieses Buch beschäftigt sich mit Sicherheitslösungen, die vor Bedrohungen in unsicheren Netzen wie dem Internet schützen. IT-Sicherheit ist dabei nicht allein eine technisch-organisatorische Aufgabe, sondern steht im gesellschaftspolitischen Zusammenhang. Deshalb beginnt dieses Kapitel mit einem kurzen historischen Überblick.

1.1 Entwicklung von Informationstechnologie und IT-Sicherheit

Schon immer hatte der technologische Fortschritt Einfluss auf alle Bereiche der Gesellschaft. Wasserleitungen machten einerseits Wasserträger brotlos, ermöglichten andererseits erst die Siedlungsform Großstadt. Der Traktor verdrängte das Pferd, die elektrische Schreibmaschine die mechanische und so fort. Die Agrargesellschaft wurde in Europa durch die Industriegesellschaft abgelöst, Triebfedern waren Stahl, Kohle und Dampfkraft, später Erdöl und Elektrizität.

Mit Energie, Maschinen, menschlicher Arbeitskraft und Intelligenz wurde zunehmend mehr Materie formbar. Mit hoher Eigendynamik bildeten sich neue Lebensumgebungen; Mobilität für Güter und Menschen beschleunigte die Entwicklung, Handwerk und Wissenschaften organisierten sich.

Durch den Buchdruck wurde Wissen verteilbar, durch die Nachrichtentechnik körperlos (elektronisch) übermittelbar und schließlich – nun »Information« genannt – durch die Informationstechnik »prozessierbar«.

Gegenwärtig erleben wir den *Wandel zur Informations- und Kommunikationsgesellschaft*. Die dazu gehörenden Technologien sind die Schlüsseltechnologien für unsere Arbeits- und Lebenswelt von heute und morgen.

Meilensteine der Kryptographie bis zum II. Weltkrieg

1900 v. Chr.	Ägyptische Schreiber benutzten spezielle Hieroglyphen zur Verschlüsselung von Nachrichten; später wurde in Palästina ein »umgekehrtes Alphabet« zur Kodierung verwendet.
50-60 v. Chr.	Julius Caesar verwendete eine einfache Verschiebesubstitution von Buchstaben für vertrauliche Regierungskommunikation. Er ersetzte jedes A durch ein D, jedes B durch ein E usw. Nur wer die einfache Regel »Verschiebung um drei Buchstaben« kannte, konnte die Nachrichten entziffern.
1518	Johannes Trithemius schrieb das erste Buch zur Kryptographie.
1586	Maria Stuart wurde das prominente Opfer einer unzureichend verschlüsselten Nachricht
1660	Leon Batista Alberti konstruierte die erste Verschlüsselungsmaschine.
1917	Gilbert S. Vernam erfand bei AT&T in den USA eine praxistaugliche polyalphabetische Chiffriermaschine, die einen absolut zufälligen und niemals wiederholten Schlüssel verwendete. Dies war die erste beweisbar sichere Verschlüsselungsmaschine.
1918	Der deutsche Ingenieur Arthur Scherbius meldete das Rotorprinzip für Chiffriermaschinen zum Patent an und gründete 1923 die »Chiffriermaschinen Aktiengesellschaft« für Herstellung und Verkauf seiner ENIGMA. Die nach dem griechischen Wort für »Rätsel« benannte Maschine war für die vertrauliche Übertragung von geschäftlichen Mitteilungen und Telegrammen vorgesehen, war aber zunächst kein kommerzieller Erfolg. Später wurde sie in verbesserter Form zu Zehntausenden als Standard-Verschlüsselungsautomat bei Militär und diplomatischem Dienst eingesetzt.

Leser, die sich für die detaillierte Geschichte der Kryptographie interessieren, finden in David Kahns 1200-seitigen Standardwerk »The Code-Breakers« ausführliche Informationen /Kahn97/.

Die effiziente Verbindung von Kodierung und Prozessierbarkeit belegt ein schreckliches Beispiel: Datenbanksysteme mit IBM-Hollerith-Lochkarten lieferten dem Nazi-Regime die Informationsstruktur für Völkermord, von der Volkszählung 1939 über DV-gestützte Selektion nach »Rassemerkmalen« bis zur »Verwaltung« des Holocaust /Black2001/.

Entwicklung der Informationstechnik und -sicherheit seit 1938:

- Konrad Zuse entwickelte 1938 den ersten mechanischen Ziffernrechner »Z1«. Im II. Weltkrieg konnten die Briten mit einem Röhrenrechner die bis dahin als sicher geltende Verschlüsselung der deutschen mechanischen ENIGMA-Apparate brechen und gewannen den passiven Zugang zu dem weltweiten Funknetz. 1948 legte Claude E. Shannon mit dem »Bit« (Kürzel aus binary digit) als kleinste Dateneinheit den Grundstein für die Informationstheorie.
- Nach 1950 begann der Siegeszug des Transistors, der die langsame, anfällige, voluminöse und energiefressende Röhrentechnik ablöste. »Silicon, the new steel« lautete schließlich das Credo, als lochkartengespeiste Großrechneranlagen seinerzeit unglaubliche Datenmengen verarbeiteten. Als sich damals die Frage der Sicherheit stellte, wurde sie räumlich (Zugangsregelungen zum Rechenzentrum) und administrativ (Aufgabenteilung: Systemadministrator, Anwender, Daten-Eingabekraft) geregelt.
- Seit den 60er Jahren wurden, ausgehend von den USA, Terminals an Großrechner angeschlossen und der Siegeszug der Vernetzung begann. Die IT-Sicherheit hatte endgültig ihre räumliche Abgeschlossenheit verloren. Das ISO-Referenzmodell, TCP/IP-Technologie und Ethernet-Topologie wurden entwickelt; bald gab es dezentrale militärische Netze und Firmennetze wie SNA, DEC-Net und das globale IBM-Netz. 1973 entstand das Arpanet als Vorläufer des Internet, dieses wurde 1991 »öffentlich«, und mit dem World Wide Web begann das Online-Zeitalter.
- Parallel zur Entwicklung der Informationstechnologie entwickelte sich die Kryptographie. Wichtige Algorithmen entstanden, unter anderem 1976 der US Data Encryption Standard (DES), 1977 RSA, 1990 IDEA und 1991 Phil Zimmermanns Verschlüsslungssoftware PGP.
- Ein Technologiesprung aus dem Silicon Valley brachte den (Home-)PC mit eigenem Betriebssystem und schnellem Prozessorboard, immer größeren Festplatten, Floppy-Disk- und später ZIP-, CD- und DVD-Laufwerken zum Datenaustausch. Die Datenträger waren mobil, durch Miniaturisierung wurden es dann auch die Computer selbst (Laptops und Palmtops). Immer preiswertere und leistungsfähigere PCs ermöglichten die Integration von Audio und Video. Inzwischen besitzt in den Industrienationen ein erheblicher Teil der Bevölkerung einen eigenen Multimedia-PC, oft mit zahlreichen Peripheriegeräten (Scanner, Drucker etc.). Firmen wie Privatleute rüsteten ihre PCs mit Modems für den Zugang zu Mailboxen und später zu Online-Diensten über das Telefonnetz aus.
- Die Frage der IT-Sicherheit wurde zunächst viel zu einseitig auf den Bereich »Computerviren« bezogen. Dabei gedieh im Verborgenen längst der Datenmissbrauch. In Deutschland wird seit 1987 der Bereich Computerkriminalität von der Polizei eigenständig erfasst (siehe Anhang A).

1.2 Siegeszug des Internet

In den letzten Jahren hat sich das Internet als universales, bidirektionales und globales Kommunikationsmedium etabliert. Das »Netz der Netze« ist unabhängig von den räumlichen und zeitlichen Begrenzungen, die den Informationsfluss über die klassischen Print- und Rundfunkmedien einengen.

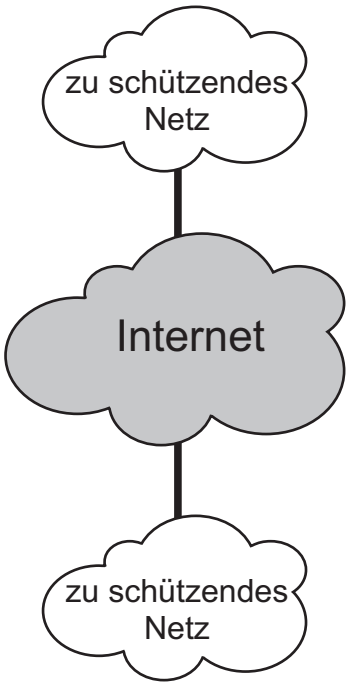


Abb. 1.1: Kommunikation über das Internet

Merkmale des Internet als das globale Datennetz:

- Einfacher und kostengünstiger Zugang
  Vom Notebook über PCs und Workstations bis zum Großrechner kann jeder Computer einfach und kostengünstig angeschlossen werden .
- Einheitlicher Standard
  Es gibt keine länderspezifischen Besonderheiten wie bei X.25-Netzen oder ISDN, denn die TCP/IP-Technologie ist netzunabhängig und für alle Betriebssysteme verfügbar.
- Weltweites Netz, shared infrastructure
  Hunderttausende Netzwerke verbinden über 100 Millionen angeschlossene Rechnersysteme in mehr als 240 Ländern. In praktisch allen Ländern der Welt

kann man über das Telefonnetz Zugangsrechner von Online-Diensten wie AOL, CompuServe und T-Online anwählen oder sich über Internet-Provider wie EUnet, MAZ und DFN direkt an das Internet anschließen.

- Steigende Akzeptanz
  Ende 2001 nutzten schätzungsweise 500 Millionen Menschen weltweit das Internet. Die Zuwachsrate ist weiterhin hoch, denn selbst in den Vereinigten Staaten haben lediglich knapp über 50 % der Haushalte einen Internet-Anschluss, in Deutschland sogar erst knapp über 25 %. Daraus kann man jedoch nicht ohne weiteres auf die Anzahl der Internetnutzer schließen, da zum einen eine erhebliche Zahl von Personen einen Internetzugang am Arbeits- oder Ausbildungsplatz hat und zum anderen die Nutzung eines Internet-Anschlusses durch mehrere Personen nur schwer abzuschätzen ist.

  Es ist zu erwarten, dass die Internetnutzung in diesem Jahrzehnt genauso alltäglich wird wie die Nutzung des Telefons und neuerdings des Mobiltelefons. Das Karlsruher Fraunhofer Institut für Systemtechnik und Innovationsforschung (ISI) berichtete im August 1998, dass nur 7 % der Internetnutzer in Deutschland aus der Arbeiterschicht kommen, was zeigt, dass starke gesellschaftliche Ungleichgewichte bestehen. Andererseits zeigt dies auch, dass das Potenzial hoch ist, denn in den nächsten Jahren werden sich die Unterschiede weiter angleichen. So berichtet die Gesellschaft für Konsumforschung (GfK) in Nürnberg, dass zwischen Ende 1997 und März 2001 der Anteil von Frauen unter den deutschen Internetnutzern von 29 % auf 42 % gestiegen ist.

  Ein neues gesellschaftliches Phänomen ist übrigens die Internetsucht, siehe »Münchener Ambulanz für Internet-Abhängige«:
  `www.psychiater.org/Internetsucht/ambulanz2.htm`.

- Extranet, Intranet
  Unternehmensweite *Intranets* können über das Internet zu einem *Extranet* verbunden werden. Das Extranet ist damit Teil des globalen Kommunikationssystems.

- Günstig für internationale Geschäftsbeziehungen
  Mitarbeiter eines Unternehmens, zum Beispiel im Vertrieb, greifen aus allen Ländern der Welt über das Internet auf die Rechnersysteme der Zentrale zu. Die Vorteile liegen auf der Hand: Preise, Lieferzeiten, neue Informationen können schnell abgerufen und Bestellungen sofort übermittelt und bearbeitet werden. Es gibt keinen Medienbruch, die Informationen müssen nur einmal eingegeben werden. Dies ermöglicht die effiziente Abwicklung immer komplexer werdender Aufgaben.

1.3 Allgemeine Bedrohungen aus dem Internet

In den letzten Jahren hat sich die Moral der Hacker gewandelt: Früher waren Hacker Tüftler, die aus Spaß an der Sache oder um ihr Können unter Beweis zu stellen, in fremde Datenbanken einbrachen und sich einen Jux erlaubten, der dem Betroffenen allenfalls einen Schreck einjagte oder ihn ärgerlicherweise teure Arbeitszeit kostete.

Heute agieren sie professionell und organisiert als Cracker – was nicht weiter verwunderlich ist, wenn man bedenkt, wie viel Gewinn sich mit den Daten und Informationen erzielen lässt, die in Netzen kursieren. Dabei haben die meisten Cracker kein Unrechtsbewusstsein und keine Moralvorstellung.

Obwohl viele Fälle von Computerkriminalität und Spionage bekannt geworden sind und die dadurch entstehenden Schäden in Milliardenbeträgen gerechnet werden (siehe Anhang A), wurde das Thema Sicherheit lange unterschätzt und sorglos übergangen. Die Schnelligkeit und die Informationsvorteile der Kommunikationsnetze werden genutzt, ohne dass man sich – bildlich gesprochen – um Sicherheitsgurte, Knautschzone und Airbag kümmert.

Der Missbrauch von Kommunikationsnetzen ist bereits heute ein großes Problem. Hinter mancher Hackergeschichte in der Presse verbirgt sich vielleicht eine Legende – das darf aber nicht darüber hinwegtäuschen, dass die Frage der Sicherheit vermutlich noch brisanter ist, als die bisher bekannt gewordenen Fälle von Einbrüchen und Missbrauch nahe legen.

Cracker und ihre Methoden werden immer erfindungsreicher, zumal die Beute, um die es geht, immer lohnender wird. Anders als bei einem Bankraub in der realen Welt ist das Risiko für Cracker nicht allzu groß, denn sie sind nur schwer zu verfolgen. Sind die Einbrecher erst einmal im System, ist es fast unmöglich, sich an ihre Fersen zu heften. Noch leichter ist es, Daten während der ungeschützten Übertragung durch das Internet »abzufangen« – die Möglichkeit besteht an fast jedem beliebigen Netzknoten, und die Wahrscheinlichkeit, dass ein solcher Angriff auf die Kommunikationsbeziehung überhaupt bemerkt wird, ist gering.

1.4 Notwendigkeit von IT-Sicherheit

Wozu brauchen wir Sicherheit in der Informationstechnik?

Ein moderner Arbeitsplatzrechner hat heute die gleiche Leistungsfähigkeit wie ein klassisches Rechenzentrum vor einigen Jahren. Bei diesen Rechenzentren genügten noch Sicherheitsmaßnahmen, die mit Hilfe von organisatorischen und personellen Regelungen durchgeführt wurden. Dazu gehörten unter anderem

- Zugangskontrolle zu den Gebäuden und Räumen der Rechenzentren
- kontrollierte und definierte Arbeitsabläufe und eine dementsprechende Auftragsabwicklung
- Trennung zwischen dem Personal der Fachabteilung (den Anwendern) und den DV-Mitarbeitern (Programmierern, Operateuren usw.)

Die EDV stand abgeschottet in einem Gebäude, wodurch die externen Bedrohungen überschaubar waren, und das Betriebssystem des Hosts war für den Schutz der Ressourcen vor unerlaubtem Zugriff zuständig.

Durch moderne informationstechnische Konzepte wie Client-Server-Verbindungen, Down-Sizing, Out-Sourcing, Internet, Intranet usw., in denen Informationen über ein angreifbares Netz ausgetauscht werden, verlassen Daten die »geschützte Umgebung« und sind damit neuen Gefahren ausgesetzt.

Die heutigen verteilten Rechnersysteme mit ihren »offenen« Verbindungen lassen sich nicht mehr allein durch organisatorische Maßnahmen schützen. Es müssen zusätzliche *technische Sicherheitsmechanismen* bereitgestellt werden, die eine sichere und kontrollierbare Informationsübertragung und -verarbeitung ermöglichen. Dazu sind strategische Sicherheitskonzepte notwendig, die *Vertraulichkeit und Integrität* der per Netzwerk übermittelten Daten gewährleisten. Außerdem müssen Verbindlichkeit und Zurechenbarkeit der Vorgänge und Veranlassungen – wo immer notwendig – garantiert werden.

Welche Rolle spielt IT-Sicherheit in der Informationsgesellschaft?

In den letzten Jahren hat sich der Wert der Informationen und damit der Schutzbedarf beträchtlich vergrößert.

Der steigende Wert von Informationen ist ein wichtiger, wenn nicht der wichtigste Wirtschaftsfaktor geworden. Beispiele sind:

- Vollständige Entwicklungs- und Fertigungsunterlagen: Manche Organisationen besitzen Hardware im Wert von 5000 EUR, auf der Informationen im Millionenwert gespeichert sind.
- Geschäfts- und Betriebsergebnisse, Strategiepläne: Wenn solche Ergebnisse oder Pläne der Öffentlichkeit bekannt werden, können damit beispielsweise Börsen-Aktivitäten in Bewegung gebracht werden, die wiederum hohe Verluste verursachen können.
- Logistikinformationen: Falls Daten nicht mehr verfügbar oder nicht mehr verlässlich sind, weiß kein Mitarbeiter mehr, wie groß der Lagerbestand ist, welche Kunden welche Produkte bestellt haben und wann an wen geliefert werden soll.
- Kundendaten: Diese stellen einen erheblichen Wert dar, den es zu schützen gilt.

Netzwerkstrukturen ermöglichen eine effiziente Abwicklung von Aufgaben, die in vielen Bereichen anders kaum noch zu erfüllen sind. Wir sind in solchem Ausmaß von Kommunikationssystemen abhängig, dass unsere wirtschaftliche Leistungsfähigkeit gefährdet ist, wenn die Funktionsfähigkeit der Systeme nicht in angemessener Weise gewährleistet werden kann.

Globale Ausdehnung und Veränderung der Geschäftsprozesse

Die meisten Geschäftsprozesse (Angebotserstellung, Auftragsannahme, Bestellung, Liefereingang) wurden in der Vergangenheit auf dem Papier oder persönlich bei Kundenbesuchen abgewickelt. Diese Abläufe können weitaus rationeller gestaltet werden, indem der personelle und materielle Aufwand durch elektronische Verfahren verringert wird. Geschäftsunterlagen können per Rechnersystem erstellt und elektronisch übertragen werden, so dass kein Medienbruch mehr auftritt.

Unsere Rechnersysteme und insbesondere die darauf verarbeiteten Informationen werden dadurch immer attraktiver für potenzielle Angreifer. Gleichzeitig kommt heute keine Behörde und kein Unternehmen mehr ohne die Verlagerung von Geschäftsprozessen und die Vernetzung von Rechnersystemen aus.

Einerseits möchte man leicht handhabbare und immer verfügbare Verbindungen nach außen haben. Andererseits müssen geschäftsinterne Daten und Beziehungen zu Geschäftspartnern vor Diebstahl, Manipulation und mutwilliger Zerstörung geschützt werden.

In Kaufhäusern sind Wachpersonal und Detektive, Videoüberwachung und stählerne Rollläden selbstverständlich. Aber erst in jüngster Zeit machen sich Organisationen Gedanken darüber, dass auch Daten vor unbefugtem Zugriff geschützt werden sollten, weil sie einen erheblichen Wert darstellen – oft sogar den Hauptanteil ihres Vermögens.

Die Informationstechnologie hat Möglichkeiten geschaffen, Wirtschaftsspionage bequem mit Rechnersystemen zu betreiben. Für diese neue Form der Spionage, bei der keine Wände eingerissen oder Tresore geknackt werden müssen, fehlt häufig jegliches Unrechtsbewusstsein der Täter, die ihre Arbeit vom Wohnzimmer aus erledigen. Die Tools für solche Aktivitäten sind auf dem Softwaremarkt oder im Internet frei erhältlich, ausführliche Informationen dazu gibt es in der Literatur und im Web.

Experten schätzen die wirtschaftlichen Schäden, die durch Computerkriminalität entstehen, bereits heute auf Milliardenbeträge – mit steigender Tendenz.

Staatliche Industrie- und Wirtschaftsspionage

IT-Kriminalität wächst mit dem Kommunikationsmöglichkeiten: Wirtschaftsspionage ist ein Hauptproblem im heutigen Business und hat seit Beendigung des Kalten Kriegs die militärische Spionage abgelöst. Dabei werden die wesentlichen Gefahren nicht mehr geographisch-politisch (westliche und östliche Staaten), sondern nach der Konkurrenzfähigkeit der Staaten eingeschätzt.

US-Präsident Bill Clinton erklärte »ökonomische Aufklärung« zum Staatsziel und stattete den »Supergeheimdienst« National Security Agency (NSA) mit entsprechenden Mitteln aus.

Die USA unterhalten mit einigen befreundeten Staaten das globale Echelon-System, um Kommunikation (per Telefon, Fax, DFÜ, Internet, ...) abzuhören und automatisiert auszuwerten. Bürgerrechtler verfolgen dies mit Sorge. Ein Zitat von `www.echelonwatch.org`:

> *»Echelon is perhaps the most powerful intelligence gathering organization in the world. Reports suggest that this network is being used to spy on private citizens everywhere, including on the Internet.«*

Aufschlussreich ist auch der STOA-Report des Europäischen Parlaments »An Appraisal of the Technologies to Political Control« (Download und aktuelle Ergänzungen unter `www.europarl.eu.int/dg4/stoa/en` oder `http://cryptome.org/stoa-atpc.htm`).

Schließlich meldete die Berliner Tageszeitung »taz« am 10. Januar 2000 unter der Schlagzeile

> *»Präsident Clinton legt Zwei-Milliarden-Dollar-Programm auf: Gegen Internet-Terroristen und für die Ausbildung des Spionage-Nachwuchses«,*

in dem Drei-Jahres-Plan seien – so die »taz« – allein 150 Millionen Dollar »Stipendien« enthalten, um Wissenschaftler und Studenten in »IT-Sicherheitsfragen auszubilden«.

1.5 IT-Sicherheit als Wirkungs- und Handlungszusammenhang

IT-Sicherheit beschäftigt sich mit dem Schutz von Werten gegen Angriffe, wobei Angreifer das Ziel haben, die Werte für eigene Zwecke zu nutzen oder den Eigentümer zu schädigen /Comm98/:

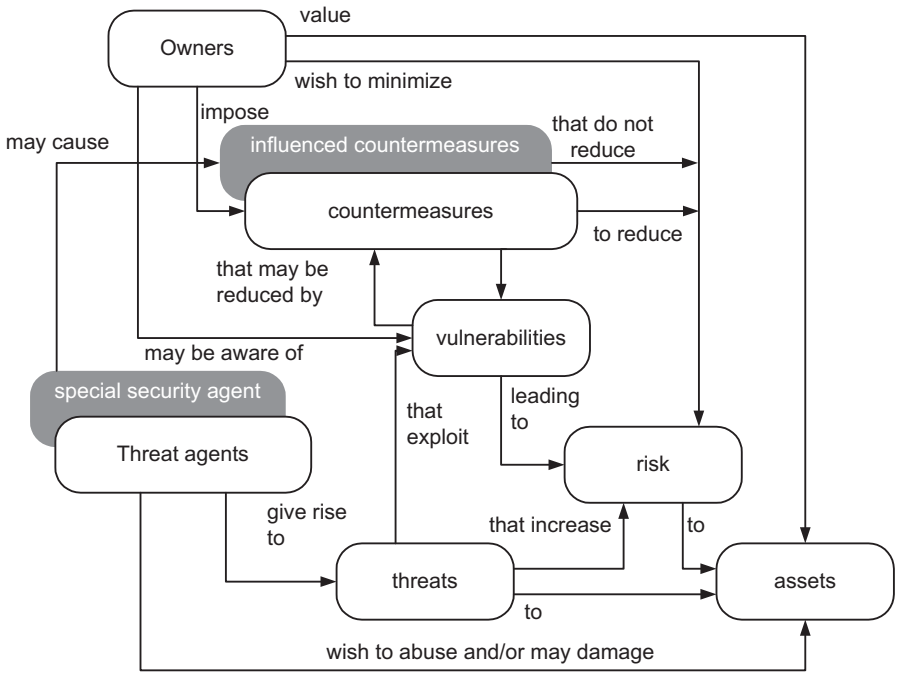


Abb. 1.2: IT-Sicherheit als Wirkungs- und Handlungszusammenhang

Die Sicherung der Werte (Assets) liegt in der Verantwortung ihres Eigentümers (Owner). Die Angreifer (Threat Agents) wollen mit einem Angriff (Threat) auf die Werte deren Vorteile ausnutzen und handeln somit gegen den Eigentümer der Werte. Der Eigentümer nimmt den Angriff – sofern er ihn bemerkt – als Reduzierung seiner Werte wahr. Spezielle Angreifer (zum Beispiel Geheimdienste) sind in der Lage, die Hersteller von Gegenmaßnahmen so zu beeinflussen, dass diese Möglichkeiten einbauen, die es diesen Angreifern erlauben, trotz der Gegenmaßnahmen auf die Werte zuzugreifen.

Für den Eigentümer bedeutet dies wiederum eine Reduzierung seiner Werte und ist als »trügerische Sicherheit« in Wirklichkeit nur eine scheinbare Reduzierung seines Risikos.

Die Angriffe auf IT-Werte beziehen sich in der Regel – aber nicht ausschließlich – auf:

- Verlust der Vertraulichkeit:
  Angreifer kommen unberechtigt in den Besitz der Werte (Informationen).
- Verlust der Integrität:
  Angreifer sind in der Lage, unautorisiert Werte (Informationen) zu manipulieren.

- Verlust der Verfügbarkeit:
  Angreifer enthalten dem Eigentümer den berechtigten Zugriff auf Werte (Informationen, Betriebsmittel etc.) vor.
- Verlust der Verbindlichkeit:
  Die Verbindlichkeit der Transaktion ist nicht gewährleistet. Das Senden und Empfangen von Werten/Information kann geleugnet werden.
- Verlust der Authentizität:
  Die Echtheit des Kommunikationspartners wird gefälscht, der Ursprung der Information (Daten) ist nicht gesichert.

1.6 Chancen und Risiken der Informationstechnik

Jeder Eigentümer von (Informations-) Werten sollte eine Analyse durchführen, welche Angriffe für ihn relevant sind und welche er vernachlässigen kann. Diese Analyse der möglichen Angriffe hilft ihm, geeignete Gegenmaßnahmen auszuwählen, die sein Risiko der Verwundbarkeit auf ein akzeptables Maß reduzieren.

Die Verwundbarkeit und damit der eigene Schutzbedarf ist in der Regel für verschiedene Anwendungen sehr unterschiedlich /Bans96/.

Die eingeführten Gegenmaßnahmen reduzieren die Verwundbarkeit und müssen mit der jeweiligen Sicherheitspolitik übereinstimmen. Auch nach der Einführung der Gegenmaßnahmen bleibt eine Rest-Verwundbarkeit bestehen, die mit anderen Maßnahmen weiter eingeschränkt werden kann /Zurf99/.

Die folgende Grafik symbolisiert den durch »best practice« maximierten Geschäftserfolg:

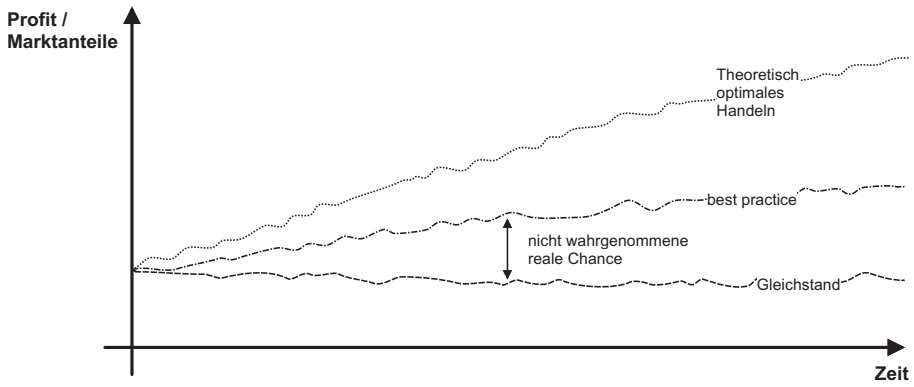


Abb. 1.3: Chancenoptimiertes geschäftliches Handeln

Es besteht weitgehend Einigkeit darüber, dass zum einen die Ungewissheit über das Kommende und zum anderen die negative Valenz des möglichen Ereignisausgangs die zentralen Bestimmungsstücke des Risikos darstellen.

Die Nutzung von Informationstechnik ist immer Chance und Risiko zugleich: Chance, ein angestrebtes Ziel zu erreichen, beispielsweise die Vorteile des Internet zu nutzen und dadurch etwas zu gewinnen (Profit, Marktanteile etc.), und Risiko, dass man etwas Existierendes (Werte) durch das eigene Handeln – zum Beispiel durch die Nutzung des Internet – zur Disposition stellt und dass dadurch Informationswerte beeinträchtigt werden oder man diese sogar verliert /Birn96/ (siehe Abb. 1.4).

Unternehmen und Organisationen sollten die Chancen nutzen, die die Informationstechnik eröffnet – zum Beispiel durch Nutzung des Internets – aber zugleich durch Investitionen in die geeigneten Gegenmaßnahmen (Firewall-Systeme, VPNs, Intrusion-Detection-Systeme, Anti-Virus-Systeme, ...) dafür sorgen, dass das Risiko einer Verwundbarkeit reduziert wird. Hierdurch ist verantwortungsvolles Handeln möglich und die Leistungsfähigkeit beziehungsweise Profit und Marktanteil wird gesteigert – zur betriebswirtschaftlichen und in summa schließlich auch zur volkswirtschaftlichen Blüte /Mcke95/.

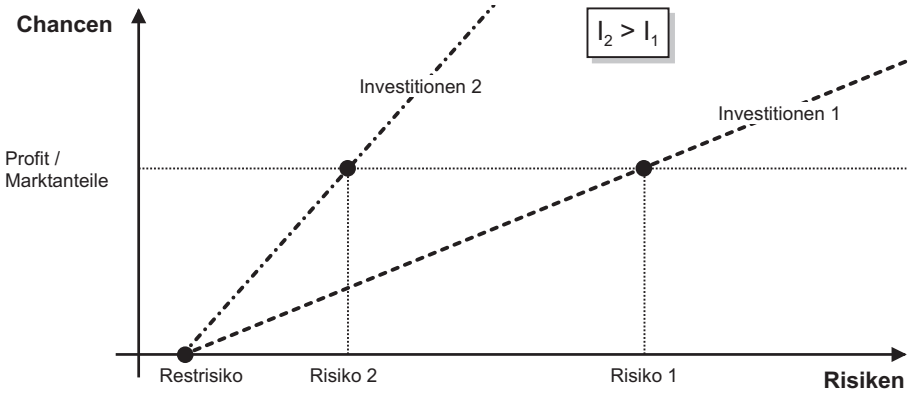


Abb. 1.4: Angemessene Investitionen

In diesem Zusammenhang sei auf zwei Bücher von Tim Cole hingewiesen: »Erfolgsfaktor Internet – Warum kein Unternehmen ohne Vernetzung überleben wird« /Cole99a/ sowie: »Managementaufgabe Sicherheit« /Cole99b/.

1.7 Der VPN-Markt

Das Thema VPN ist so sehr in Bewegung, weil es vor allem durch die Anwender vorangetrieben wird und erst in zweiter Linie durch die Hersteller von Geräten und Software.

Im Rahmen von E-Commerce, E-Business und Remote-Access-Projekten ist die Ausdehnung der Unternehmensnetze gegenwärtig ein zentraler Aspekt in der IT-Welt. Daran wird sich auch in den kommenden Jahren wenig ändern. Soll eine vertrauenswürdige Kommunikation über öffentliche Netzwerke erfolgen, liegt die Erwägung nahe, ein VPN einzurichten.

Was den Einstieg in das Thema VPN interessant macht, ist zum einen die Verfügbarkeit des IPSec-Standards in einer Vielzahl marktreifer Produkte. Denn mit dem IPSec-Standard ist auch ein Haupthemmnis im Bereich der Netzwerksicherheit beseitigt: Anwender erhalten die notwendige Gewährleistung der Investitionssicherheit bei der Anschaffung neuer Produkte, weil sie auch herstellerübergreifend weitgehend interoperabel sind. Zum anderen bewirkt der durch Innovationen angeregte Wettbewerb, dass den Anwendern neue und auf ihre Anforderungen zugeschnittene Lösungen bereitgestellt werden.

Ein weiterer Trend, der zu beobachten ist, ist das Auslagern von Dienstleistungen rund um das Thema Sicherheit: In Organisationen mit geringem Netzwerk-Know-How können in Zukunft externe Dienstleister mit »managed VPNs« die Inhouse-Lösung ersetzen.

Von geringerer Relevanz ist der Wunsch der Organisationen, Kosten zu sparen. Dennoch ist dieses Motiv nicht von der Hand zu weisen, wenn Niederlassungen oder Telearbeitsplätze günstig mittels eines VPN über das öffentliche Telefonnetz anstatt über teuer gemietete Standleitungen angebunden werden können.

Natürlich ist auch der Einsatz von VPNs mit Kosten verbunden, doch kann sich dieser Aufwand auf zweierlei Arten amortisieren:

1. Wie bereits beschrieben, können Niederlassungen, Telearbeitsplätze und mobile Mitarbeiter über günstige lokale Wählverbindungen an das Unternehmensnetz gekoppelt werden und es müssen keine teuren »Leased Lines« verwendet werden.
2. Durch Investitionen in Sicherheitstechnologie kann eine Organisation sich bei Ihren Kunden einen Vertrauensvorsprung vor möglichen Wettbewerbern erarbeiten. Das erhöhte Sicherheitsniveau wird von den Kunden registriert und mit dauerhaften Geschäftsbeziehungen honoriert werden. Schließlich gehen Schreckensnachrichten über Angriffe auf E-Commerce- und E-Business Webseiten beinahe regelmäßig durch die Medien. Und so werden sich die sicherheitsbewussten Kunden bei den Unternehmen wiederfinden, die ein angemessen hohes Sicherheitsniveau bieten. Die Ausgaben, die für ein VPN

entstehen, können daher als vertrauensstiftende Maßnahmen angesehen werden. Damit können möglicherweise auch Investitionen in E-Commerce-Projekte gerettet werden, deren Akzeptanz aufgrund mangelnden Vertrauens niedrig ist.

Als Bremsen für den Einsatz von VPNs haben sich bisher die Investitionskosten und die möglicherweise übertriebenen Versprechungen der Hersteller erwiesen. Gerade hier setzt sich auf dem Markt jedoch eine rationellere Sichtweise über die Möglichkeiten und Grenzen von VPNs durch. Die renommierten Anbieter haben nun schon einige – auch große – Installationen bewältigt und können diese Erfahrungen auf neue Projekte übertragen. Somit verkürzen sich derzeit die Einkaufs- und Einführungsprozesse, und ein VPN ist ein »must-have« für die Mehrzahl von Unternehmen.

Auch Service Provider haben sich mit dem Thema VPN noch nicht ausreichend auseinandergesetzt. Bisher haben nur wenige erkannt, dass sie den Kunden mit einer erhöhten und in Service Level Agreements (SLAs) garantierten Sicherheit einen Mehrwert bieten können. Insbesondere kleineren und mittleren Organisationen können die Service Provider die Sorgen um die ungesicherte Kommunikation nehmen, wenn sie in diesem Bereich Produkte und Servicepakete anbieten. Diese Entwicklung wird zusätzlich durch die – vermutlich anhaltende – Knappheit an qualifizierten Sicherheits-Mitarbeitern forciert. Auch aus diesem Grund werden Fachleute von außerhalb herangezogen und Sicherheitsdienstleistungen ausgelagert.

Bisher galten »Dedicated Line Networks« als die sicherste Form einer Kommunikationsinfrastruktur. Mit der Erkenntnis beziehungsweise dem Nachweis, dass dies nicht der Fall ist, investieren nun viele Organisationen in den Aufbau sicherer VPNs. Weil der Anschluss an das Internet wesentlich günstiger ist als »Dedicated Line Networks«, können nun auch einzelne Rechner beziehungsweise Arbeitsplätze und weltweit verteilte Büros kostengünstig angebunden werden. Selbst für kleinere Organisationen, Mittelständler und in einem Projektnetz arbeitende Freiberufler ist dies möglich. Weil die öffentlichen Leitungen in diesem Fall von Beginn an für geschäftskritische Anwendungen und Informationen genutzt werden, steht die Frage nach Sicherheit in Form von Vertraulichkeit, Manipulationsschutz und Verfügbarkeit sofort im Raum.

Die Nachfrage auf dem europäischen VPN-Markt wird von Unternehmen und Organisationen verschiedenster Art und Größe bestimmt. Service Provider haben nun das Potential dieser Technologie erkannt; sie entwickeln und bieten Lösungen für die verschiedenen Einsatzgebiete an. Viele der großen multinationalen Konzerne planen, ihre Netzwerke über IP-VPNs zu erweitern und werden ihre ATM- und Frame-Relay-Netzwerke nach und nach ersetzen.

VPN-Marktzahlen nach einer Studie von Frost & Sullivan

Dem VPN-Markt in Europa wird – auch zukünftig – ein kräftiges Wachstum bescheinigt: Für 1999 wurde eine Marktgröße von ca. 85 Millionen US-$ festgestellt; das jährliche Marktwachstum soll zwischen 1996 und 2006 bei durchschnittlichen 45,1% liegen. Markt- und Technologieanalysten unterscheiden den VPN-Markt nach Hardware- und Softwarelösungen.

Millionen $	1996	1997	1998	1999	2000	2001	2002	2004	2006
Hardware	10.6	22.4	44.7	84.9	148.6	237.8	368.6	799.9	1149.9
Software	7.5	15.9	31.7	60.2	102.4	176.1	308.2	644.9	890.0
Gesamt	18.2	38.2	76.4	145.2	251.0	413.9	676.8	1445	2040

Tabelle 1.1: VPN Markt 1996-2006
(aus: European Internet Communications Security Market, Frost&Sullivan, 11/2000)

1.8 Fazit

Die internationale wirtschaftliche Ausdehnung vieler Organisationen – man denke an die Mega-Fusionen von Daimler-Benz und Chrysler, Vodafone und Mannesmann oder die größte Fusion der bisherigen Wirtschaftsgeschichte zwischen AOL und Time Warner – braucht vernetzte IT-Strukturen und eine Kommunikationsplattform wie das Internet. Das Internet dringt in viele öffentliche und private Lebensbereiche vor und eröffnet gleichzeitig neue rechtliche, soziale und ethische Probleme, denen wir uns stellen müssen. Politische und juristische Instrumente stehen noch nicht zur Verfügung, um einem Missbrauch wirksam begegnen zu können.

Informationstechnologie kann nur sinnvoll eingesetzt werden, wenn sie sicher und beherrschbar ist. Die Bedrohungen, die aus der neuen Technik resultieren, können wir nicht beeinflussen, sehr wohl aber unsere Verletzbarkeit.

Voraussetzung dafür ist jedoch, dass für bewährte klassische Sicherheitsmechanismen wie Pförtner, Briefumschlag, Siegel, handgeschriebene Unterschrift, Rohrpost und Sicherheitstransporter elektronische Äquivalente eingesetzt werden.

Kapitel 2

Notwendigkeiten, Ziele und Anwendungsformen von VPN-Systemen

In diesem Kapitel werden die Notwendigkeiten und allgemeinen Ziele von Virtual Private Networks (VPNs) dargestellt. Die grundsätzliche Idee, die hinter dem Betrieb solcher Systeme steht, wird erläutert und grundlegende Anwendungsformen werden beschrieben.

2.1 Idee und Definition von VPNs

Das Thema VPN hat einen bemerkenswerten Aufschwung erhalten. Leider besteht eine Unschärfe in der Bedeutung des Begriffs.

In der Fachliteratur wird der Begriff VPN in zwei verschiedenen Bedeutungen verwendet:

1. als eine Methode von Bandbreiten-Management und Quality of Service (QoS) oder
2. als Möglichkeit zur Realisierung einer vertrauenswürdigen Kommunikation mit Hilfe von kryptographischen und anderen Sicherheitsfunktionen

In diesem Buch wird der Begriff VPN nur im Sinne der vertrauenswürdigen Kommunikation verstanden und verwendet.

Die grundsätzliche Idee von Virtual Private Networks (VPNs) ist, die Vorteile einer offenen Kommunikationsinfrastruktur zu nutzen – zum Beispiel der kostengünstigen, weltweit verfügbaren »shared infrastructure« des Internet – aber dabei allen Gefährdungen der Informationssicherheit sinnvoll und angemessen entgegenzuwirken.

Ein VPN soll gewährleisten, dass sensible Daten während der Übertragung über verschiedene, sicherheitstechnisch nicht einschätzbare Netzwerke (LANs und WANs, private und/oder öffentliche Netze) vertrauenswürdig übertragen werden, so dass nur die dazu berechtigten Organisationen oder Personen auf die zu schützenden Daten zugreifen können und ihren Informationsgehalt veränder kann.

Definition »V... P... N...«

- »Virtual« bedeutet, dass es sich – aus Anwendersicht – scheinbar um nur »ein« Netzwerk handelt, auch wenn sich viele reale Teilnetzwerke hinter »einem« VPN verbergen.
- »Private« bedeutet, dass die Kommunikation vertrauenswürdig – also nicht öffentlich – durchgeführt und das Risiko eines Schadens bei der Übertragung minimiert wird.
- »Network« bedeutet, dass eine definierte Gruppe von Rechnersystemen miteinander verbunden wird und mit Hilfe eines Protokolls (typischerweise ist das die TCP/IP-Protokollfamilie) kommuniziert.

2.2 Analogien

Um die grundsätzliche Idee eines VPN zu verdeutlichen und so das Verständnis zu erleichtern, werden im Folgenden zwei Analogien erläutert: zum einen ein Sicherheitstransporter und zum anderen eine Pipeline. Beides schützt die zu übertragenden Werte elektronisch vor Diebstahl, Einsichtnahme und Veränderung.

Sicherheitstransporter

Anders als normale LKWs, bei denen die zu transportierenden Werte nicht explizit geschützt sind, dient ein Sicherheitstransporter dazu, die auszutauschenden Werte während des Transports wirkungsvoll gegen Angriffe zu schützen. Dabei nutzen die Organisationen die gemeinsame öffentliche Infrastruktur der Straßen (Landstraßen, Autobahnen etc.), ohne eine eigene Infrastruktur (Privatstraßen) aufbauen zu müssen.

Entsprechend dient ein VPN dazu, Daten (elektronische Werte, so genannte E-Assets) sicher über die öffentliche Infrastruktur von Netzwerken (LANs und WANs) zu transportieren, ohne dass Unbefugte die Daten einsehen oder manipulieren können.

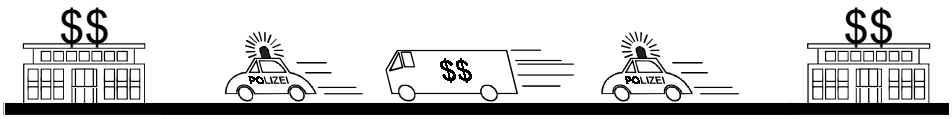


Abb. 2.1: Sicherheitstransporter

Pipeline und Rohrpost

Durch eine Pipeline werden Güter, zum Beispiel Öl, sicher von einem festgelegten Ort zu einem anderen transportiert. Zum Beispiel unterhält die NATO das – in der Öffentlichkeit weitgehend unbekannte – Central European Pipeline System (CEPS); es ist das weltweit umfangreichste und komplizierteste militärische Kraftstoffversorgungssystem.

Durch Beobachtung einer Pipeline kann man allenfalls erkennen, wie hoch der absolute Durchfluß ist, nicht aber, woher der Inhalt stammt und wohin er gelangt. Das Transportgut Öl hat keinen Informationsgehalt, sondern lediglich einen materiellen Wert (»Brennwert«).

Bei einem VPN muss zwischen allen Endpunkten sichergestellt sein, dass tatsächlich alle Daten durch die »VPN-Pipeline« laufen, das heißt, dass sie nicht abgezweigt werden können, und dass kein Unbefugter in die »VPN-Pipeline« eindringen kann.

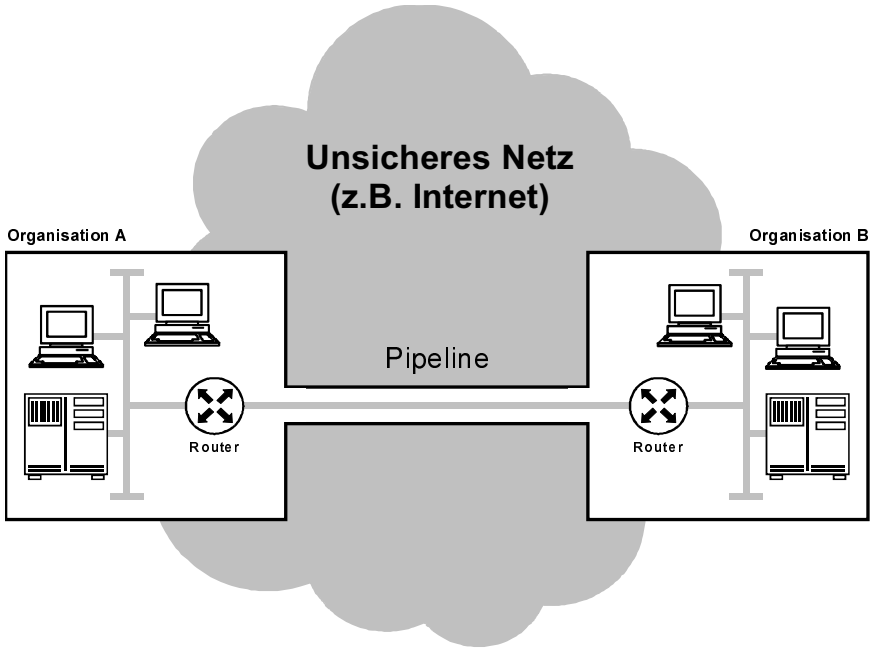


Abb. 2.2: Pipeline

Schon vor mehr als 100 Jahren wurde das Konzept der Pipeline für die gesicherte Übertragung von Schriftgut – also von Information – verwendet: Die Rohrpost in Berlin und anderen Großstädten hatte ihre Blütezeit zwischen 1875 und 1945. Seine größte Ausdehnung hatte das Berliner Netz 1944 mit mehr als 300 offiziellen und rund 100 streng geheimen Kilometern /Arno2000/.

Auch heutzutage befördern Rohrpostanlagen – meist aber nur innerhalb von Unternehmen – Bargeld, Schecks, Dokumente, gefährliche Güter oder auch »nur« Produktionsmittel (übrigens bis 15 kg Gewicht, 30 cm Durchmesser, kilometerweit und bis zu 90 km/h schnell).

Es ist dabei nicht möglich, durch die Beobachtung einer Rohrpost-Hauptleitung zu erkennen, wie sich die Werte bei den Absendern zusammenstellen und bei den Empfängern wieder aufteilen. Außerdem können die Sendungen mit einer Versiegelung der Box zusätzlich geschützt werden.

Tunnel

Der Vollständigkeit wegen sei hier auch der Begriff »Tunnel« erwähnt, der insbesondere in der amerikanischen Fachliteratur verwendet wird (»tunneling«). Diese Analogie bedeutet »Zugriffsschutz« – wie bei der virtuellen Pipeline durch das Internet.

2.3 Moderne IT-Konzepte und IT-Sicherheit

Wie schon in Kapitel 1 ausgeführt, werden heute die meisten Geschäftsprozesse – Angebotserstellung, Auftragsannahme, Bestellung usw. – mit Hilfe moderner IT-Konzepte abgewickelt. Der Trend zur Globalisierung macht es für fast alle Unternehmen und Organisationen unverzichtbar, immer mehr Arbeitsprozesse über sichere Netzwerke zu realisieren, wenn sie im Wettbewerb bestehen wollen.

Der personelle und materielle Aufwand, der in der Vergangenheit schriftlich auf Papier, mit Hilfe der Post oder durch persönlichen Kontakt abgewickelt wurde, wird also größtenteils durch elektronische Verfahren ersetzt, was weitaus rationeller ist.

Diese Informationsverarbeitungs- und Telekommunikationsprozesse sind zum Beispiel Client-Server-Verbindungen, Web-Systeme und E-Mail-Austausch. Dabei werden in der Regel preiswerte, verfügbare und allgemein zugängliche Kommunikationsinfrastrukturen wie das Internet oder andere öffentlich angebotene Backbones genutzt.

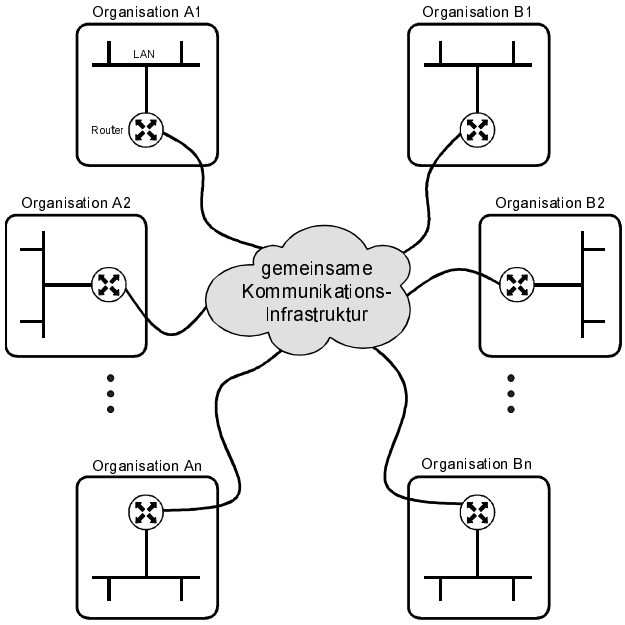


Abb. 2.3: Kopplung von Organisationseinheiten über öffentliche Kommunikationsinfrastrukturen

Technologische Weiterentwicklungen schaffen drastisch höhere Zugangsgeschwindigkeiten zu den öffentlichen Kommunikationsinfrastrukturen.

Während ISDN im Duplex-Betrieb schon bis zu 128 KB pro Sekunde ermöglicht, erreicht die neue ADSL-Technik (Asymmetric Digital Subscriber Line) bis zu 8 MB pro Sekunde – und das mit dem konventionellen Telefonkabel, wie es auf der »letzten Meile« zwischen der Vermittlungsstelle des Telekommunikations-Anbieters und dem Teilnehmeranschluss verlegt ist.

Weitere Entwicklungen stehen bevor, insbesondere Verfahren zur drahtlosen Anbindung.

2.4 Corporate Network versus öffentliche Kommunikationsinfrastruktur

Es gibt zwei unterschiedliche Wege, um die notwendige sichere Kommunikation einer Organisation zur realisieren /Pohl 99b/:

1. Eine Organisation kann für die interne Kommunikation zwischen den einzelnen Organisationseinheiten ein Corporate Network mit eigener Kommunikationsinfrastruktur aufbauen (beispielsweise mit Hilfe von Standleitungen,

ATM-, Frame-Relay- oder X.25-Netzen) und die Kommunikation nach außen – zu Kunden, Lieferanten und Geschäftspartnern – über eine zentrale Stelle realisieren, die an eine öffentliche Kommunikationsinfrastruktur angebunden ist.

2. Die gesamte Kommunikation – nach innen wie nach außen – wird über eine öffentliche Kommunikationsinfrastruktur realisiert. Dabei müssen jedoch geeignete IT-Sicherheitsmechanismen eingebunden werden, die den zusätzlich entstehenden Gefahren entgegen wirken.

Im Folgenden werden die Vor- und Nachteile der beiden Möglichkeiten diskutiert.

Corporate Network

Vorteile:

- Die Organisation hat völlige Freiheit bei der Gestaltung der eigenen Kommunikationsinfrastruktur mit allen gewünschten (technisch realisierbaren) Features.
- Da die Kommunikationsinfrastruktur nur von der eigenen Organisation genutzt wird, ist die Sicherheit und zugleich die Verfügbarkeit höher.
- Die eigene Sicherheitspolitik kann auf allen Ebenen eigenverantwortlich umgesetzt werden.

Nachteile:

- Hohe Investitionen, Betriebs- und Wartungskosten müssen selbst getragen werden.
- Innovationen im IT-Bereich zwingen jeweils zu neuen Investitionen.
- Der maximale Durchsatz bestimmt die maximale Bandbreite und damit auch die Kosten.

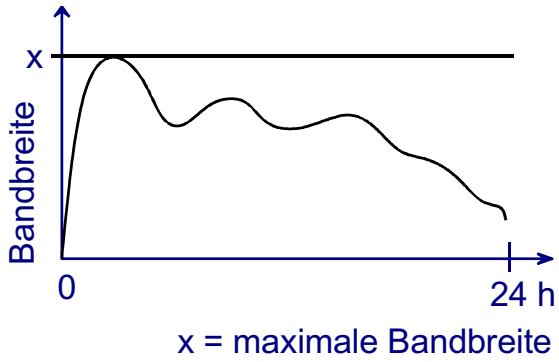


Abb. 2.4: Dimensionierung nach maximaler Bandbreite

Öffentliche Kommunikationsinfrastruktur

Vorteile:

- Innovationen durch die Anbieter stehen den Anwendern unmittelbar zur Verfügung, ohne dass eigene Investitionen notwendig werden.
- Die Kosten für die öffentliche Kommunikationsinfrastruktur sind in der Regel niedriger.
- Die Infrastruktur kann flexibel für die Kommunikation mit Kunden, Lieferanten und Geschäftspartnern benutzt werden.
- Der Anbieter ist verantwortlich für die gleichbleibende Qualität der Dienste in punkto Verfügbarkeit, Geschwindigkeit und Management (Accounting / Billing).
- Die durchschnittliche Bandbreite bestimmt die Kosten, die maximale Bandbreite kann in definierten Bereichen größer sein.

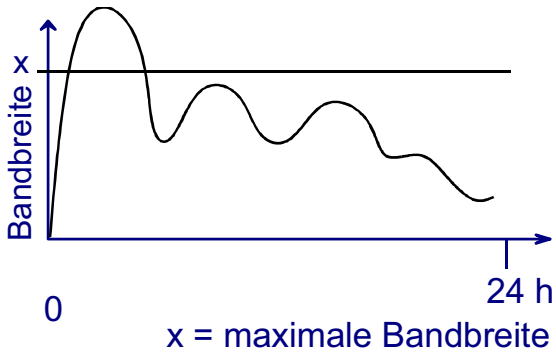


Abb. 2.5: Dimensionierung nach durchschnittlicher Bandbreite

Nachteile:

- Der Anwender ist abhängig vom Anbieter und dessen Sicherheitsstrategie.
- An die öffentliche Kommunikationsinfrastruktur sind auch andere Benutzer angeschlossen, die einen anderen Schutzbedarf haben (Extrembeispiel: Hacker neben professionellen Business-Anwendern).
- Die Security Policy des Anbieters ist nicht immer klar nachvollziehbar und überprüfbar.

2.5 Zielsetzung eines VPN

Die moderne Informationstechnik arbeitet zunehmend mit verteilten Anwendungen. Das bedeutet, dass Daten an verschiedenen Orten erstellt oder bearbeitet und dann über Kommunikationsnetze ausgetauscht werden.

Diese Kommunikationstechniken bieten unübersehbare Vorteile im Hinblick auf die Schnelligkeit und Flexibilität der Informationsübermittlung. Zugleich aber entstehen nicht zu unterschätzende Sicherheitsrisiken, die unter Umständen allen Nutzen zunichte machen können:

- Die Daten können durch Dritte gelesen und verändert werden, während sie über öffentliche Netze (Kommunikationsinfrastrukturen) übertragen werden.
- Durch die Ankopplung an ein offenes Netzwerk können Unbefugte auf die Rechnersysteme des eigenen Netzes zugreifen und Schaden anrichten.

Moderne IT-Sicherheitstechniken können die Daten auf ihrem Weg über öffentliche Netze so schützen, dass ihre Vertraulichkeit (Privatheit) gewährleistet bleibt und niemand in der Lage ist, unbefugt auf die eigenen Rechnersysteme zuzugreifen.

Diese Sicherheitsmaßnahmen ermöglichen es, die Vorteile öffentlicher Kommunikationsinfrastrukturen zu nutzen und zugleich die Vertraulichkeit und Informationssicherheit eines privaten Netzwerks zu bewahren.

Damit dieses Ziel erreicht werden kann, müssen kryptographische Verfahren und andere Sicherheitsmechanismen eingesetzt werden.

Dazu zählen zum Beispiel:

- Verschlüsselung
- Authentikation
- Digitale Signaturen für die Unversehrtheit der Daten
- Tunneling
- Firewalling

2.6 Anwendungsformen von VPNs

Verschiedene Anwendungsformen von VPNs stellen spezifische Anforderungen hinsichtlich Connectivity (Verbindlichkeit), Verfügbarkeit, Datendurchsatz, Einsatz von Standards und Schlüsselmangement. Optimal wäre ein VPN, das alle Anforderungen abdeckt und auch den unterschiedlichen Ansprüchen an die Kosten gerecht wird.

Unternehmensweites VPN

Darunter versteht man »private« Netzwerkverbindungen zwischen verschiedenen LAN-Standorten eines Unternehmens (Zentrale und Niederlassungen), die dazu dienen, Unternehmensdaten vertrauenswürdig über ein unsicheres Netz wie das Internet austauschen zu können. Hier spielt die Transparenz der Lösung eine wichtige Rolle.

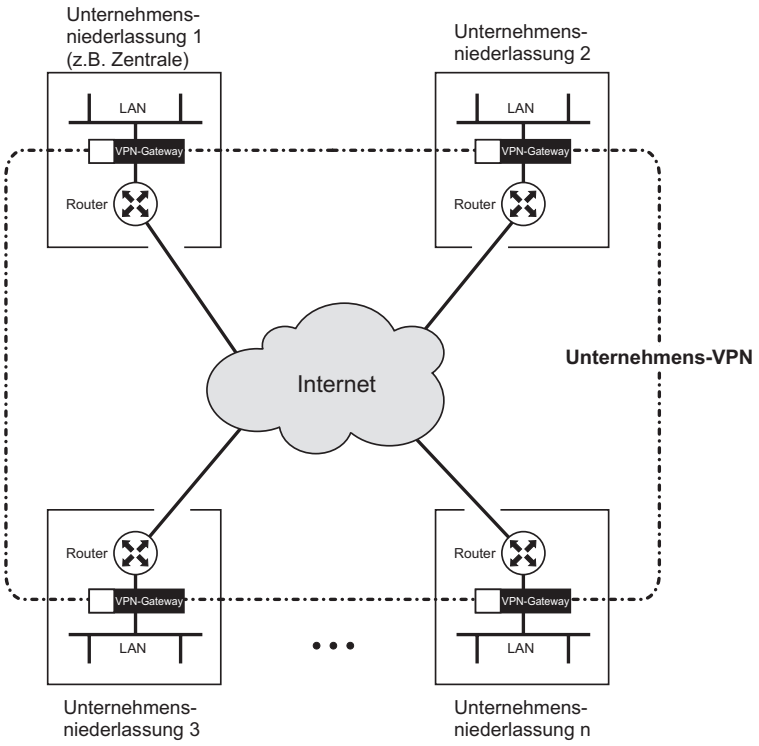


Abb. 2.6: Unternehmensweites VPN

Sichere Remote-Ankopplung

Heim- und/oder Mobil-Arbeitsplätze greifen innerhalb eines VPN über ein öffentliches Netzwerk (zum Beispiel das Internet) geschützt auf die zentral gespeicherten Unternehmensdaten zu. Hier spielt die Identifikation und Authentikation des Nutzers, der auf die Daten zugreifen möchte, eine besondere Rolle.

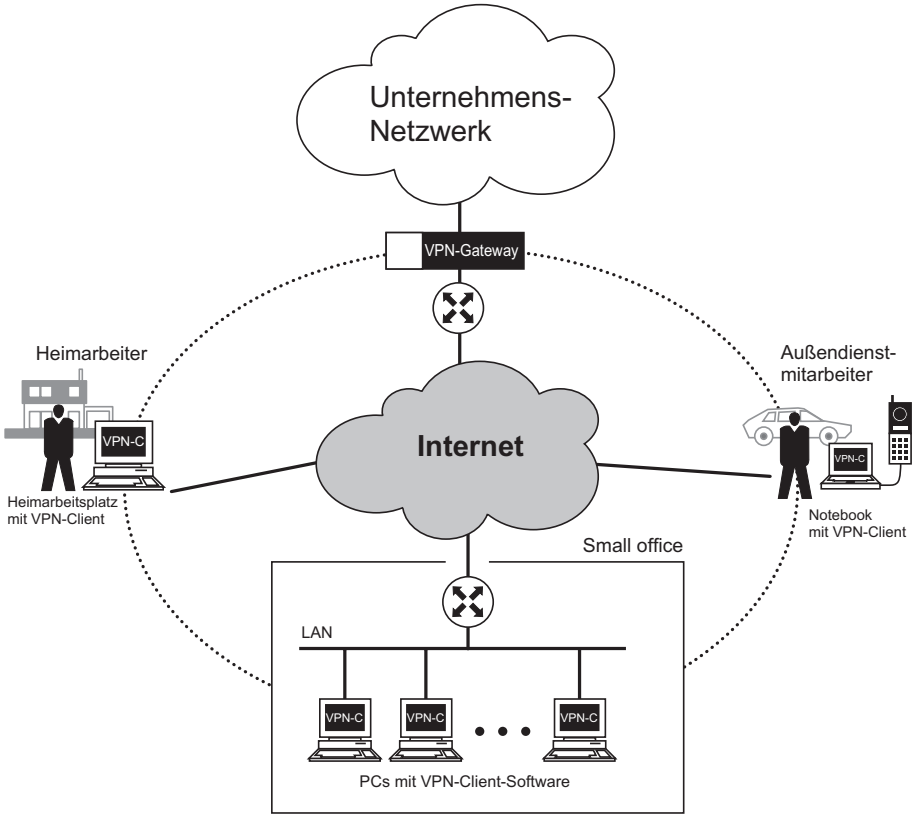


Abb. 2.7: Remote-Ankoppelung mit Hilfe eines VPN

VPN zwischen verschiedenen Unternehmen

In einer definierten Gruppe von Unternehmen – beispielsweise von Automobilherstellern und -zulieferern – können alle Partner miteinander mit Hilfe von VPNs eine vertrauenswürdige, untereinander und nach außen hin geschützte Kommunikation realisieren. Hier spielt das unternehmensübergreifende Sicherheitsmanagement eine besondere Rolle.

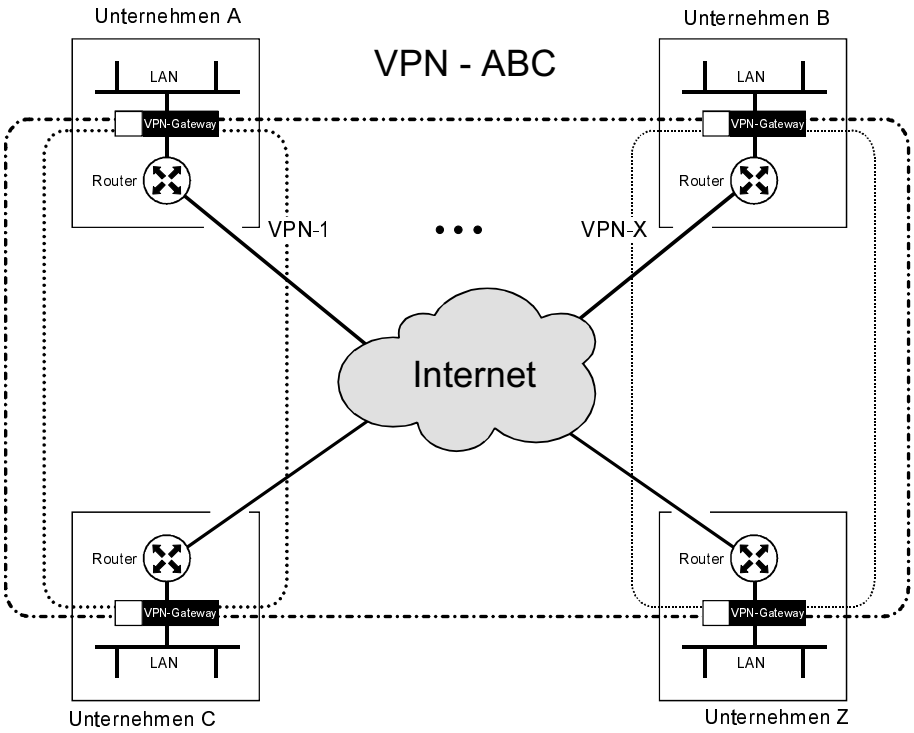


Abb. 2.8: Kooperatives VPN verschiedener Unternehmen

Kombinationen der Anwendungsformen

Natürlich gibt es auch Kombinationen der oben beschriebenen Anwendungsformen. Hier spielt die Verwendung eines einheitlichen Standards und die Möglichkeit eines flexiblen und unternehmensübergreifenden Sicherheitsmanagements eine besondere Rolle.

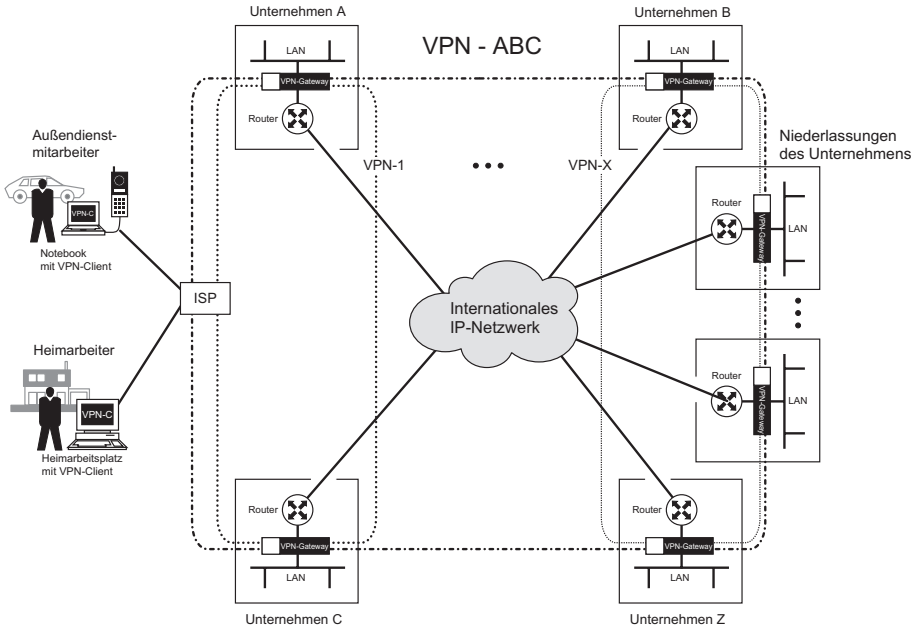


Abb. 2.9: VPN-Kombinationen

Kapitel 3

Bedrohungen im Netz

In diesem Kapitel werden die potentiellen Bedrohungen beschrieben, die in Netzen wie Intranets und dem Internet bestehen.

Angreifer

Personen greifen Rechnersysteme und Netzwerke an. Sie tun dies aus sehr unterschiedlichen Motiven.

Im Folgenden werden einige Arten von Angreifern und deren Ziele dargestellt:

- Hacker
  Hacker brechen in Rechnersysteme und Netzwerke ein, weil sie darin eine Herausforderung sehen und mit dem Erfolg ihren Status vergrößern wollen. Oft handelt es sich um Jugendliche, die aus »Spieltrieb«, also ohne böse Absicht handeln. Sie sind aber unberechenbar und können hohen Schaden verursachen.
- IT-Spione
  Bezahlte Spezialisten – teilweise mit einem sehr hohem Budget – versuchen, über gezielte Angriffe an Informationen zu kommen. Ihre Ziele sind politisch oder auch wirtschaftlich begründet (siehe »Echelon«).
- IT-Terroristen
  Terroristen können Rechnersysteme und Netzwerke angreifen, um aus politischen Gründen Angst und Chaos zu verursachen.
- Unternehmens-Cracker
  Dies sind Mitarbeiter, die auf Rechnersysteme und Netzwerke von Konkurrenzunternehmen zugreifen, um ihrem Unternehmen finanzielle Vorteile zu schaffen. Dazu spähen sie beispielsweise Entwicklungsunterlagen oder Strategiepläne aus.
- Professionelle Kriminelle
  Diese Personen wollen sich mit Angriffen persönlich bereichern, beispielsweise durch die nicht bezahlte Nutzung von Dienstleitungen oder durch das Abbuchen von fremden Konten.
- Vandalen
  Vandalen sind Personen, die Angriffe durchführen, um Organisationen oder Personen gezielt Schaden zuzufügen.

3.1 Angriffsmöglichkeiten in Kommunikations-Systemen

Die stärksten Bedrohungen von IT-Systemen zielen auf das Kommunikations-System, das heißt auf die Nachrichten, die über Systeme wie Internet und Intranet ausgetauscht werden. Zunächst werden die verschiedenen Angriffsarten definiert und anschließend die Schäden kategorisiert, die durch Angriffe entstehen können.

Auf eine Nachricht (ein oder mehrere IP-Pakete) reagiert ein Empfänger mit einem bestimmten Verhalten (Abb. 3.1):

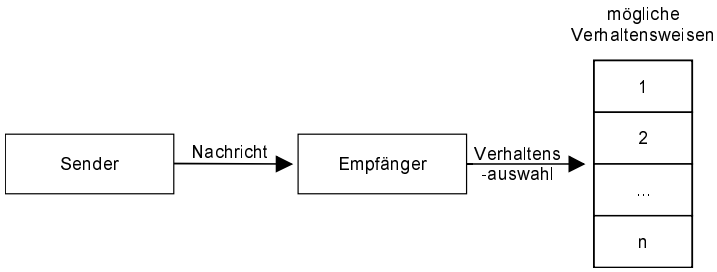


Abb. 3.1: Reaktionsmöglichkeiten des Empfängers einer Nachricht

Ein Angreifer, der die Kommunikationsverbindung abhört, kann das Verhalten des Empfängers und des Senders interpretieren. Der Angreifer kann die Reaktionen des Empfängers zielgerichtet beeinflussen, wenn er die Möglichkeit hat, die Nachricht zu wiederholen, zu verändern, zu löschen oder zu ergänzen.

Aus dieser Überlegung heraus werden grundsätzlich zwei Arten von Angriffen unterschieden: passive Angriffe und aktive Angriffe.

3.1.1 Passive Angriffe

Bei passiven Angriffen werden die übertragenen Nachrichten und der Betrieb des Kommunikations-Systems nicht geändert. Passive Angriffe sind Bedrohungen, die vom Angreifer bewusst und gezielt durchgeführt werden, um sich unerlaubt Informationen zu beschaffen.

Passive Angriffe können zum Beispiel mit Hilfe von Klemmen oder Induktionsschleifen an der Leitung oder durch das Abfangen der Signale von Richtfunk- und Satellitenverbindungen durchgeführt werden (Abb. 3.2).

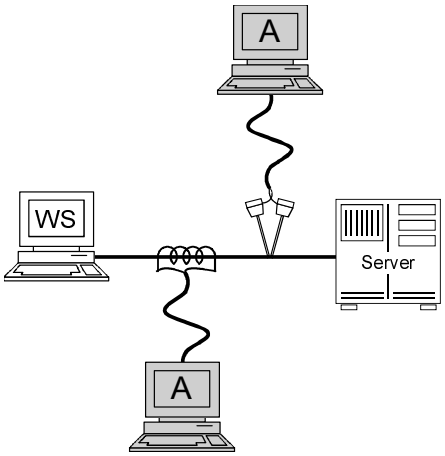


Abb. 3.2: Passive Angriffe auf Nachrichten oder auf das Kommunikations-System

Man kann folgende passive Angriffsarten unterscheiden:

- Abhören von Daten
  Ein Abhörer gelangt unmittelbar in den Besitz der Nachricht und kann sie zu seinem Zweck verwerten. Beispielsweise kann ein Angreifer bei einer IP-Verbindung zwischen einem Telnet-Server und einem Telnet-Client während der Login-Prozedur die Identität und das Passwort eines Teilnehmers abhören und später mit diesem Passwort unerlaubt Zutritt zum Serversystem erlangen. Weitere Möglichkeiten sind das Abfangen von vertraulichen Informationen, wie Entwicklungsunterlagen von neuen Produkten, das Abhören von Daten, die unter das Datenschutzgesetz fallen, oder Angebote auf Ausschreibungen. Solche Angriffe sind bei der Nutzung von frei zugänglichen LAN-Anschlüssen problemlos durchführbar.
- Abhören der Teilnehmer-Identitäten
  Der Lauscher erfährt, welche Teilnehmer (Benutzer oder Rechnersysteme) untereinander eine Datenverbindung aufbauen und Daten austauschen. Allein aus der Kenntnis, wer mit wem zu welchem Zeitpunkt Nachrichten ausgetauscht hat, sind oft Rückschlüsse auf den Inhalt der Nachricht oder auf das Verhalten der Teilnehmer möglich. Wenn zum Beispiel jemand auf die Web-Seiten eines Waschmaschinenherstellers zugreift, kann vermutet werden, dass er eine Waschmaschine kaufen möchte. Tauschen zwei bis dahin konkurrierende Unternehmen in großem Umfang Nachrichten aus, kann dies ein Anzeichen für eine bevorstehende Zusammenarbeit sein.

- Verkehrsflussanalyse
  Auch wenn die Daten verschlüsselt sind, ist es einem Abhörer möglich, durch eine »Verkehrsflussanalyse« gewisse Informationen zu erhalten. Dabei kann es sich um Größenordnungen, Zeitpunkte, Häufigkeit und Richtung des Datentransfers handeln. Diese Informationen können für bestimmte spezielle Anwendungen interessant sein, wie etwa Börsen-Transaktionen oder militärische Operationen.

Spezielle Gefahren beim Einsatz lokaler Netze

Besonderen passiven Angriffen sind lokale Netze (LANs) ausgesetzt, da sie im Allgemeinen »Broadcast-Medien« verwenden. Es werden alle Nachrichten an alle Teilnehmer gesendet und es wird davon ausgegangen, dass die Teilnehmer nur die Nachrichten verwenden, die für sie bestimmt sind. In der Praxis werden zusätzliche Netzwerk-Steckdosen eingerichtet, um flexibel für Umzüge, weitere Rechnersysteme etc. zu sein. Diese zusätzlichen Steckdosen sind meist nicht blockiert, solange sie nicht benutzt werden. Sie können dadurch jederzeit missbraucht werden, um Analysegeräte anzuschließen und den gesamten Nachrichtenstrom mitzuverfolgen.

Lokale Netze sind aber auch so konzipiert, dass im laufenden Betrieb zusätzliche Steckdosen und Rechnersysteme montiert werden können, ohne den Verkehr zu stören. Diese Flexibilität und Robustheit ist aus Sicht der Datensicherheit von großem Nachteil. Beide beschriebenen Faktoren bergen die Gefahr, dass zusätzliche Rechnersysteme unbefugt und unbemerkt angeschlossen werden können. Aber auch die Stationen befugter Teilnehmer können dazu verwendet werden, den gesamten Nachrichtenstrom abzuhören.

Mit einfachen Hilfsmitteln wie Protokollanalysatoren (z. B. TCPDump oder Snoop als Standard-UNIX-Tools) können möglicherweise von jedem Rechnersystem im LAN alle Pakete mitgelesen werden. Da viele Organisationen die Systemadministration der Rechnersysteme »remote« durchführen, können »root«-Passworte mitgelesen werden. Mit deren Hilfe können dann weitere Angriffe durchgeführt werden.

Protokollmitschnitt einer Telnet-Session

Im folgenden Protokollmitschnitt einer Telnet-Sitzung ist die Phase des Login festgehalten. Die Software, die den Protokollmitschnitt realisiert hat, kann auf jedem üblichen PC laufen, der an ein LAN angeschlossen ist (siehe Abb. 3.3). An das Rechnersystem, mit dem der Mitschnitt durchgeführt wurde, werden von der Analysesoftware (A) keine besonderen Anforderungen gestellt.

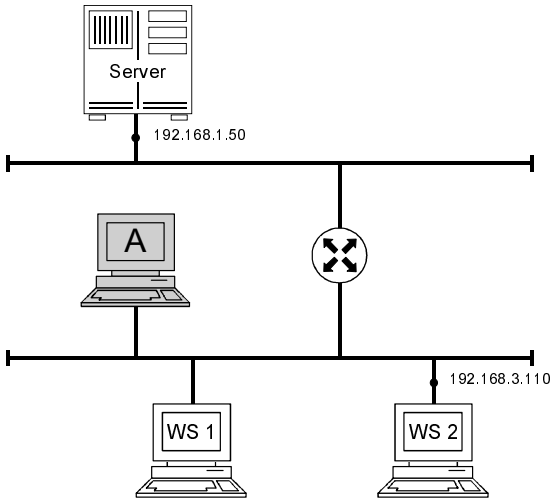


Abb. 3.3: Passiver Angriff mit Hilfe eines Protokollanalysators

Der Benutzer der Workstation 2 hat ein Login am Server durchgeführt. Als Benutzeridentifikation wurde »Nutzer1« eingegeben. Diese Eingabe wurde vom Server zur Kontrolle zurückgesendet, aus diesem Grund sind die einzelnen Buchstaben doppelt im Protokollmitschnitt zu sehen. Das Passwort, das der Benutzer »Nutzer 1« verwendet hat, lautet »1beutlin« (siehe Tab. 3.1). Die Buchstaben des Passworts werden vom Server nicht zurückgesendet, so dass sie nur einmal zu sehen sind. Diese Eigenschaft erleichtert die Suche nach dem Passwort in Protokollmitschnitten.

Wenn ein Protokollmitschnitt aufgenommen wird, während sich alle Netzwerk-Teilnehmer am Server einloggen – beispielsweise bei Arbeitsbeginn in einem Unternehmen –, können alle Passworte festgehalten werden.

Es muss betont werden, dass mangelhafte Vertraulichkeit ein großes Problem beim Betrieb lokaler Netze ist, da sie auch mit der mangelhaften Sicherheit der üblichen Zugangs- und Zugriffskontrollen auf Serversystemen und jeglichen Betriebsmitteln im lokalen Netz zusammenhängt.

Weitere Gefahrenpunkte in lokalen Netzen, an denen Nachrichten abgehört werden können, sind Hubs, Brücken, Router und Gateways.

Ziel	Quelle	Nachricht
192.168.3.110	192.168.1.50	Telnet :login:
192.168.1.50	192.168.3.110	Telnet :n
192.168.3.110	192.168.1.50	Telnet :n
192.168.1.50	192.168.3.110	Telnet :u
192.168.3.110	192.168.1.50	Telnet :u
192.168.1.50	192.168.3.110	Telnet :t
192.168.3.110	192.168.1.50	Telnet :t
192.168.1.50	192.168.3.110	Telnet :z
192.168.3.110	192.168.1.50	Telnet :z
192.168.1.50	192.168.3.110	Telnet :e
192.168.3.110	192.168.1.50	Telnet :e
192.168.1.50	192.168.3.110	Telnet :r
192.168.3.110	192.168.1.50	Telnet :r
192.168.1.50	192.168.3.110	Telnet :1
192.168.3.110	192.168.1.50	Telnet :1
192.168.1.50	192.168.3.110	Telnet :.
192.168.3.110	192.168.1.50	Telnet :..
192.168.3.110	192.168.1.50	Telnet :Password:
192.168.1.50	192.168.3.110	Telnet :1
192.168.1.50	192.168.3.110	Telnet :b
192.168.1.50	192.168.3.110	Telnet :e
192.168.1.50	192.168.3.110	Telnet :u
192.168.1.50	192.168.3.110	Telnet :t
192.168.1.50	192.168.3.110	Telnet :l
192.168.1.50	192.168.3.110	Telnet :i
192.168.1.50	192.168.3.110	Telnet :n
192.168.1.50	192.168.3.110	Telnet :.
192.168.3.110	192.168.1.50	Telnet :..
192.168.3.110	192.168.1.50	Telnet :Last login: Tue Apr 29 14:05:20 from merry..

Tabelle 3.1: Mitschnitt einer Telnet-Sitzung

Aktive Angriffe

Neben der Gefahr, abgehört zu werden, besteht das Risiko aktiver Angriffe, die den Nachrichtenstrom und/oder den Betrieb der Kommunikation verfälschen. Aktive Angriffe werden beispielsweise durch Auftrennen der Übertragungsleitungen oder mit Hilfe der Emulation von Übertragungsprotokollen durchgeführt (Abb. 3.4).

Bei aktiven Angriffen wird grob unterschieden zwischen Bedrohungen durch Dritte und Bedrohungen durch den Kommunikationspartner.

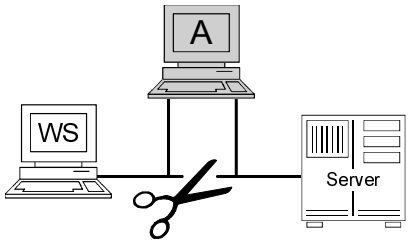


Abb. 3.4: Aktive Angriffe

Bedrohungen durch Dritte sind zum Beispiel:

- Wiederholen oder Verzögern von Informationen
  Durch Wiederholen oder Verzögern von Informationen kann der Empfänger irritiert oder zu einer falschen Aktion veranlasst werden.
  Beispiel: Mehrfache Überweisung eines Geldbetrags oder Wiederholung eines abgefangenen Logins.

- Einfügen oder Löschen bestimmter Daten
  Um ein System zu manipulieren, fügt ein Angreifer bestimmte Nachrichten oder Daten innerhalb der Nachrichten ein oder löscht sie. Ein Empfänger kann durch Unterdrückung oder zusätzlichen Empfang entscheidender Informationen zu einem falschen Verhalten veranlasst werden.
  Beispiel: In der E-Mail »Kaufen Sie *keinesfalls* neue Aktien« wird das Wort »*keinesfalls*« während der Übertragung gelöscht, so dass der Empfänger die Instruktion »Kaufen Sie neue Aktien« erhält.

- Modifikation von Daten
  Modifikation von Daten bedeutet, dass die Veränderung der Daten von den Kommunikationspartnern nicht erkannt wird. Durch Ändern der Daten während der Datenübertragung ist es dem Angreifer möglich, falsche Aktionen zu veranlassen /PoRi95/.

  Beispiel: Die Veränderung einer Kontonummer bei einer Geldüberweisung führt dazu, dass ein anderer als der intendierte Empfänger das Geld bekommt.

- Boykott des Kommunikations-Systems (Denial of Service)
  Wenn der Umfang von eingefügten oder unterdrückten Daten zu groß wird oder echtzeitorientierte Daten zu lange verzögert werden, kann hierdurch das gesamte Kommunikations-System boykottiert werden.

  Beispiel: Durch permanenten Verbindungsaufbau zu einem bestimmten Server kann dieser blockiert und isoliert werden.

Bedrohungen durch den Kommunikationspartner sind zum Beispiel:

- Vortäuschung einer falschen Identität (Maskerade-Angriff)
  Wenn sich ein Teilnehmer für einen anderen ausgibt, kann er sich Informationen erschleichen, die für diesen anderen Teilnehmer bestimmt waren, oder Aktionen auslösen, die nur der andere Teilnehmer veranlassen darf.

  Beispiel: Ein Teilnehmer verschafft sich unerlaubt Zugang zur einer Datenbank.

- Leugnen einer Kommunikationsbeziehung
  Der steigende Einsatz von Datenkommunikation zur Abwicklung vertraglich relevanter Vorgänge erfordert, dass sowohl der Abender einer Nachricht nicht leugnen kann, der Abender zu sein, als auch der Empfänger nicht abstreiten kann, die Nachricht erhalten zu haben.

  Beispiele: Die Bestellung von Waren bei einem Internet-Versandhändler oder der Abschluss von Verträgen über das Internet.

Trittbrettfahrer (Man in the middle)

Sogenannte Trittbrettfahrer verbinden sich zum Beispiel mit einem Knotenpunkt (Router oder Rechnersystem) im Internet und verfolgen einen Verbindungsaufbau mit. Die Verbindung wird dann nach der Authentikation des Benutzers für eigene Zwecke genutzt. Mit dieser Methode können Rechnersysteme, auf die der Zugriff eigentlich beschränkt ist, manipuliert und Authentikationsprozesse (auch kryptographische Methoden) unterlaufen werden.

Beschreibung eines Angriffs

Der Benutzer der Workstation 1 möchte einen Dienst des Servers X im Internet nutzen. Dazu baut der Benutzer eine Verbindung zum Server X auf und führt dort den notwendigen Login-Vorgang (Identifikation und Authentikation) durch.

Ein Angreifer (Rechnersystem A), der sich aktiv in die Kommunikationsverbindung im Internet eingeklinkt hat, verfolgt diese Prozedur und wartet, bis der Server die Bestätigung des erfolgreichen Login sendet. Diese Bestätigung gibt er nicht an die Workstation 1 weiter, sondern signalisiert dieser beispielsweise einen Verbindungsabbau. Der Angreifer trennt damit die Workstation 1 ab, ohne dass deren Benutzer den Angriff »bemerkt«. Nun kann der Angreifer die authentisierte Verbindung für sich und seine Ziele nutzen (Abb. 3.5). Diese Angriffsmethode kann auch bei kryptographischen Authentikationsverfahren benutzt werden.

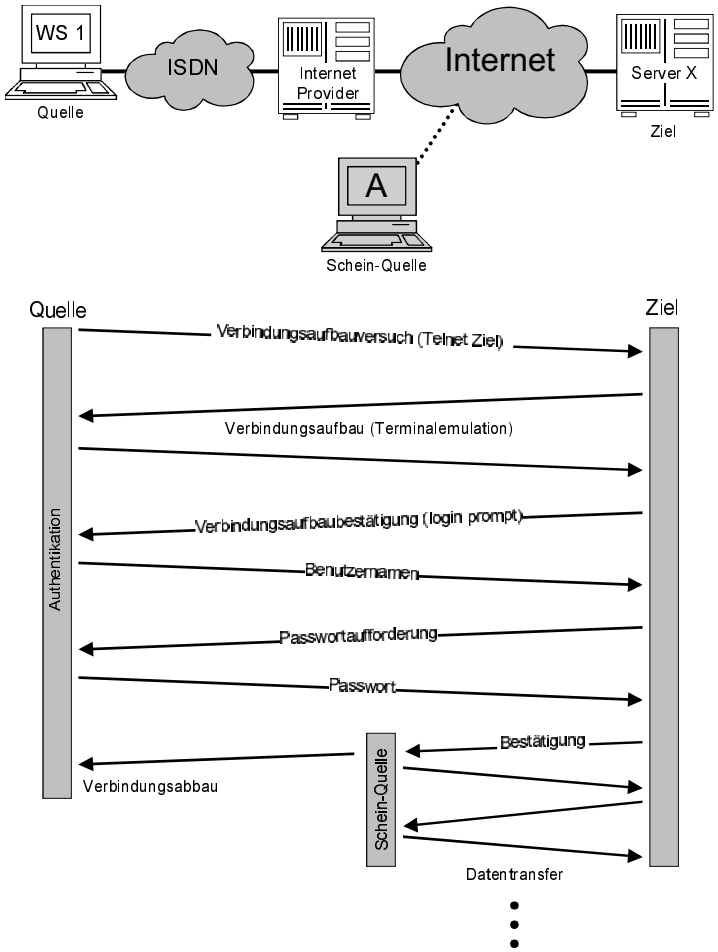


Abb. 3.5: Trittbrettfahrer

3.1.2 Zufällige Verfälschungsmöglichkeiten

Neben den Gefahren, die Kommunikations-Systemen durch absichtliche passive und aktive Angriffe drohen, gibt es auch verschiedene Möglichkeiten unbeabsichtigter Verfälschungen.

Unbeabsichtigte Verfälschungsmöglichkeiten sind zum Beispiel:

- Fehlrouting von Informationen
  In den Routern im Internet/Intranet können Informationen auf einen falschen Weg geraten und an einen fremden Teilnehmer ausgeliefert werden. Ein solches Fehlrouting kann bereits beim Verbindungsaufbau erfolgen, so dass die Verbindung zu einem falschen Teilnehmer hergestellt wird.

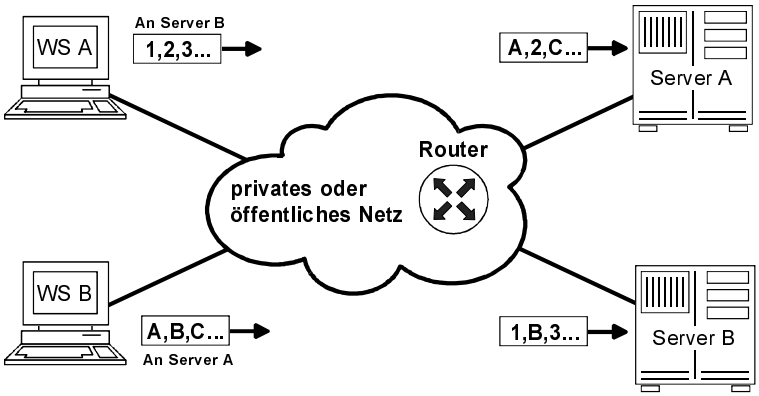


Abb. 3.6: Fehlrouting von Informationen

- Übertragungsfehler
  Übertragungsfehler können durch Übersprechen von Nachbarkanälen oder durch Wählgeräusche verursacht werden. Die Bitfehlerwahrscheinlichkeiten bei Datenübertragungswegen liegen zwischen 10^{-4} bis 10^{-7}. Auch hier können sicherheitskritische Fehler bei der Kommunikation über TCP/IP-basierte Netze auftreten.

- Software-Fehler
  99 % aller Software ist nicht verifiziert. Das bedeutet, dass in allen Softwarepaketen Fehler vorhanden sind, die in bestimmten Situationen zu Fehlreaktionen führen können.

  Beispiel: Die Software wählt durch einen internen Fehler einen falschen Teilnehmer an und sendet diesem vertrauliche Daten.

- Hardwarefehler durch Umwelteinflüsse
  Umwelteinflüsse wie elektromagnetische Emissionen können mit einem bestimmten Wahrscheinlichkeitsgrad die Ursache dafür sein, dass in einem Rechnersystem Bits umkippen, wodurch ein falsches Verhalten zu erwarten ist.

  Beispiel: Durch das Umkippen eines Bits im Router wird ein vertrauliches IP-Paket auf einem falschen logischen Kanal zu einem falschen Teilnehmer gesendet.

- Fehlbedienung
  Der Benutzer löst versehentlich Aktionen aus, die er nicht auslösen wollte.

  Beispiel: Der Benutzer wählt aus Versehen einen falschen Teilnehmer an und sendet diesem vertrauliche Informationen.

Fazit: Zufällige Verfälschungsmöglichkeiten können – wie aktive Angriffe – praktisch nicht ausgeschlossen werden. Wenn sie aber bekannt sind und beim Aufbau

der Kommunikations-Systeme berücksichtigt werden, kann der mögliche Schaden begrenzt werden.

3.2 Weitere Aspekte potentieller Bedrohungen bei Internet-Kommunikation

Fernmeldegeheimnis

In Deutschland gilt für alle Anbieter von Telekommunikationsdienstleistungen das Fernmeldegeheimnis. Dies bedeutet, dass Anbieter von Telekommunikationsdienstleistungen darlegen müssen, wie ihre Kommunikations-Systeme (Knoten, Netzwerkmanagement, usw.) abgesichert werden, um eine Manipulation von außen zu verhindern. Daher kann davon ausgegangen werden, dass im Fall einer Kommunikation über Netze in Deutschland und in anderen europäischen Ländern von den Telekommunikations-Dienstleistern ein hohes Maß an Sicherheit gewährleistet wird.

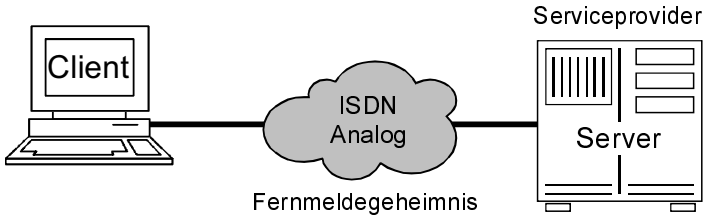


Abb. 3.7: Fernmeldegeheimnis

Beim Anschluss an das Internet, in dem die Kommunikation über Provider möglicherweise »um die ganze Welt geht«, verlassen wir diesen geschützten Bereich, da in anderen Ländern Vorschriften bezüglich des Fernmeldegeheimnisses nicht oder in nicht ausreichender Form existieren. Es kann also nicht davon ausgegangen werden, dass außerhalb Deutschlands oder Europas der gleiche rechtliche und technische Schutz gewährleistet ist.

Kommunikationswege der IP-Pakete im Internet

Da beispielsweise E-Mails unter Umständen über viele Netzknoten geleitet werden, worauf die Benutzer keinen Einfluss haben, ist die Gefahr eines organisierten Angriffs nicht zu unterschätzen.

Die Abbildung 3.9 zeigt, welchen abenteuerlichen Weg die IP-Pakete einer E-Mail genommen haben, die von der Niederlassung Aachen der Utimaco Safeware AG zu einem Institut der Rheinisch-Westfälischen Technischen Hochschule Aachen (RWTH Aachen) gesendet wurde, das nur 3 Kilometer entfernt liegt.

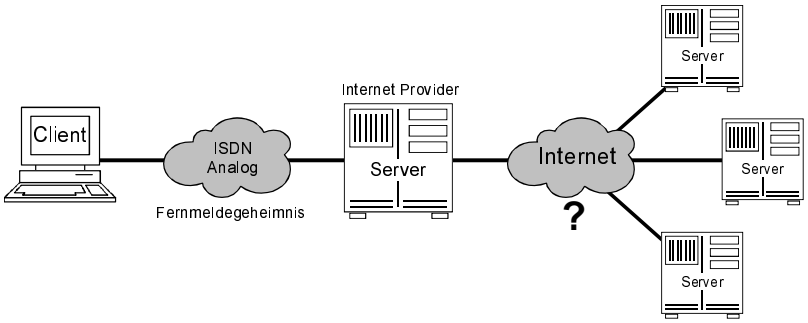


Abb. 3.8: Internet und das Fernmeldegeheimnis

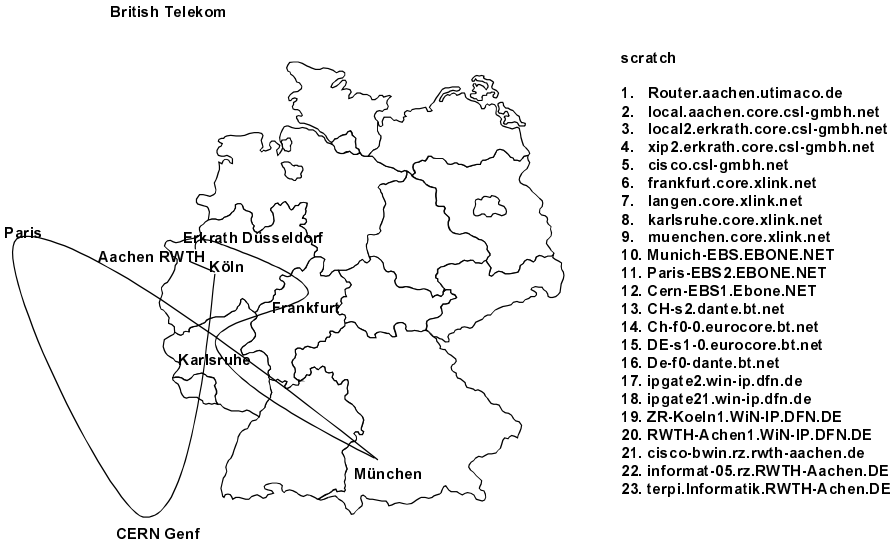


Abb. 3.9: Weg der IP-Pakete einer E-Mail

Diese E-Mail ist über 23 Router gelaufen, die sie empfangen und weitergesendet haben. Hierbei handelt es sich um ein harmloses Beispiel. Abhängig vom jeweiligen Internet-Provider werden manche IP-Pakete sogar über die USA geroutet.

3.2.1 Angriffstools aus dem Internet

Im Internet sind eine Reihe von Tools (z. B. ISS, Nessus) abrufbar, mit denen eine Analyse der Netzschwachstellen von TCP/IP-basierten Systemen, aber auch gezielte Angriffe möglich sind. Mit Hilfe dieser Tools kann jeder Benutzer, auch wenn er nicht über spezielles Fachwissen verfügt, solche Angriffe durchführen.

3.2.2 Implementierungsfehler in Anwendungen und fehlerhafte Konfigurationen

Anwendungen wie »Sendmail« wiesen in der Vergangenheit Implementierungsfehler auf, die es ermöglichten, auf einem entfernten IT-System beliebige privilegierte Kommandos auszuführen. Mit Hilfe dieser privilegierten Kommandos wurden dann Angriffe durchgeführt.

Für jeden Dienst, der über einen Netzzugang ermöglicht werden soll, existiert ein Daemon-Prozess, der falsch konfiguriert oder fehlerhaft sein kann, wodurch wiederum Angriffe durchgeführt werden können /CERT95/.

3.2.3 Echelon

Das größte Spionage-System der Welt heißt Echelon. Mit Hilfe von mehr als 120 Abhör-Satelliten werden über 3.000.000 Kommunikationsverbindungen (Telefon, Fax, ISDN, ...) in der Stunde analysiert. Es werden bis zu 90 % des Kommunikationsaufkommens im Internet gefiltert. Die US-amerikanische National Security Agency (NSA) beschäftigt zu diesem Zweck 140.000 Mitarbeiter, davon 20.000 bis 30.000 Mathematiker, und ist damit der weltweit größte Arbeitgeber für Mathematiker. Mit einem Budget von mehr als 10 Milliarden US-$ – sechsmal so viel wie das Budget des CIA – kann die NSA der militärischen und wirtschaftlichen Spionage »erfolgreich« nachgehen.

Kennen Sie Bad Aibling?

Bad Aibling ist das älteste Moorbad Bayerns, 50 Kilometer südöstlich von München im Mangfalltal gelegen, ein hübscher Kurort mit 16.000 Einwohnern. Er bietet einen schönen Ausblick auf die Tölzer Berge und über das Inntal (`www.kur-online.de`).

Gleichzeitig ist Bad Aibling der Standort eines US-Luftwaffengeländes mit einer Abhörstation. Unter der Leitung der NSA wird hier jede Art von Kommunikation abgehört und decodiert, die für die Sicherheit der USA von Interesse sein könnte.

Neben dem kaum vorstellbaren organisierten Abhören nimmt die NSA immer wieder (auf politischem oder finanziellem Weg – die Mittel dafür sind vorhanden) Einfluss auf Unternehmen, damit diese in ihre Sicherheitsprodukte sogenannte Trap-Doors oder andere verborgene Möglichkeiten einbauen. Diese Praxis ist durch viele Beispiele in der Vergangenheit belegt worden (Crypto AG, Lotus Notes, Microsoft, usw.).

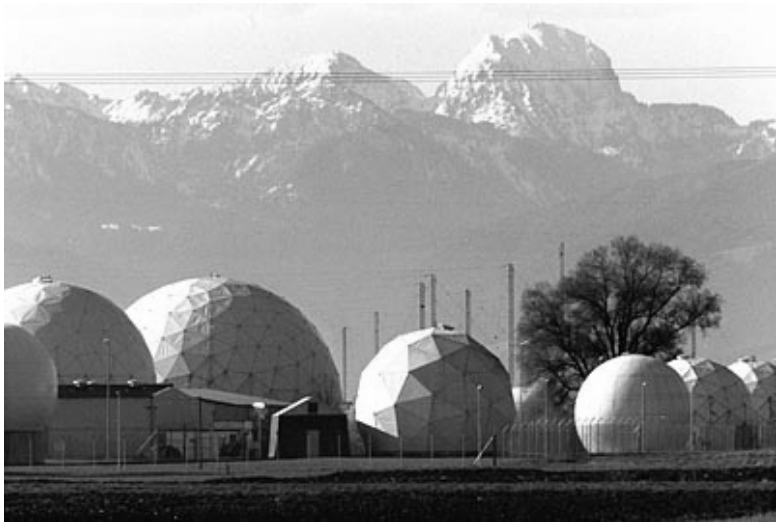


Abb. 3.10: Abhörstation der NSA in Bad Aibling

3.3 Wie hoch ist das Risiko?

Bei der Betrachtung der oben dargestellten potentiellen Bedrohungen stellt sich die Frage, wie groß die Eintrittswahrscheinlichkeit von Angriffen ist. Bei der Einschätzung des Angriffsrisikos spielen drei Faktoren eine wesentliche Rolle: Die lokalen Gegebenheiten, der Wert beziehungsweise die Verwertbarkeit der Daten und die Frage, wie hoch technischer und materieller Aufwand für einen Angreifer sind.

In Bürogebäuden mit mehreren Firmen verlaufen die Datenleitungen oft durch die Räumlichkeiten anderer Firmen oder sind im Hausanschluss-Raum für jedermann zugänglich. In diesem Fall ist es kein Problem, eine geeignete Stelle zu finden, an der die Datenleitungen angezapft werden können (Abb. 3.10).

Mögliche Angriffspunkte liegen auf den Fluren, in Kabelschächten, in der Tiefgarage und an den Einspeisungspunkten von Versorgungsunternehmen. Das sind zum Beispiel die Telefonanschlusskästen, die oft gleich neben den Mülltonnen stehen. Die leichte und für potentielle Angreifer relativ risikolose Zugänglichkeit der Datenleitungen erhöht die Gefahr, besonders dann, wenn der Wert der Daten einen Angriff auf das Rechnersystem lohnenswert erscheinen lässt.

Technisch ist das Anzapfen solcher Leitungen selbst für Laien kein Problem. Die Kosten für ein Analysegerät, mit dem die Kommunikationsdaten intelligent analysiert werden können, liegen zwischen 2 500 EUR und 5 000 EUR. Außerdem stehen im Internet zunehmend kostenlose Angriffstools zur Verfügung, mit denen »intelligente« Angriffe auf Rechnersysteme durchgeführt werden können.

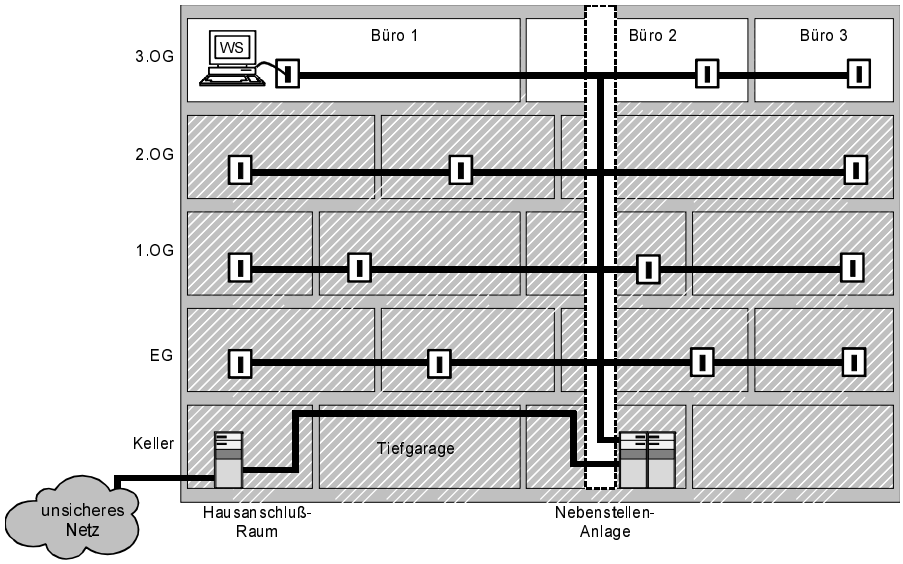


Abb. 3.11: Lokale Gegebenheiten, die das Angriffsrisiko erhöhen

Fazit

Die jeweiligen lokalen Gegebenheiten, die technische Machbarkeit und die relativ niedrigen Beschaffungskosten für Analysegeräte machen das Angriffsrisiko sehr hoch, vor allem, wenn der Angreifer sich davon ein lohnendes Geschäft versprechen kann.

Seit Jahren wächst die Computerkriminalität überdurchschnittlich. Da in den nächsten Jahren immer mehr Geschäftsprozesse über Rechner- und Kommunikations-Systeme abgewickelt werden, wird dieser Trend anhalten, wenn keine höheren Sicherheitsmaßnahmen eingeführt werden.

3.4 Schadenskategorien und Folgen

Um mögliche Schäden besser einschätzen zu können, werden nachfolgend einige typische Schadenskategorien erläutert /BSI99/. Diese beziehen sich auf die Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit.

3.4.1 Verstoß gegen Gesetze/Vorschriften/Verträge

Verstöße dieser Art können aus dem Verlust der Vertraulichkeit, der Integrität und der Verfügbarkeit resultieren. Die Schwere eines solchen Schadens ist dabei oftmals abhängig davon, ob es sich nur um einen Bagatellverstoß handelt, oder ob aus dem Vorgang rechtliche Konsequenzen für die Organisationen entstehen können. Zu den relevanten Gesetzen, Vorschriften und Verträgen gehören:

- Grundgesetz
- Bürgerliches Gesetzbuch
- Strafgesetzbuch (2. Wirtschaftskriminalitätsgesetz)
- Bundesdatenschutzgesetz und Datenschutzgesetze der Länder
- Sozialgesetzbuch
- Handelsgesetzbuch
- Telekommunikationsgesetz
- Personalvertretungsgesetz
- Betriebsverfassungsgesetz
- Urheberrechtsgesetz
- Patentgesetz
- Produkthaftungsgesetz
- Organisationsanweisungen und Dienstvorschriften
- Dienstleistungsverträge im Bereich Datenverarbeitung
- Verträge, die die Wahrung von Betriebsgeheimnissen vereinbaren
- Betriebsvereinbarungen
- EU-Recht
- Völkerrecht, bi- und multilaterale Abkommen

3.4.2 Beeinträchtigung der persönlichen Unversehrtheit

Die Fehlfunktion eines Rechnersystems kann unmittelbar die Verletzung, die Invalidität oder den Tod von Personen nach sich ziehen. Die Höhe des Schadens ist am direkten persönlichen Schaden zu messen.

Beispiel:

- Verletzung einer Person durch Fehlfunktionen einer Produktionsmaschine aufgrund von Softwaremanipulation über das Internet

3.4.3 Beeinträchtigung der Aufgabenerfüllung

Gerade der Verlust der Verfügbarkeit eines Rechnersystems oder der Integrität von Daten kann die Aufgabenerfüllung in einer Organisation erheblich beeinträchtigen. Die Schwere des Schadens richtet sich hierbei nach der zeitlichen Dauer der Beeinträchtigung und nach dem Umfang der Einschränkungen der angebotenen Dienstleistungen.

Beispiele:

- verzögerte Bearbeitung von Verwaltungsvorgängen,
- verspätete Lieferung aufgrund verzögerter Bearbeitung von Bestellungen,
- falsche Liefermenge aufgrund falscher Steuerungsdaten,
- unzureichende Qualitätssicherung durch Ausfall eines Mess-Systems.

3.4.4 Negative Außenwirkung

Durch den Verlust eines der Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit in einem Rechnersystem können verschiedene negative Außenwirkungen entstehen, beispielsweise:

- Renommeeverlust einer Organisation,
- Beeinträchtigung der wirtschaftlichen Beziehungen zusammenarbeitender Organisationen,
- Vertrauensverlust gegenüber einer Organisation,
- verlorenes Vertrauen in die Arbeitsqualität einer Organisation,
- Zuspielen vertraulicher Daten an die Presse oder die Konkurrenz,
- Einbuße der Konkurrenzfähigkeit.

Die Höhe des Schadens orientiert sich an der Schwere des Vertrauensverlustes und am Verbreitungsgrad der Außenwirkung.

Ursachen für solche Schäden können vielfältiger Natur sein, unter anderem:

- Handlungsunfähigkeit einer Organisation durch Ausfall der IT-Systeme,
- fehlerhafte Veröffentlichungen durch manipulierte Daten,
- Fehlbestellungen durch mangelhafte Lagerhaltungsprogramme,
- Verstoß gegen die Schweigepflicht durch Vertraulichkeitsverlust von Daten.

Der mögliche Schaden durch eine negative Außenwirkung kann in vielen Organisationen sehr hoch sein.

3.4.5 Finanzielle Auswirkungen

Unmittelbare oder mittelbare finanzielle Schäden können durch den Verlust der Vertraulichkeit schutzbedürftiger Daten, durch die Veränderung von Daten oder durch den Ausfall eines Rechnersystems entstehen.

Beispiele:

- unerlaubte Weitergabe von Forschungs- und Entwicklungsergebnissen,
- Manipulation finanzwirksamer Daten in einem Abrechnungssystem,
- Ausfall eines IT-gesteuerten Produktionssystems und dadurch bedingte Umsatzverluste,
- Einsichtnahme in Marketingstrategiepapiere oder Umsatzzahlen.

Die Höhe des Gesamtschadens wird bestimmt durch die direkt entstehenden finanziellen Schäden und die daraus resultierenden pekuniären Folgeschäden.

3.5 Ergebnisse der KES/Utimaco-Studien

Die KES/Utimaco-Studien der Jahre 1996, 1998 und 2000 zeigen, wie der Status der Informationssicherheit in der betrieblichen Wirklichkeit in Deutschland ist. Die wichtigsten Ergebnisse finden sich konzentriert in /Görtz99/, wo folgende Fragen mit Blockdiagrammen aufgeschlüsselt sind:

- Welche Gefahren haben zu Beeinträchtigungen der IT-Sicherheit geführt?
- Wie ist die aktuelle Risikosituation in Unternehmen?
- Welche Probleme behindern die Verbesserung der Informationssicherheit?
- Wer ist für die Probleme der betrieblichen Informationssicherheit verantwortlich?
- Welche Maßnahmen werden zum Schutz der Kommunikation in öffentlichen Netzen angewandt?

3.6 Zusammenfassung

Mit dem enormen Anwachsen von Kommunikationsnetzen wie Internet und Intranets in der modernen Informationsgesellschaft wächst auch das Risiko, dass Daten manipuliert oder gestohlen werden können und dadurch ein Schaden auftritt.

Wir sind zwar nicht in der Lage, die Bedrohungen zu beeinflussen, aber wir können dafür sorgen, dass unsere Verletzbarkeit reduziert wird.

Aus diesem Grund wird es in Zukunft immer wichtiger, die Kommunikations-Systeme sicherer zu gestalten, damit eine vertrauenswürdige und beherrschbare Kommunikation realisiert werden kann.

Immer größere Bedeutung erlangen dabei aktive Abwehrmechanismen wie Security Audit-Systeme und Intrusion-Detection-/Response-Systeme. Schließlich können große Organisationen unmöglich ihren IT-Betrieb herunterfahren, nur weil jemand zum Beispiel an den Ports »fingert«.

Allerdings verbleibt trotz aller Sicherungsmaßnahmen immer noch ein kleines Restrisiko. Jede Organisation tut gut daran, Notfallpläne für den »Fall der Fälle« auszuarbeiten, in dem Verfahren und Zuständigkeiten festgelegt werden. Diese Pläne sollten von Zeit zu Zeit auch in einem Manöver getestet werden, um im Ernstfall Panik und damit unter Umständen zusätzlichen Schaden zu verhindern.

Ein abschließender Hinweis

In diesem Kapitel wurden prinzipiell die Gefahren aus dem Netz erklärt. Dies musste ohne Anspruch auf Vollständigkeit und Detailtiefe geschehen, sonst hätte es den Rahmen dieses Fachbuchs überschritten. Jeder Interessierte sollte sich bei Bedarf weiter informieren, beispielsweise in Web-Foren.

Besonders aktuell ist der 14-täglich verschickte »Security-Newsletter« aus dem INTEREST-Verlag. Er ist im Abonnement des »Organisationshandbuchs Netzwerksicherheit« enthalten und kann mit einem E-Mail-Warndienst kombiniert werden (siehe: `www.interest.de`).

Kapitel 4

Grundlegende Sicherheitsmechanismen

Im Kapitel 4.1 werden zuerst einige grundlegende Sicherheitsmechanismen beschrieben, mit denen Kryptographiekonzepte für VPN-Systeme aufgebaut werden können. Anschließend erfolgt die Beschreibung der eigentlichen kryptographischen Algorithmen und der zur Verwaltung von Schlüsseln benötigten Infrastruktur.

4.1 Sicherheitsmechanismen für Verschlüsselung und Digitale Signatur

Dieses Kapitel erklärt Sicherheitsmechanismen, mit denen Daten auf ihrem Weg über öffentliche Netze geschützt werden können. Sicherheitsmechanismen sind die Werkzeuge, mit denen die jeweils erforderlichen Sicherheitsdienste wie Verschlüsselung und Digitale Signatur realisiert werden können.

Die Vertraulichkeit von Daten kann nur gewährleistet sein, wenn die Übertragung der Daten verschlüsselt erfolgt. Bei der Verschlüsselung gibt es verschiedene Verfahren (siehe auch /Rula94/).

4.1.1 Private-Key-Verfahren

Verschlüsselungsverfahren, die für die Verschlüsselung von Daten den gleichen Schlüssel verwenden wie für ihre Entschlüsselung, werden als symmetrische oder Private-Key-Verfahren bezeichnet.

Eines der bekanntesten, am weitesten verbreiteten und meistuntersuchten symmetrischen Verschlüsselungsverfahren ist der DES-Algorithmus, der 1978 in den USA normiert wurde (ANSI X3.92). DES steht für »Data Encryption Standard«. Der DES-Algorithmus wird heute meist als Triple-DES mit 112 Bit effektiver Schlüssellänge verwendet, wobei der DES-Algorithmus dreimal durchlaufen wird und zwar entweder mit zwei oder drei verschiedenen Schlüsseln (Abfolge A-B-A oder A-B-C). Bei dreimaligem Durchlauf mit je 56-Bit Schlüssellänge entspricht die Sicherheit des Verfahrens aber nicht etwa derjenigen einer einmaligen Verschlüsselung mit der Schlüssellänge von 3 * 56 Bit = 168 Bit, sondern ist geringer. Kryptologen haben deshalb den Begriff »effektive Schlüssellänge« eingeführt.

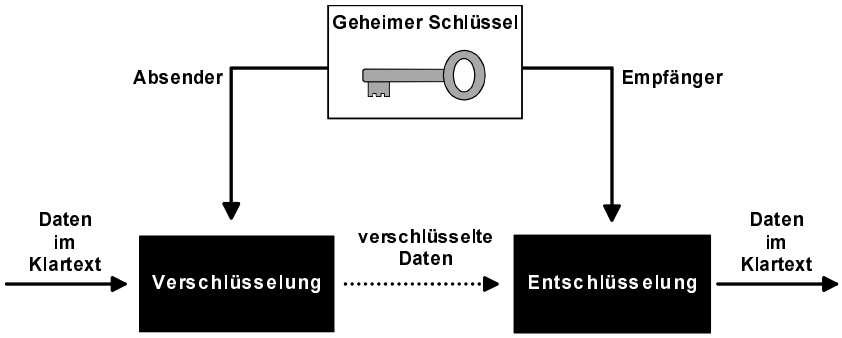


Abb. 4.1: Symmetrisches Verschlüsselungsverfahren (Private-Key-Verfahren)

Weitere symmetrische Verschlüsselungsverfahren sind beispielsweise IDEA (International Data Encryption Algorithm) und Safer (Secure And Fast Encryption Routine).

Zukünftig wird vermehrt der neue AES (Advanced Encryption Standard) verwendet, der mit einer Schlüssellänge von bis zu 256 Bit arbeitet.

Ein wesentlicher *Nachteil von Private-Key-Verfahren* (z.B. DES) ist, dass beide Kommunikationspartner über den gleichen Schlüssel verfügen müssen. Der Schlüssel, von dessen Geheimhaltung die Sicherheit abhängt, muss von einem Kommunikationspartner an den anderen übermittelt werden. Dies ist ein Unsicherheitsfaktor, dessen Risiko minimiert werden muss, indem man eine sichere Methode zur Schlüsselverteilung findet. Im Extremfall könnte dies die persönliche Übermittlung durch einen Kurier sein. Das Sicherheitsrisiko besteht darin, dass die Schlüssel, die geheimgehalten werden müssen, durch Nachlässigkeit, Vorsatz oder Zufall in falsche Hände geraten können.

Der *Vorteil von Private-Key-Verfahren* (z.B. DES) ist, dass sie sehr schnell sind. Es gibt zur Zeit schon Hardware-Lösungen, die bis zu 2,4 GBit/s und Software-Lösungen, die mehr als 100 MBit/s verschlüsseln.

4.1.2 Public-Key-Verfahren

Um das klassische Problem der Kryptographie, die Schlüsselverteilung, zu vereinfachen, wurden Verfahren entwickelt, die mit sogenannten öffentlichen Schlüsseln (Public Keys) arbeiten. Ein Public-Key-Verfahren oder asymmetrisches Verfahren arbeitet mit zwei verschiedenen Schlüsseln. Wird eine Verschlüsselung mit einem der beiden Teilschlüssel durchgeführt, kann nur mit dem dazu passenden Teilschlüssel die korrekte Entschlüsselung erfolgen.

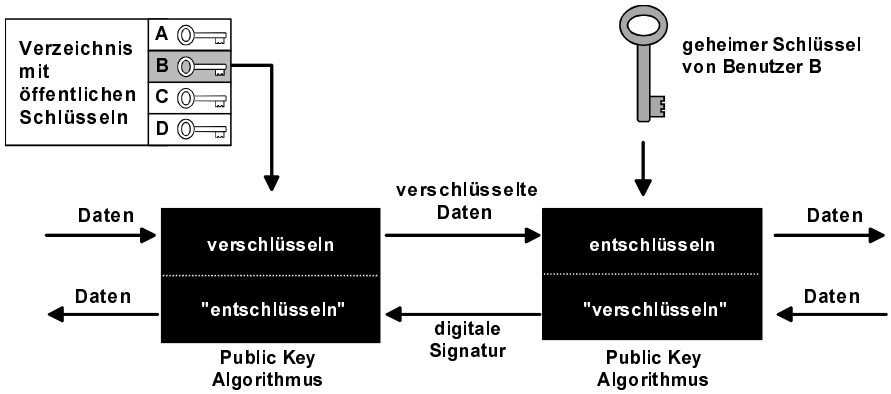


Abb. 4.2: Asymmetrisches Verschlüsselungsverfahren (Public-Key-Verfahren)

Aus der Kenntnis des einen Teilschlüssels kann der andere nicht berechnet werden. Aus diesem Grund kann ein Teilschlüssel ohne Bedenken veröffentlicht werden. Diesen bezeichnet man als »öffentlichen Schlüssel« (Public Key). Der andere Schlüssel muss geheimgehalten werden und heißt dementsprechend »geheimer Schlüssel« (Private Key) /Pohl90/.

Digitale Signatur

Eine wichtige Anwendung des Public-Key-Verfahrens ist die Digitale Signatur.

Daten, die mit einem bestimmten geheimen Schlüssel »verschlüsselt« wurden, können nur mit Hilfe des dazugehörigen öffentlichen Schlüssels wieder »entschlüsselt« werden (siehe Abb. 4.2). Hat nun eine Person die Daten mit ihrem geheimen Schlüssel digital signiert, kann mit Hilfe des öffentlichen Schlüssels überprüft werden, ob die digitale Signatur wirklich von dieser Person stammt.

Die erfolgreich durchgeführte Überprüfung ist der Beweis für die Authentizität der Signatur. Mit dem Prinzip der Digitalen Signatur steht somit ein Äquivalent zur handgeschriebenen Unterschrift zur Verfügung.

Das bekannteste Public-Key-Verfahren ist das RSA-Verfahren, mit dem gleichzeitig signiert und verschlüsselt werden kann (Das Kürzel RSA steht für die Entdecker Ron Rivest, Adi Shamir, Leonard Adleman).

Vertraulicher Austausch von Sicherheitsinformationen

Wird eine Information zuerst mit dem öffentlichen Schlüssel einer bestimmten Person verschlüsselt, kann diese Information nur von der Person, die den geheimen Schlüssel besitzt, rekonstruiert werden. Diese Anwendung erlaubt den vertraulichen Austausch sicherheitsrelevanter Informationen – zum Beispiel von Schlüsseln für symmetrische Verfahren wie DES.

Vorteile von Public-Key-Verfahren sind die Einsatzmöglichkeiten für ein einfaches Key-Management (Schlüsselverteilung) und für die Digitale Signatur.

Ein Nachteil von Public-Key-Verfahren ist, dass sie aufgrund ihrer Herkunft aus der Komplexitätstheorie sehr rechenaufwändig und deshalb nicht für die Verschlüsselung von großen Datenmengen geeignet sind.

4.1.3 One-Way-Hashfunktion

Die Digitale Signatur entspricht einer Operation mit dem Public-Key-Verfahren und ist daher sehr rechenintensiv.

Um den Aufwand zu vermindern, berechnet man nicht die gesamte Information mit dem Public-Key-Verfahren, sondern erstellt ein »Konzentrat« der Nachricht, das dann digital signiert wird.

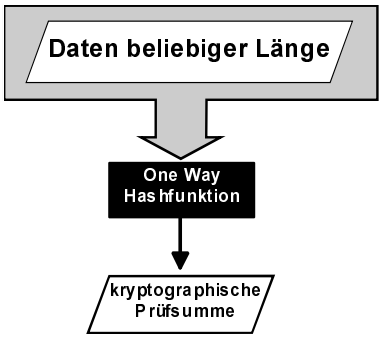


Abb. 4.3: One-Way-Hashfunktion

Auf eine Nachricht, deren Länge variabel ist, wird eine sogenannte One-Way-Hash-Funktion angewendet, die eine kryptographische Prüfsumme fester Länge als Ergebnis erzeugt. Zu den besonderen Eigenschaften von One-Way-Hash-Funktionen gehört, dass die Berechnung des Funktionswerts einfach ist, während es aber praktisch unmöglich ist, systematisch einen Wert zu finden, der dieselbe kryptographische Prüfsumme ergibt. Es ist also unmöglich, die Daten aus dem Hashwert zu ermitteln.

Eine kryptographische Prüfsumme muss eine Vielzahl von weiteren Eigenschaften aufweisen, die in ISO 10118 sowie in der Fachliteratur beschrieben sind. Verfahren in der Praxis sind unter anderem die One-Way-Hashfunktionen RIPEMD (EU-Projekt Réseaux IP Européens Message Digest), MD5 (Message Digest) und SHA-1 (Secure Hash Algorithmus).

4.1.4 Hybride Verschlüsselungstechnik

Da Public-Key-Verfahren wegen ihrer Komplexität zur Verschlüsselung von großen Datenmengen nicht geeignet sind und bei symmetrischen Verfahren die Schlüsselverteilung zu aufwändig ist, erweist sich eine Kombination von beiden als ideale Lösung: Die eigentliche Verschlüsselung der Daten eines Dokuments wird mit einem symmetrischen Verfahren (beispielsweise mit dem Triple-DES-Verfahren) durchgeführt, jedoch der Schlüssel für seine Verteilung mit dem Public-Key-Verfahren verschlüsselt wird. Eine Kombination des symmetrischen mit dem asymmetrischen Verschlüsselungsverfahren bietet neben der höchstmöglichen Sicherheit die Vorzüge der praktischen Handhabung.

4.1.5 Ein Wettlauf um die Sicherheit

Für die Sicherheit einer Verschlüsselung sind vier Faktoren ausschlaggebend:

- der verwendete Algorithmus,
- die Schlüsselgenerierung,
- die Schlüssellänge sowie
- die Aufbewahrung des Schlüssels.

Bei symmetrischen Verschlüsselungsverfahren geht man heute davon aus, dass die Praxissicherheit gegeben ist, wenn man eine Schlüssellänge von 128 Bit und mehr verwendet.

Eine vollständige Suche zur Entschlüsselung hieße, 2^{128} Schlüssel auszuprobieren. Damit stößt man auf ein praktisches Problem, denn mit den derzeitigen Ressourcen ist die Berechnung nicht in einer angemessenen Zeit möglich. Da aber die Geschwindigkeit von Computern, die man für diesen Angriff nutzen kann, immer weiter steigt, müssen in der Folge auch die Schlüssellängen von Zeit zu Zeit entsprechend vergrößert werden. Galt vor 10 Jahren noch eine praktische Sicherheit bei einer Schlüssellänge von 64 Bit als gegeben, so sind heute 128 Bit und in naher Zukunft 256 Bit erforderlich.

Gleiches gilt auch für Public-Key-Verfahren. In der Vergangenheit galt eine Schlüssellänge von 512 Bit als »sicher«, heute sind es 1024 Bit. Um langfristig Sicherheit zu gewährleisten, wird man zur Verwendung von 2048-Bit-Schlüsseln übergehen müssen.

Trotz aller Bemühungen gibt es keine absolute Sicherheit, da die Sicherheit anwendbarer Algorithmen mathematisch nicht bewiesen werden kann. Ein Algorithmus gilt dann als »sicher«, wenn fünf Jahre nach seiner Veröffentlichung die Mathematiker der Welt nicht in der Lage sind, ihn erfolgreich mathematisch anzugreifen. Nicht publizierte »geheime« Algorithmen gelten – weil nicht durch Experten überprüfbar – als »unsicher«.

4.1.6 Zertifizierungs-Systeme

Ein offenes Problem bei Public-Key-Verfahren ist die Frage, wie der öffentliche Schlüssel auf vertrauenswürdige Weise zum Kommunikationspartner gelangt. Selbst wenn man öffentliche Schlüssel verwendet, müssen diese authentisch ausgetauscht werden. Eine elegante Möglichkeit, öffentliche Schlüssel authentisch auszutauschen, ist die Einrichtung eines Zertifizierungs-Systems oder Trustcenters.

Der öffentliche Schlüssel jedes Benutzers wird dem Rechnersystem in Form eines Zertifikats von der vertrauenswürdigen dritten Instanz – der Zertifizierungs-Instanz – zur Verfügung gestellt. Dieses Sicherheitsprinzip ist im Directory-Authentication Framework /CCITT/ beschrieben.

Bei der Authentikation von Personen mit Hilfe von Ausweisen (Personalausweis, Reisepass usw.) fungieren die Behörden (Einwohnermeldeämter) als vertrauenswürdige dritte Instanz. Nachdem sich eine Person vorgestellt hat, kann man mit Hilfe eines Ausweises die Echtheit dieser Aussage verifizieren. Eine entsprechende Funktionalität muss zur Verfügung gestellt werden, um komplexe Sicherheitssysteme elektronisch zu realisieren.

Eine PKI stellt in aller Regel zentrale Sicherheitsdienste zur Verfügung, schafft also die Voraussetzungen dafür, daß eine Anwendung vertrauenswürdig realisiert werden kann.

Das folgende Bild zeigt im oberen Teil den prinzipiellen Aufbau einer Public-Key-Infrastruktur sowie einige Kommunikationskanäle. Im unteren Bereich ist schematisch eine Anwendung abgebildet, die auf der PKI-Grundfunktionalität basiert.

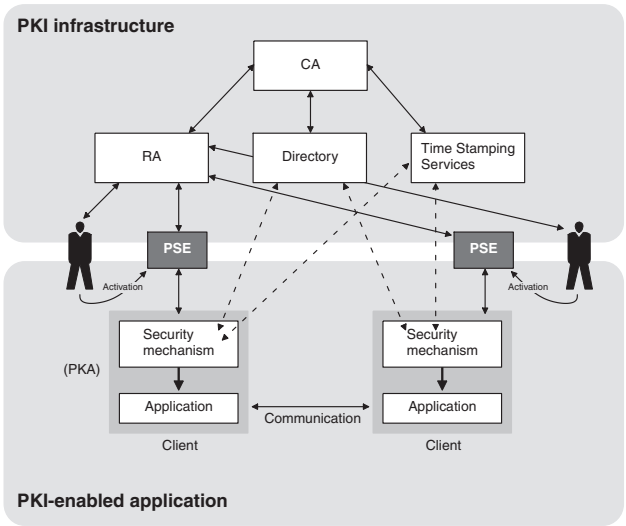


Abb. 4.4: PKI und PKA

Aufgaben und Komponenten einer PKI

Public-Key-Infrastrukturen bestehen aus Hardware, Software und einem abgestimmten Regelwerk, der Policy.

Die Policy definiert, nach welchen Sicherheitsregeln die Dienstleistungen erbracht werden. Dazu zählt das Betriebskonzept der PKI, die Benutzerrichtlinien sowie Organisations- und Arbeitsanweisungen.

Im Allgemeinen ist es üblich, die Registrierung der Teilnehmer und die Zertifizierung der Schlüssel voneinander zu trennen und zum Teil auch an unterschiedlichen Orten vorzunehmen.

Die **Registration Authority (RA)** kann als private (innerhalb einer Organisation) oder öffentliche Einrichtung betrieben werden. Ihre Hauptaufgabe besteht darin, die Anträge auf Zertifizierung zu erfassen und die Identität der Antragsteller entsprechend der Policy zu prüfen. Die Identitätsprüfung kann sehr einfach, z. B. per E-Mail, oder auch aufwendiger und sicherer, z. B. durch persönliches Erscheinen und Vorlage des Ausweises, erfolgen.

Die Registration Authority bildet die Schnittstelle zwischen den Teilnehmern bzw. Antragstellern und der **Certification Authority (CA),** an die sie die Anträge weiterleitet.

Die **Certification Authority** vergibt eindeutige Identitäten und verwaltet für jeden Teilnehmer ein oder mehrere Schlüsselpaare mit den dazugehörigen Zertifikaten. Jedes von der CA erzeugte Zertifikat verbindet den öffentlichen Schlüssel des Teilnehmers mit dessen Namen und zusätzlichen Daten (Gültigkeitszeitraum, Seriennummer, evtl. weitere Attribute).
Die Certification Authority gibt die Zertifikate aus und verwaltet sie, damit die öffentlichen Schlüssel und Attribute (Position im Unternehmen, Rechte usw.) der Teilnehmer möglichst einfach verifiziert werden können.

Zur Verwaltung der Zertifikate unterhält jede PKI einen **Directory Service**. Hier werden die gültigen zertifizierten öffentlichen Schlüssel der Teilnehmer veröffentlicht. Zurückgezogene oder kompromittierte Schlüssel werden in einer Sperrliste (**»Certificate Revocation List«, CRL**) zum Abruf bereitgehalten.

Ein **Zeitstempeldienst** dient dazu, gesicherte Zeitsignaturen gemäß der Policy zu erstellen. Damit wird ein Dokument oder eine Transaktion mit der aktuellen Zeitangabe verknüpft und diese Gesamtinformation anschließend digital signiert.

Das **Personal Security Environment (PSE)** ist die Sammlung aller sicherheitsrelevanten Daten eines Teilnehmers. Dazu gehören seine geheimen Schlüssel, die Zertifikate seiner Kommunikationspartner sowie der öffentliche Schlüssel der Zertifizierungsinstanz.

PKI-enabled Application

Als »PKI-enabled Application« (PKA) wird eine Anwendung bezeichnet, die auf der Grundlage der von der PKI zur Verfügung gestellten Sicherheitsdienste (Zertifikate, Verzeichnisdienst etc.) eine vertrauenswürdige Nutzung ermöglicht. Eine PKA enthält selbst unterschiedliche Sicherheitsmechanismen oder -verfahren (Authentisierung, Verschlüsselung etc.), mit denen Vertrauenswürdigkeit (Authentizität, Integrität, Verbindlichkeit, Einmaligkeit und Vertraulichkeit) erzielt wird.

Eine PKI bildet die Sicherheitsgrundlage für die vertrauenswürdige Nutzung von Anwendungen wie

- E-Mail
- Dokumentverschlüsselung (z. B. von MS-Office-Dokumenten)
- Transaktionen im Finanzbereich (EDIFACT)
- XML Prozessen
- SSL-Kommunikation
- VPN-Kommunikation
- Identifikations- und Authentisierungsprozessen
- Zahlungssystemen

Modelle von Public-Key-Infrastrukturen

Es gibt prinzipiell verschiedene Modelle von Public-Key-Infrastrukturen, die im folgenden kurz dargestellt werden:

- **Geschlossene Systeme**
  Eine Organisation betreibt eine PKI für eine oder mehrere Anwendungen (PKAs), die in ihrem eigenen Verantwortungsbereich liegen. Sicherheitsdienste wie z. B. gesicherte Kommunikation oder Authentisierung stehen nur innerhalb der Infrastruktur zur Verfügung.

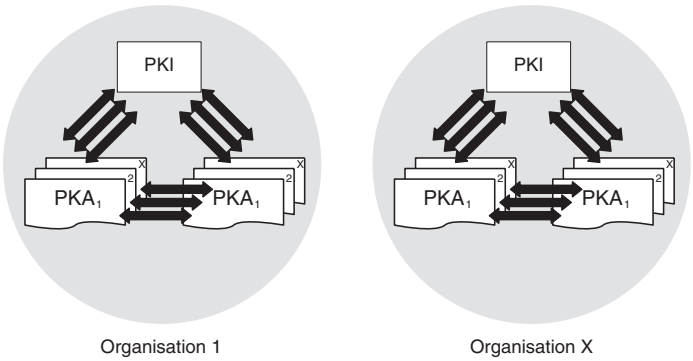


Abb. 4.5: Geschlossene PKI-Systeme

- **Offene Systeme**
  Mehrere Organisationen betreiben PKIs für eine oder mehrere Anwendungen, die in den Verantwortungsbereichen der unterschiedlichen Organisationen liegen. So ist z. B. die gesicherte Kommunikation zwischen den Organisationen möglich. Der Austausch beruht auf gegenseitigem Vertrauen sowie auf kompatiblen Technologien und Verfahren.

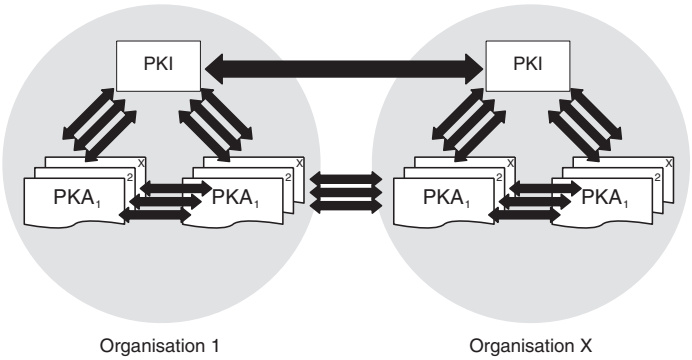


Abb. 4.6: Offene PKI-Systeme

- **Zentral administrierte Systeme**
  Ein PKI-Anbieter betreibt die PKI für eine oder mehrere Anwendungen, die in den Verantwortungsbereichen der sie nutzenden Organisationen liegen. Wenn die verschiedenen Organisationen der zentralen PKI vertrauen und kompatible Technologien und Verfahren verwendet werden, kann eine vertrauenswürdige Kommunikation realisiert werden.

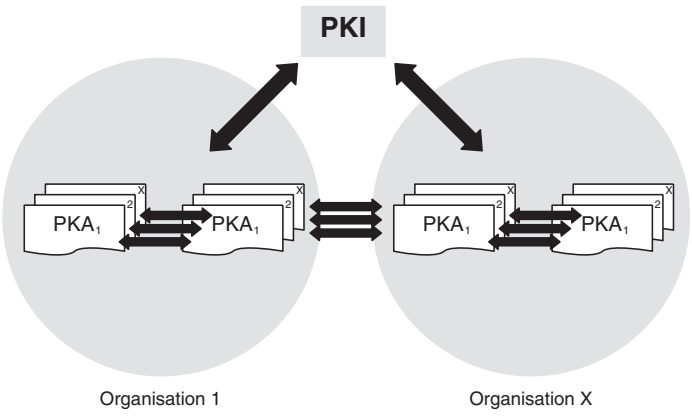


Abb. 4.7: Zentral administriertes PKI-System

Probleme mit PKIs in der Praxis

Bei der Nutzung von PKIs gab und gibt es einige Probleme, die im Folgenden diskutiert werden.

- Probleme bei geschlossenen Systemen
  »Geschlossenes System« bedeutet, dass die PKI nur innerhalb einer Organisation verwendet wird und nicht für die Kommunikation nach außen genutzt werden kann. Da jedoch in der Praxis viele organisationsübergreifende Prozesse stattfinden, ist der Nutzen einer solchen PKI sehr eingeschränkt.

- Probleme bei offenen Systemen
  Bei offenen Systemen muss zum Aufbau einer organisationsübergreifenden Kommunikation ein Abgleich der verschiedenen organisationsspezifischen Policies erfolgen. Ziel ist ein gemeinsames »Level of Trust«. Hier müssen geeignete Instrumente implementiert werden, um die organisatorischen sowie die IT-infrastrukturellen Konzeptionen zu bewerten, zu analysieren und zu gewichten.

  Gerade bei der Nutzung für personenbezogene organisationsübergreifende Prozesse stellt sich aus ökonomischer Sicht und aus den tatsächlichen Anforderungen heraus die Frage, ob das Signaturgesetz zwingend die Grundlage für die PKI und die zum Einsatz kommenden PKAs bilden muss. Hierbei muss berücksichtigt werden, dass viele organisationsübergreifende Prozesse automatisiert sind und somit nicht mehr personenbezogen arbeiten. Die Kardinalfrage in diesem Zusammenhang ist, ob innerhalb des Sicherheitskonzepts der PKI beispielsweise die Verantwortlichkeit für von Servern erstellte Signaturen geregelt ist (Haftungsausschluss).

  Hinzu kommt, dass eine Vielzahl von unterschiedlichen, teilweise sehr komplexen Standards existiert, die darüber hinaus der ständigen Weiterentwicklung unterliegen. Die Ursache hierfür liegt in der großen Vielfalt der Anwendungen (SSL, E-Mail etc.) und den daraus resultierenden besonderen Anforderungen.

- Unterschiedliche Verantwortung für PKIs und PKAs in Unternehmen
  Ein weiteres Problem, dem insbesondere große Organisationen gegenüberstehen, beruht darauf, dass die PKAs und PKIs zwar voneinander abhängig sind, aber häufig organisatorisch getrennt werden. In derartigen Fällen müssen sich beispielsweise verschiedene Abteilungen auf gemeinsame Ziele und Vorgehensweisen verständigen, um die entsprechenden technologischen Grundlagen zu erarbeiten.

- »Henne-Ei-Problem«
  Public-Key-Infrastrukturen sind nur dann ökonomisch sinnvoll, wenn der Einsatz dieser Strukturen und damit der vertrauenswürdige Ablauf von Geschäftsprozessen so umfassend wie möglich realisiert wird, d.h. wenn die gesicherte

Kommunikation mit so vielen Partnern wie möglich stattfinden kann. Voraussetzung dafür ist der konsequente Einsatz der bestehenden Technologien und die Umsetzung der Security Policies.

Die Realität ist aber, dass sich die beteiligten Organisationen nur schwer auf den Abgleich ihrer individuellen Sicherheitskonzepte einigen können. Dadurch gestaltet sich der Aufbau eines gemeinsamen »Level of Trust« langwierig und längst fällige Entscheidungen werden nicht getroffen. Zu viele Beteiligte nehmen noch eine abwartende Haltung ein und der Ausbau der bestehenden PKI-Infrastrukturen stagniert.

- Hoher personeller und organisatorischer Aufwand
  Die Einführung und der Betrieb einer Public-Key-Infrastruktur erfordert neben der technischen Umsetzung auch einen hohen personellen und organisatorischen Aufwand. Gerade in der Einführungsphase einer PKI ist die Sensibilisierung der Anwender für die IT-Sicherheit, die Schulung der Anwender auf die Produkte und die Planung und Durchführung des Roll-Outs ein nicht zu vernachlässigender Faktor.
- Key-Recovery bei der Verschlüsselung
  Falls Unternehmenswerte verschlüsselt werden, muss ein Verfahren realisiert werden, das bei technischen Defekten, bei einem PSE-Verlust oder beim Ausscheiden eines Mitarbeiters aus dem Unternehmen garantiert, dass die Unternehmenswerte sicher wieder entschlüsselt werden können.

Erstellung und Verifizierung von Zertifikaten

Der öffentliche Schlüssel eines jeden Benutzers wird dem System in Form eines Zertifikats zur Verfügung gestellt. Dieses enthält die Kennung der Zertifizierungsinstanz, die das Zertifikat erstellt hat, die Kennung des Benutzers, für den das Zertifikat erstellt wurde, den öffentlichen Schlüssel des Benutzers und eine Angabe zur Gültigkeitsdauer des Zertifikats (siehe Abb. 4.8).

Das Zertifikat ist von der Zertifizierungsinstanz, die es erstellt hat, digital signiert.

Jeder, der den öffentlichen Schlüssel der Zertifizierungsinstanz besitzt, ist damit in der Lage, zu überprüfen, ob der öffentliche Schlüssel eines Benutzers wirklich von der Zertifizierungsinstanz stammt.

Mit anderen Worten: Die Zertifizierungsinstanz veröffentlicht Zertifikate mit öffentlichen Schlüsseln, die die Zusammengehörigkeit von Benutzern und öffentlichen Schlüsseln bestätigen.

Nach dem Erhalt eines Zertifikats wird vom Sicherheitssystem die aktuelle kryptographische Prüfsumme über den Inhalt des Zertifikat berechnet. Außerdem wird aus der Signatur des Zertifikats und dem öffentlichen Schlüssel der Zertifizierungsinstanz unter Verwendung des Public-Key-Verfahrens die ursprüngliche kryptographische Prüfsumme berechnet.

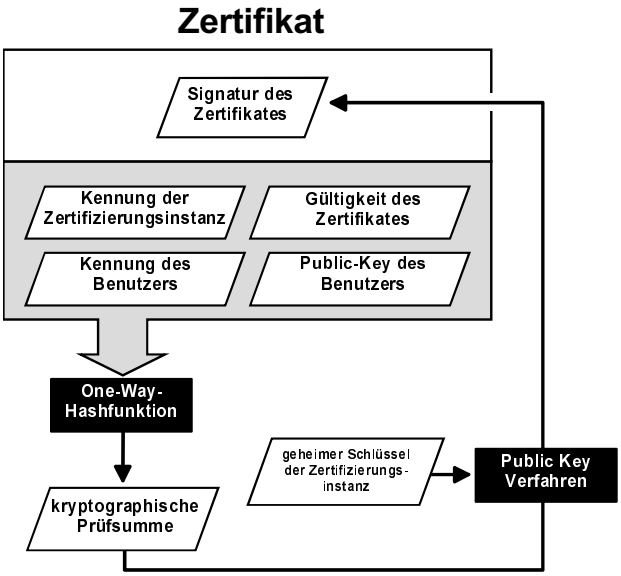


Abb. 4.8: Inhalt und Erstellung eines Zertifikats

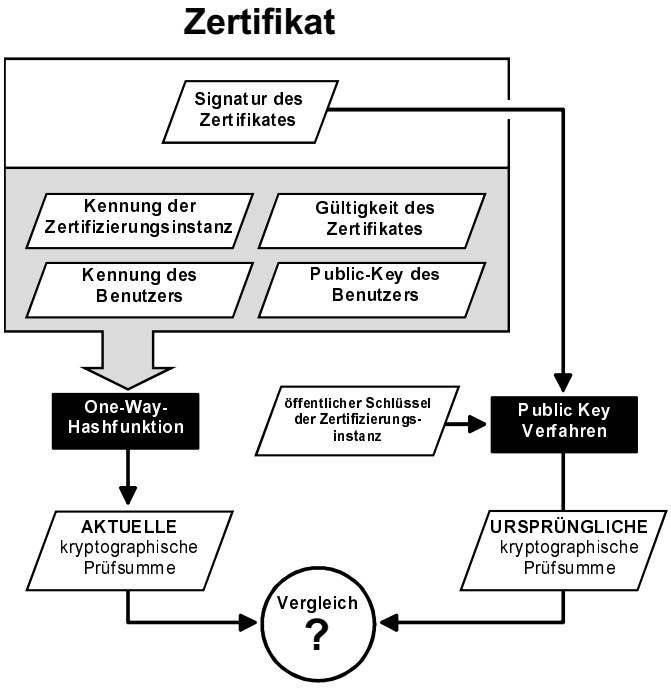


Abb. 4.9: Verifikation eines Zertifikats

Stimmen die beiden Prüfsummen überein, sind die Unversehrtheit und die Echtheit des öffentlichen Schlüssels des Benutzers, mit dem man eine Kommunikation durchführen möchte, bewiesen (siehe Abb. 4.9).

Voraussetzung ist, dass alle Benutzer des Sicherheitssystems der Zertifizierungsinstanz vertrauen können. Dazu muss die Zertifizierungsinstanz bestimmten Sicherheitsanforderungen genügen. Im Gesetz zur Digitalen Signatur werden die Sicherheitsanforderungen beschrieben, die eine Zertifizierungsinstanz erfüllen muss, die rechtlich anerkannte Zertifikate ausgeben möchte. Dazu zählen unter anderem vertrauenswürdiges Personal, zertifizierte Sicherheitskomponenten und eine vertrauenswürdige Systemumgebung. In einem globalen Sicherheitssystem können parallel oder hierarchisch verteilte Zertifizierungsinstanzen zusammengefasst sein.

Das hierarchische Schlüsselverteilverfahren ist die Grundlage für den Aufbau eines komplexen Sicherheitssystems.

4.1.7 Chipkarte (SmartCard)

Eine »intelligente Chipkarte« (»SmartCard«) ist ein Rechnersystem in der genormten Größe der EC-Karte (86 x 54 x 0,76 mm), das dem Benutzer Sicherheitsdienstleistungen zur Verfügung stellt.

Eine SmartCard enthält:

- eine CPU
- RAM- und ROM-Speicher
- ein »schlankes« Betriebssystem im ROM
- eine I/O-Schnittstelle, über die die gesamte Kommunikation stattfindet (Kontaktflächen oder kontaktloses Interface)
- ein EEPROM, auf dem die geheimen Schlüssel, zum Beispiel ein privater RSA-Schlüssel oder andere symmetrische Schlüssel, sowie persönliche Daten (Passworte etc.) sicher gespeichert sind
- sonstiges, beispielsweise einen Co-Prozessor, der symmetrische oder asymmetrische Verschlüsselung sehr schnell durchführt (Krypto-Prozessor)

Eine SmartCard stellt dem Benutzer in der Regel folgende Sicherheitsdienstleistungen zur Verfügung:

- Laden und Entladen von Werteinheiten für elektronisches Bezahlen (auch ohne Crypto-Prozessor)
- Kryptographische Anwendungen wie Digitale Signaturen usw.
- Identifikation/Authentikation des Benutzers (Aktivieren der Chipkarte)
- Single Sign On-Anwendungen (z. B. Passwort und PIN von unterschiedlichen Anwendungen)
- Lesen gespeicherter Servicedaten
- Sicheres Speichern von Daten auf der Chipkarte
- Ausführen sonstiger Rechenoperationen

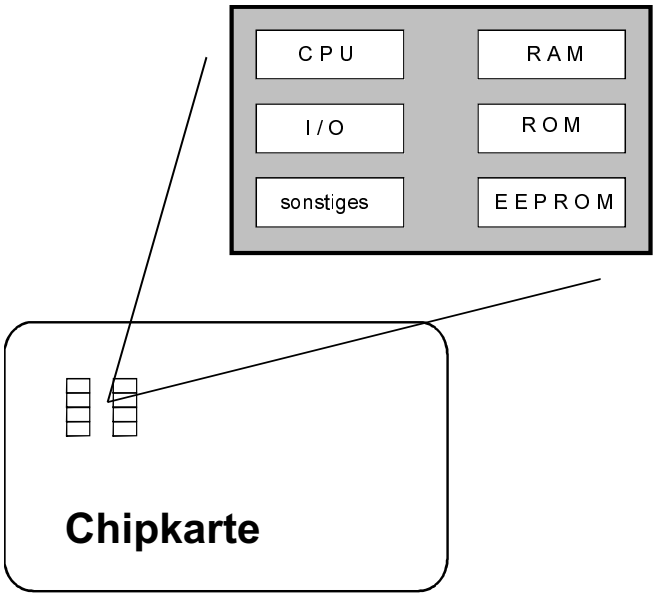


Abb. 4.10: Chipkarte

In Anwendungen wie dem Sicherheitssystem zum Schutz von elektronischen Dokumenten werden der öffentliche Schlüssel der Zertifizierungs-Instanz und der geheime Schlüsselteil des Benutzers gesichert in eine »intelligente Chipkarte« geladen. Die Chipkarte wird dann dem Benutzer vertrauenswürdig übergeben.

Aktivierung der Chipkarte

Die Chipkarte kann zum Beispiel durch ein Passwort geschützt werden. Wenn ein Benutzer des Sicherheitssystems Sicherheitsfunktionen in Anspruch nehmen will, muss er seine Chipkarte mit Hilfe seines persönlichen Passwortes aktivieren. Verliert der Benutzer seine Chipkarte, kann ein Finder diese nicht verwenden, da er das Passwort nicht kennt. Kennt jemand das individuelle Passwort eines anderen Benutzers, kann er keinen Nutzen daraus ziehen, wenn er nicht auch die Chipkarte besitzt. Außerdem kann ein Benutzer sein Passwort jederzeit ändern.

Sicherer als ein Passwort sind biometrische Identifikationsverfahren, die Körpermerkmale – zum Beispiel einen Fingerabdruck, die Stimme oder Gesichtszüge – zur eindeutigen Identifikation von Personen nutzen. Im Gegensatz zu einem Passwort kann ein solches Merkmal nicht gestohlen, verloren, vergessen oder weitergegeben werden.

Im englischsprachigen Bereich verwendet man häufig die Schlagworte »What you know« (Passwort), »What you have« (Chipkarte) und »What you are« (Biometrik) und fordert, bei einer Authentikation mindestens zwei dieser drei Verfahren zu kombinieren.

Multifunktionalität

Die Chipkarte ist so konzipiert, dass mit ihr mehrere Anwendungen möglich sind. Je nach Anwendung werden kontaktlose Chipkarten (z. B. für Zutrittssysteme) oder Chipkarten mit Kontakten verwendet.

Möglich ist zum Beispiel das Bezahlen an öffentlichen Telefonen oder an Point-of-Sales-Systemen (POS-Systemen), die Digitale Signatur von Dokumenten oder die Zugangskontrolle zu Gebäuden.

Mögliche Sicherheitsmechanismen einer SmartCard

SmartCard Hardware:

- Unter- und Überspannungsdetektion
- Erkennung niedriger Frequenzen
- gescramblete Busse
- Sensoren für Licht, Temperatur usw.
- Passivierungs- bzw. Metallisierungsschichten über Bus- und Speicherstrukturen oder über der gesamten CPU
- Zufallszahlengenerator in der Hardware
- spezielle CPU-Befehle für kryptographische Funktionen
- Speicherschutzfunktionen

SmartCard Software (z. B. Betriebssystem nach ISO 7816-4):

- Zugriffskontrolle auf Objekte
- Zustandsautomaten, die in Abhängigkeit von Identifikations- und Authentikationsmechanismen Befehle zulassen

Vorteile von SmartCards:

- Die kryptographischen Operationen werden auf der SmartCard ausgeführt. Der geheime Schlüssel verlässt die Karte niemals und kann somit nicht ausgelesen werden.
- SmartCards sind so klein wie Kredit- oder ec-Karten und können leicht überallhin mitgenommen werden.
- SmartCards sind flexibel für verschiedene Anwendungen einsetzbar.
- SmartCards sind mit Stückpreisen von 1,50 EUR bis 17,50 EUR (abhängig von der Stückzahl und dem Aufdruck) bedeutend preisgünstiger als andere Sicherheitsmodule.

Einsatzumfeld einer SmartCard

SmartCards werden typischerweise als Sicherheitskomponenten für Personen eingesetzt.

4.2 Kryptographische Algorithmen

Wie bereits erwähnt, nutzen VPNs eine Kombination von schnellen symmetrischen Verschlüsselungs-Verfahren bei der Online-Übertragung der Nutzdaten und langsamen asymmetrischen Verfahren zur Übertragung der geheimen symmetrischen Schlüssel. Nur so können die für eine Echtzeit-Übertragung erforderlichen Bandbreiten garantiert werden. Mit den zunehmenden Anforderungen bezüglich Schnelligkeit und Sicherheit wurden in der letzten Zeit vermehrt neue Verfahren entworfen, die VPN-Designer und -Entwickler in der nächsten Zeit beschäftigen werden.

Dabei ist die Länge der eingesetzten Schlüssel nur ein Kriterium, mit dem die Sicherheit eines Verfahrens bewertet werden kann. Ist das Verfahren nur mittels Brute-Force-Angriffen (Ausprobieren aller möglicher Schlüssel) zu knacken, steigt die Sicherheit exponentiell mit der Schlüssellänge. Das setzt aber ein ideales und fehlerfreies Verfahren voraus. Kann ein Algorithmus direkt gebrochen oder der Bereich für eine Brute-Force-Attacke eingeschränkt werden, tritt die Schlüssellänge als Sicherheitskriterium zurück. Verfahren, bei denen eine Entschlüsselung schneller als mittels Brute-Force vorgenommen werden kann, werden auch als »schwache Algorithmen« bezeichnet. Schwächen in Algorithmen zeigen sich manchmal erst nach Jahren, so dass eine hundertprozentige Sicherheit niemals garantiert werden kann.

4.2.1 Einführung

Ziel aller Krypto-Algorithmen ist es, eine unverschlüsselte Menge von Nutzdaten so zu manipulieren, dass der Besitzer eines passenden Schlüssels aus dem Ergebnis, den verschlüsselten Daten, den Klartext zurückgewinnen kann. Dabei wird zwischen zwei Klassen von symmetrischen Algorithmen unterschieden, den Block- und den Stromverschlüsselern.

Stromverschlüsseler

Stromverschlüsseler verschlüsseln den Klartext Bit für Bit mit einer Folge von generierten Bits, dem sogenannten Schlüsselstrom. In den meisten Fällen wird ein möglichst zufällig erzeugter Schlüsselstrom mittels einer XOR-Funktion mit dem Klartext verknüpft. Der Empfänger muss zur Entschlüsselung den gleichen Schlüsselstrom generieren können (Abb. 4.11). Ist der Schlüsselstrom eine Menge von echten Zufallszahlen, ist der Algorithmus theoretisch so abgesichert, dass Brute-Force die schnellste Angriffvariante ist.

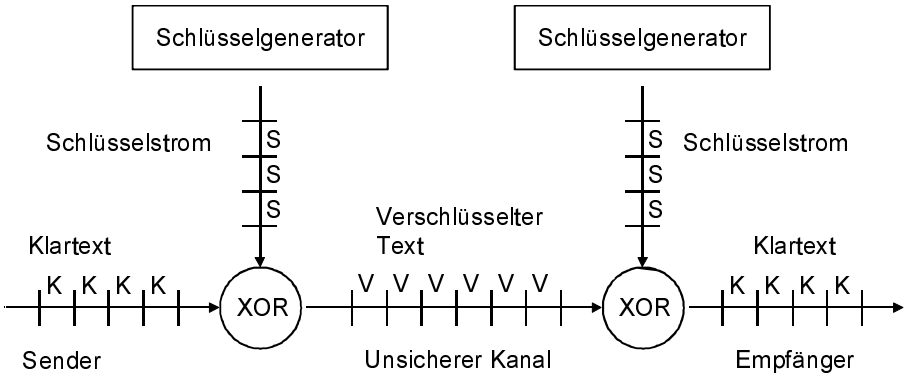


Abb. 4.11: Stromverschlüsseler

Entwickler von Stromverschlüsselern müssen sich mit dem Problem beschäftigen, wie der Schlüsselstrom des Senders zum Empfänger gelangen beziehungsweise von diesem neu berechnet werden kann. Geheimdienste verwenden oftmals Lochstreifen mit echten Zufallszahlen, die sich beim Sender und Empfänger befinden und nur ein einziges Mal benutzt werden können. Ein solches Verfahren wird auch als One-Time-PAD bezeichnet.

Da die externe Übertragung des Schlüsselstroms zum Empfänger bei der Implementierung von Online-Kommunikationsstrecken wie einem VPN nicht möglich ist, wurden Stromverschlüsseler entwickelt, bei denen Sender und Empfänger unabhängig voneinander auf beiden Seiten den Schlüsselstrom erzeugen. Dabei kann der Schlüsselstrom vom verschlüsselten Text abhängig sein oder nicht:

- Von einer synchronen Stromverschlüsselung wird gesprochen, wenn der Schlüsselstrom unabhängig vom verschlüsselten Text ist. Sender und Empfänger müssen dafür sorgen, dass der Schlüsselstrom auf beiden Seiten gleich ist (Abb. 4.12).

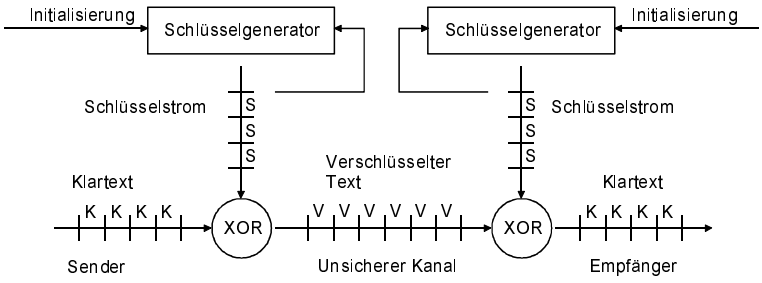


Abb. 4.12: synchroner Stromverschlüsseler

- Bei einer selbstsynchronisierenden Stromverschlüsselung ist der Schlüsselstrom eine Funktion des verschlüsselten Textes. Der interne Zustand des Algorithmus synchronisiert sich nach einer bestimmten Anzahl von entschlüsselten Bits automatisch und erzeugt anschließend den passenden Schlüsselstrom (Abb. 4.13).

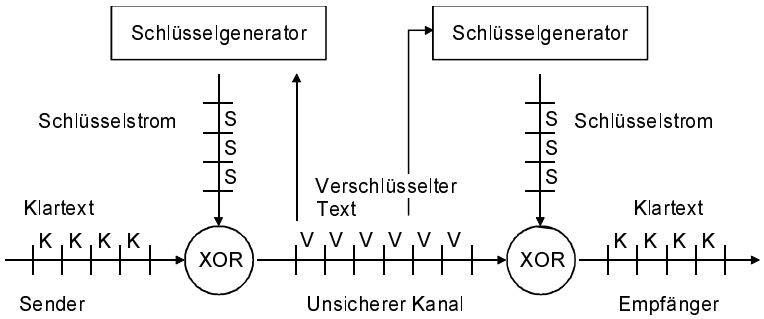


Abb. 4.13: selbstsynchronisierender Stromverschlüsseler

Blockverschlüsseler

Blockverschlüsseler zerlegen den Klartext in Blöcke konstanter Länge und erzeugen dann – abhängig vom Schlüssel – Block für Block den verschlüsselten Text. Falls der Klartext nicht exakt ein Vielfaches der Blocklänge ist, muss der letzte Block mit einem Bitmuster aufgefüllt werden (Padding). Blockverschlüsseler können ist verschiedenen Modi betrieben werden:

- Im ECB-Modus (Electronic Codebook) wird jeder Block unabhängig von den anderen verschlüsselt und gesendet (Abb. 4.14). Diese Methode birgt die Gefahr, dass ein Angreifer alte Blöcke mitschreibt und später wiederholen kann, ohne dass diese Manipulationen dem Empfänger auffällt (Replay-Angriff). Ein ECB-Verfahren kann nur komplette Blöcke verarbeiten, so dass Padding erforderlich ist.

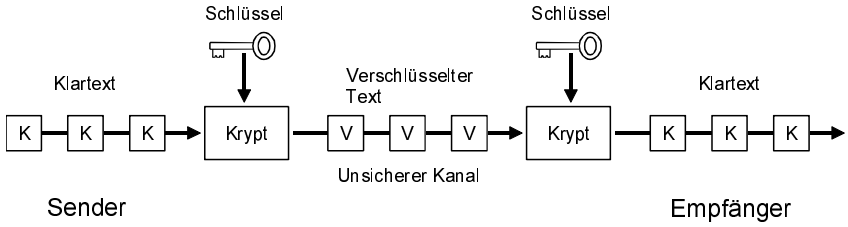


Abb. 4.14: Blockverschlüsseler im ECB-Modus

- Beim CBC-Modus (Cipher Block Chaining) findet eine Rückkopplung innerhalb des Verfahrens statt, indem ein Block des Klartextes mittels XOR mit dem letzten verschlüsselten Block verknüpft und anschließend verschlüsselt wird (Abb. 4.15). Das unbemerkte Einschleusen von Paketen ist jetzt nicht mehr möglich. Der erste Block des Klartextes wird dabei mit dem Ergebnis der Verschlüsselung einer Zufallszahl über XOR verknüpft. Diese Zufallszahl wird als Initialisierungsvektor IV bezeichnet und muss zusätzlich zum Schlüssel dem Empfänger der Nachricht übermittelt werden. Auch bei CBC können nur ganze Blöcke bearbeitet werden können.

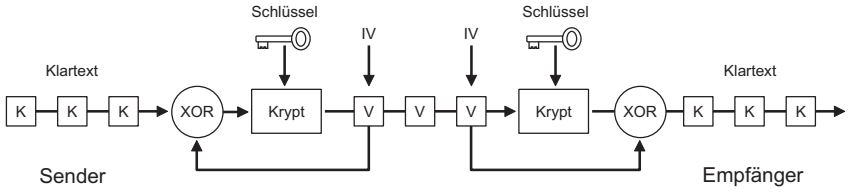


Abb. 4.15: Blockverschlüsseler im CBC-Modus

- In vielen Fällen ist es sinnvoll, aus einem Blockalgorithmus einen Stromverschlüsseler zu generieren. Das kann mit dem CFB-Modus (Cipher Feedback) geschehen, der aus einem Initialisierungsvektor IV und dem verschlüsselten Text den Schlüsselstrom erzeugt. Die zu verschlüsselnde Menge an Zeichen (meist ein Byte) wird mit dem letzten Byte des verschlüsselten IV mittels XOR verknüpft und auf die Reise geschickt. Dieses verschlüsselte Byte ersetzt zusätzlich ein einzelnes Byte des IV. Wenn acht Bytes verschlüsselt wurden und der IV ganz durch die verschlüsselten Daten ersetzt wurde, wird dieser neue Vektor verschlüsselt und steht für die nächsten XORs mit dem Klartext zur Verfügung usw. (Abb. 4.16). Da der Schlüsselstrom vom IV und den verschlüsselten Daten abhängt, handelt es sich um eine selbstsynchronisierende Stromverschlüsselung.

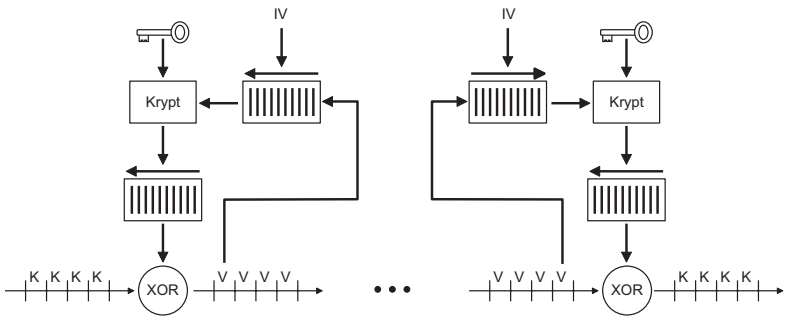


Abb. 4.16: Blockverschlüsseler im CFB-Modus

- Der OFB-Modus (Output Feedback) verläuft fast identisch zum CFB-Modus und macht ebenfalls aus einem Block- einen Stromverschlüsseler. Statt eines Bytes der verschlüsselten Daten wird jeweils das für das XOR mit den Nutzdaten benutzte Byte in das Schieberegister eingefüllt. Der Schlüsselstrom hängt nicht von Klartext oder dem verschlüsselten Text ab (Abb. 4.17), es handelt sich also um eine synchrone Stromverschlüsselung.

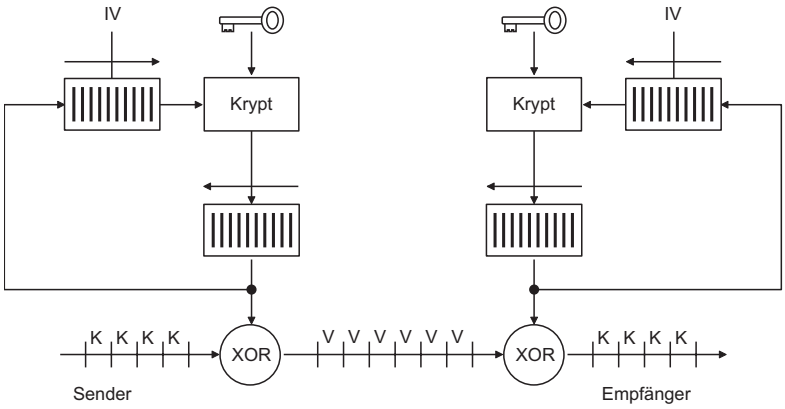


Abb. 4.17: Blockverschlüsseler im OFB-Modus

4.2.2 Symmetrische Verschlüsselungs-Verfahren

4.2.2.1 Data Encryption Standard (DES)

DES ist das wohl am weitesten verbreitete Verschlüsselungs-Verfahren. Obwohl bereits Mitte der siebziger Jahre von IBM entwickelt, konnte man ihm bis heute keine nennenswerten Schwächen nachweisen. Zahllose Applikationen auf der ganzen Welt setzen auf DES auf. In seiner ursprünglichen Implementierung hatte DES allerdings nur eine Schlüssellänge von 56 Bit, was gegen Brute-Force-Angriffe mit schneller paralleler Hardware heute als nicht mehr ausreichend gilt. Deshalb wurden Variationen von DES entwickelt, die eine größere Schlüssellänge bieten können.

Wegen der großen Verbreitung von DES gibt es zahlreiche Soft- und Hardware-Implementierungen, wobei spezielle Hardware eine verschlüsselte Übertragung von bis zu 1 GBit/Sekunde erlaubt. Die damit erzielbare Bandbreite genügt den Anforderungen an schnelle VPNs.

Beschreibung des Verfahrens

DES ist ein Blockverschlüsselungs-Verfahren, das immer ganze Datenblöcke von 64 Bit nimmt und jeden Block für sich verschlüsselt. Auch der Schlüssel hat eine Länge von 64 Bit, doch dient jedes achte Bit einer Paritätsprüfung und trägt nicht zur Verschlüsselung bei.

DES ist eine Folge von sogenannten Konfusionen und Diffusionen. Als Konfusion wird in der Kryptographie die Abbildung von Bitfolgen auf andere Bitfolgen bezeichnet. So könnte in einem trivialen Substitutions-Verfahren der Buchstabe a in den Buchstaben n, b in o usw. umgewandelt werden. Diffusion ist die Umstellung der Bits innerhalb einer Bitfolge, um das Knacken des Algorithmus mittels Häufigkeitsverteilungen zu erschweren. Eine triviale Diffusion ist die Permutation, bei der die Bits eines Blocks miteinander getauscht werden.

DES unterwirft die 64 Bit eines Blockes zunächst einer Eingangspermutation, bei der die Bits gemäß einer festen Tabelle miteinander vertauscht werden. Anschließend wird der Block in zwei Hälften zu je 32 Bit aufgeteilt. Die eigentliche Verschlüsselung besteht aus 16 »Runden«, in denen sich ebenfalls Permutationen, Substitutionen der Hälften und XOR-Operationen mit dem Runden-Schlüssel abwechseln. In jeder Runde Rx wird dabei ein anderer Anteil des Schlüssels genutzt, der aus dem Original-Schlüssel durch Permutationen erzeugt wurde. Abschließend werden die zuletzt entstandenen beiden Hälften mittels einer Schlusspermutation zu einem 64-Bit-Block kombiniert (Abb. 4.18).

Obwohl das Verfahren auf den ersten Blick etwas verwirrend erscheint, verläuft die Entschlüsselung exakt analog zur Verschlüsselung. Der verschlüsselte Text ist der Input jedes 64-Bit-Blocks, und bei Eingabe des bei der Verschlüsselung benutzten Schlüssels entsteht Block für Block der Klartext.

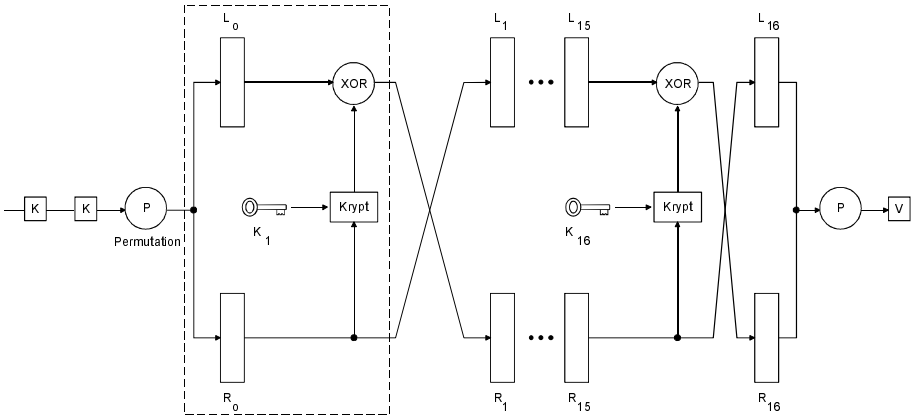


Abb. 4.18: Der DES-Algorithmus

Betriebsarten

Der DES-Algorithmus in der oben beschriebenen Form ist für viele Anwendungen nur begrenzt geeignet. Insbesondere für Terminal-Emulationen ist der Blockcharakter der Verschlüsselung ein Hindernis, da die zu übertragenden Daten in den seltensten Fällen exakt in die 64-Bit-Blöcke hinein passen. So muss gewartet werden, bis ein vollständiger Block verschlüsselt werden kann, oder es müssen unvollständige Blöcke gesendet werden. Bei vielen unvollständigen, etwa mit Nullen aufgefüllten Blöcken könnten sich Ansatzpunkte für Angreifer ergeben, da zumindest statistisch ein Teil des »Klartextes« (die Nullen) fest liegt. Um den Einsatz von DES für möglichst viele Anwendungen zu erlauben, wurden alle vier für Blockverfahren vorgesehene Betriebsarten definiert: ECB, CBC, CFB und OFB.

Bewertung der Sicherheit

Obwohl DES schon etwas in die Jahre gekommen ist, sind keine wirkungsvollen Angriffe gegen den Algorithmus selbst entwickelt worden. Die schnellste Methode des Knackens von DES-verschlüsselten Daten ist also der Brute-Force-Angriff, der gegen eine Schlüssellänge von nur 56 Bit allerdings vielversprechend erscheint. Deshalb wird DES in seiner klassischen Form heute nur noch selten eingesetzt. Mit Mehrfach-Verschlüsselung wie bei Triple-DES kann die Schlüssellänge erhöht werden. Bei höchstmöglichen Anforderungen an die Geschwindigkeit der Übertragung kann allerdings auf den klassischen DES zur Zeit nicht verzichtet werden.

Da der CBC-Modus einen guten Schutz vor eingefügten Blöcken darstellt und sich Bit-Manipulationen nur relativ gering auswirken, findet man DES (allerdings meist als Triple-DES) im CBC-Modus in vielen VPN-Implementierungen wieder.

4.2.2.2 Triple-DES

DES hat sich über Jahrzehnte hinweg als sicheres Verfahren erwiesen, einziger Nachteil ist die geringe Schlüssellänge. Deshalb schaltet man drei DES-Verschlüsselungen mit zwei oder drei Schlüsseln hintereinander, was natürlich zu einer deutlichen Verlangsamung der Ver- beziehungsweise Entschlüsselung führt. Die Verschlüsselung mit zwei Schlüsseln geschieht in der Reihenfolge A-B-A, die mit drei Schlüsseln in der Reihenfolge A-B-C (Abb. 4.19). Bei Triple-DES nach dem A-B-A Schema wird eine effektive Schlüssellänge von 112 Bit angenommen. Die effektive Schlüssellänge lässt sich mathematisch nicht geschlossen berechnen, so dass hier theoretische Überlegungen in den Vordergrund treten. Die oft zitierte effektive Schlüssellänge von 168 Bit bei einem Triple-DES nach dem Muster A-B-C ist in der Kryptographie umstritten, angenommen werden zwischen 112 und 168 Bit.

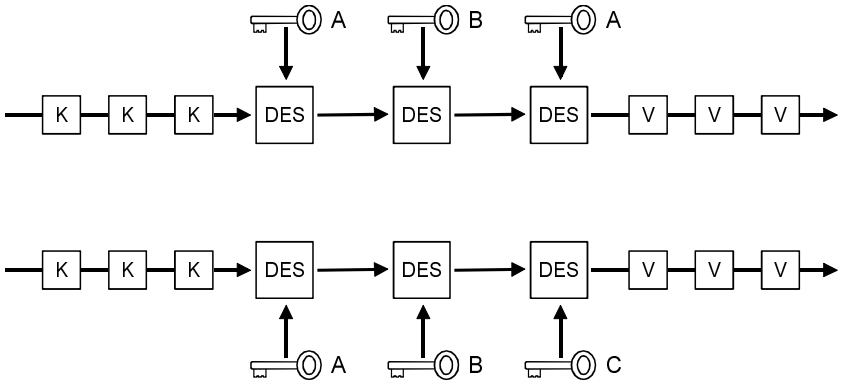


Abb. 4.19: Triple-DES in den Betriebsarten A-B-A und A-B-C

Auch Triple-DES lässt sich im CBC-Modus betreiben, wobei hier zwischen zwei Variantenunterschieden wird:

- Inner-CBC verschlüsselt die gesamte Datei dreimal hintereinander mittels DES-CBC. Bei dieser Methode sind drei Initialisierungsvektoren erforderlich (Abb. 4.20).

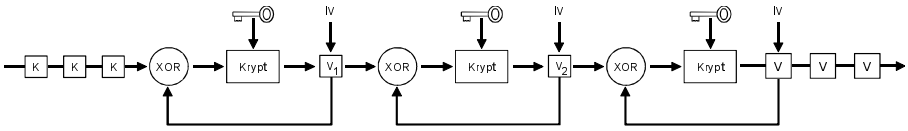


Abb. 4.20: Triple-DES im Inner-CBC-Modus

- Bei Outer-CBC durchläuft jedes Byte eine Dreifachverschlüsselung, bevor die Rückkopplung stattfindet (Abb. 4.21).

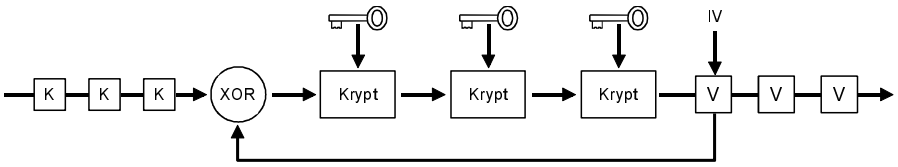


Abb. 4.21: Triple-DES im Outer-CBC-Modus

Analysen haben gezeigt, dass eine Mehrfachverschlüsselung nach dem Inner-CBC-Verfahren nur wenig mehr Sicherheit bietet als eine Einfachverschlüsselung, so dass in praktischen VPN-Implementierungen Triple-DES im Outer-CBC-Modus eingesetzt wird.

Da ein Verschlüsselungs-Vorgang mit Triple-DES exakt dreimal so lange dauert wie mit DES, kann in einem VPN mit Triple-DES nur eine Bandbreite von maximal einigen 100 KBit/s erzielt werden.

Der Vollständigkeit wegen sei auch der sogenannte Alternierende DES erwähnt. Er arbeitet so, dass er die gleichen Operationen wie der Single-DES durchführt, jedoch alternierend unterschiedliche Schlüsselsätze verwendet. Da sich somit der Schlüsselraum verdoppelt, erhöht sich die Sicherheit. Der Vorteil liegt darin, dass die Geschwindigkeit höher ist als bei einem längeren Schlüssel, der für vergleichbare Sicherheit notwendig wäre. (siehe auch www.isrc.qut.edu.au/paper.htm und eine Analyse in /Cart95/).

4.2.2.3 International Data Encryption Algorithm (IDEA)

Da das Sicherheitsbedürfnis der Europäer noch nie geringer war als das der Amerikaner, wurden auch an den europäischen Universitäten zahlreiche Projekte zur Entwicklung von kryptographischen Algorithmen durchgeführt. Eine der Triebfedern dabei waren die bis Anfang des Jahres 2000 bestehenden Exportrestriktionen für US-amerikanische Produkte, mit denen dann keine ausreichende Sicherheit mehr gewährleistet werden konnte. So hatte die Exportversion von DES nur eine Schlüssellänge von 40 Bit, die restlichen 16 Bit waren konstant und bei amerikanischen Stellen hinterlegt.

Eine dieser europäischen Entwicklungen ist der an der ETH Zürich Anfang der neunziger Jahre vorgestellte Algorithmus IDEA. Er ist allerdings patentiert, so dass bei kommerzieller Nutzung eine Lizenzgebühr an den Inhaber der Rechte (die Firma Ascom) gezahlt werden muss.

Für IDEA existieren bisher nur Software-Implementierungen, die aber immerhin doppelt so schnell sind wie Software-Versionen von DES.

Beschreibung des Verfahrens

IDEA ist ein Blockverschlüsselungs-Verfahren mit einer Blocklänge von 64 Bit und einer Schlüssellänge von 128 Bit. Zur Verschlüsselung werden Additionen, Multiplikationen und XOR-Verknüpfungen eingesetzt. Zunächst wird ein Datenblock in vier Teile zu je 16 Bit aufgespalten, die in insgesamt 8 Runden miteinander und mit sechs Teilschlüsseln der Länge 16 Bit verknüpft werden (Abb. 4.22). Um den Wertebereich dieser Teilblöcke nicht zu verlassen, werden Addition und Multiplikation modulo durchgeführt. Die Teilschlüssel werden aus dem Schlüssel durch Aufteilung und Shift-Operationen erzeugt. Die Entschlüsselung geschieht nach dem selben Verfahren, einzig die Teilschlüssel werden geringfügig anders berechnet.

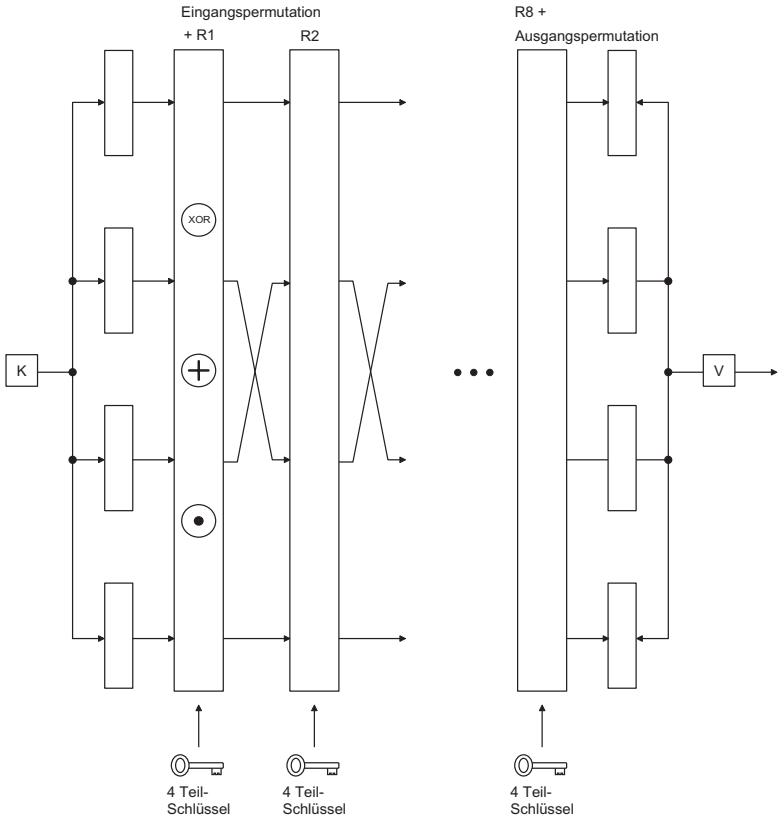


Abb. 4.22: IDEA

Betriebsarten

IDEA kann in allen Betriebsarten betrieben werden, in denen auch DES zu Hause ist: ECB, CBC, CFB und OFB. Theoretisch wäre sogar ein Triple-IDEA denkbar, das dann wegen der hohen effektiven Schlüssellänge auch von zukünftigen Hacker-Generationen mittels Brute-Force nicht anzugehen wäre. Für heutige Implementierungen ist die normale Schlüssellänge von 128 Bit allerdings ausreichend.

Bewertung der Sicherheit

Wegen der großen Schlüssellänge kann IDEA aus heutiger Sicht gegen Brute-Force-Angriffe als hoch angesehen werden. Es existieren einige schwache Schlüssel, bei denen ein »besserer« Angriff als Brute-Force möglich ist. Die Chance, einen solchen Schlüssel über einen Zufallsgenerator zu treffen, ist zum Glück verschwindend gering. IDEA ist allerdings noch nicht so gut erforscht wie DES. Es besteht also immer noch die theoretische Möglichkeit, dass eine Schwäche des

Algorithmus entdeckt wird, die Angriffe erlaubt, die um Größenordnungen effektiver sind als ein stupider Brute-Force-Angriff.

4.2.2.4 Blowfish

Das Blowfisch-Verfahren wurde 1993 vom Kryptographie-Experten Bruce Schneier entwickelt. Es handelt sich ebenfalls um eine Blockverschlüsselung mit 64 Bit-Blöcken, die Schlüssellänge ist variabel und kann bis zu 448 Bit reichen. Da Blowfish zudem frei verfügbar ist und auch von seiner Geschwindigkeit Vorteile bietet (die Software-Version ist schneller als die DES-Software-Version), hat es schnell eine beachtliche Marktpräsenz gewinnen können.

Beschreibung des Verfahrens

Die innerhalb von Blowfish verwendeten mathematischen Operationen sind auf Einfachheit hin ausgewählt; es werden Additionen, Index-Operationen und XOR-Verknüpfungen eingesetzt. Der Algorithmus besteht aus 16 Runden, in denen der in zwei Teilblöcke von je 32 Bit zerlegte 64-Bit-Block einer Permutation und einer Substitution unterworfen wird. Diese Funktionen sind von insgesamt 18 Teilschlüsseln abhängig, die aus dem vorgegebenen Schlüssel durch eine Expansionsfunktion berechnet werden (Abb. 4.23). Eine Software-Implementierung von Blowfish auf einem 32-Bit-Prozessor ist schneller als DES. Leider braucht das Verfahren recht viel Cache-Speicherplatz, so dass eine Implementierung auf Chipkarten etc. nicht möglich ist.

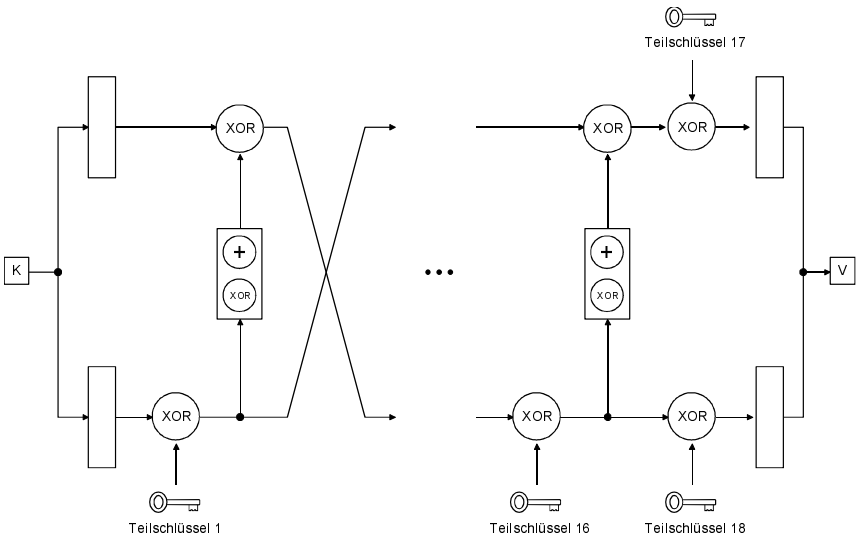


Abb. 4.23: Blowfish

Bewertung der Sicherheit

Abgesehen von eingigen schwachen Schlüsseln ist bisher kein Makel am Blowfish-Algorithmus bekannt. Wird die maximal mögliche Schlüssellänge von 448 Bit gewählt, ist ein Brute-Force-Angriff auch in der mittelfristigen Zukunft aussichtslos. Der aus Blowfish abgeleitete Algorithmus Twofish unterlag im Wettstreit im den neuen AES-Standard allerdings klar seinem Konkurrenten Rijandael.

4.2.2.5 RC4 und RC5

RC4 ist eine synchrone Stromchiffrierung mit einer variablen Schlüssellänge von bis zu 128 Bit, bei der der Klartext Byte für Byte mit einer Pseudo-Zufallszahl über ein XOR verknüpft ist. Der Algorithmus wurde schon 1987 von Ron Rivest entwickelt und lange Jahre geheim gehalten. Nachdem der Quellcode jedoch im Internet veröffentlicht wurde, konnten sich Kryptologen endlich ein Bild von der Qualität des Verfahrens machen. RC4 ist geschützt, die Rechte liegen bei der US-amerikanischen Firma RSA-Security. RC5 ist eine Weiterentwicklung des RC4-Verfahrens, die hier jedoch nicht näher behandelt wird.

Beschreibung des Verfahrens

Der Schlüsselstrom für RC4 wird aus einem Feld mit 8 * 8 = 64 Bytes erstellt, das zunächst mit einer Untermenge der Zahlen von 0 bis 255 gefüllt wird. Auswahl und Reihenfolge der Zahlen hängen vom Schlüssel ab. Aus diesem Feld wird dann der Schlüsselstrom über einige Additionen und eine Tauschoperation erzeugt (Abb. 4.24). Durch diese recht einfache Berechnung ist der Algorithmus sehr schnell, etwa fünf bis zehn mal so schnell wie DES.

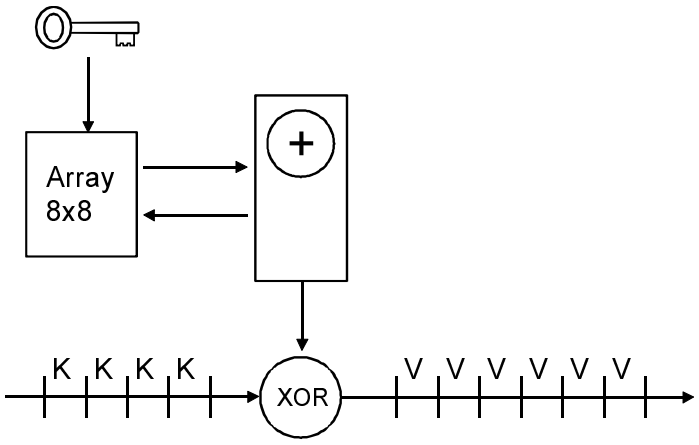


Abb. 4.24: RC4

Bewertung der Sicherheit

RC4 kommt in zahlreichen kommerziellen Produkten zum Einsatz. Deshalb ist es schon fast katastrophal, dass der Algorithmus sich als sehr schwach erwiesen hat (siehe /Fluh01/ und /Stubb01/). Es existieren viele Schlüssel, bei denen man dem verschlüsselten Text schon mit einer gewissen Wahrscheinlichkeit ansehen kann, wie der geheime Schlüssel aussehen könnte. Bei genügend vielen abgehörten Netzwerkpaketen ist das Knacken der RC4-Kommunikation dann möglich. RC4 sollte unter keinen Umständen mehr eingesetzt werden.

4.2.2.6 Advanced Encryption Standard (AES)

Die Entwickler von VPNs müssen oft Kompromisse zwischen Schnelligkeit und Sicherheit eingehen. Das schnellste der klassischen Systeme, Hardware-DES, hat wegen seiner geringen Schlüssellänge nach heutigen Maßstäben nur eine relativ geringe Sicherheit. Der Einsatz größerer Schlüssellängen führt zu Einbußen bei der Geschwindigkeit.

Das US-amerikanische NIST (National Institute of Standards and Technology) begann deshalb 1997 mit der Suche nach einem Nachfolger für DES, der »AES« (Advanced Encryption Standard) genannt wurde. In einer Ausschreibung wurden bis August 1998 fünfzehn Algorithmen präsentiert, die Kryptologen und anderen Interessenten zur Untersuchung übergeben wurden.

Die Verfahren wurden nach den Kriterien Sicherheit, Kosten (Speicher, Prozessorlast) sowie der Charakteristik von Algorithmen und möglichen Implementierungen untersucht. Am 2. Oktober 2000 wurde der von den belgischen Kryptologen Joan Daemen und Vincent Rijmen (Universität Leuven) entwickelte Algorithmus Rijndael zum Sieger erklärt. Rijndael ist frei von Patenten, so dass seiner raschen Verbreitung nichts im Wege steht. Der Algorithmus kann einfach auf verschiedenen Prozessor-Typen (8-Bit oder 32-Bit) implementiert werden. Da interne Tabellen direkt in der Hardware verdrahtet werden können und zudem bestimmte Operationen parallel ausgeführt werden können, ist die Entwicklung schneller Hard- und Software-Varianten nur eine Frage der Zeit.

Rijndael ist, ähnlich wie DES, ein Blockverschlüsselungs-Verfahren, welches aus mehreren Runden besteht. Die Länge der zu verschlüsselnden Blöcke kann 128, 192 oder 256 Bit betragen, ebenso wie die Länge des Schlüssels. Wird eine Schlüssellänge von 256 Bit gewählt, ist eine erfolgreiche Brute-Force-Attacke wegen der immerhin 2^{256} Möglichkeiten auf Jahrzehnte hinaus praktisch ausgeschlossen. Die Anzahl der Runden hängt von der Blocklänge und der Schlüssellänge ab und beträgt 10, 12 oder 14 (Tab. 4.1).

AES-Runden	Nb = 4	Nb = 6	Nb = 8
Ns = 4	10	12	14
Ns = 6	12	12	14
Ns = 8	14	14	14

Tabelle 4.1: Anzahl der AES-Runden in Anhängigkeit von der Blocklänge Nb und der Schlüssellänge Ns (in Bytes)

Jede der Runden von Rijndael besteht aus einer Reihe von Byte-orientierten Transformationen, in denen die Autoren die Stärken vieler anderer Verschlüsselungs-Algorithmen kombiniert haben. Die eingesetzten Operationen haben sich bei anderen Verschlüsselungs-Verfahren in der Vergangenheit als widerstandfähig gegenüber Angriffen erwiesen.

Die in einem zweidimensionalen Array abgelegten Zeichen des Klartext-Blocks werden zunächst der sogenannten ByteSub-Transformation unterworfen. Es handelt sich um eine nichtlineare Substitution der einzelnen Bytes, die über eine Tabelle (S-Box) festgelegt wird. Abbildung 4.25 zeigt die Transformation für den Fall einer Blocklänge von 192 Bit, bei denen der Block in einem Array von 6x4 Bytes abgelegt ist.

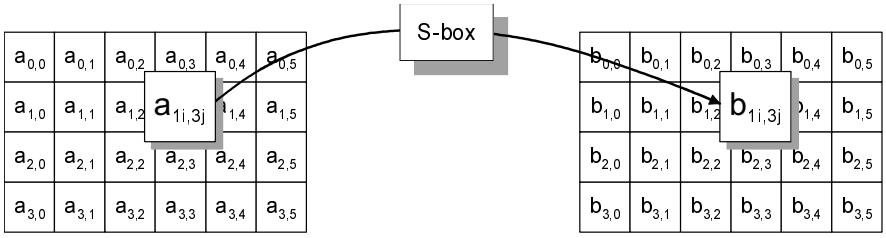


Abb. 4.25: ByteSub-Transformation

Die Bytes werden anschließend der ShiftRow-Transformation unterworfen, bei der die Zeilen des Arrays bis auf die erste zyklisch geshiftet werden, jede Zeile um eine andere Anzahl von Bytes. Abb. 4.26 zeigt wieder den Fall der Blocklänge von 192 Bit.

Die MixColumn-Transformation unterwirft jede Spalte des Arrays einer Multiplikation mit einem festen Polynom (Abb. 4.27).

In der abschließenden AddRoundKey-Transformation wird der aus dem geheimen Schlüssel ermittelte Rundenschlüssel mit dem Array durch ein bitweises XOR verknüpft (Abb. 4.28).

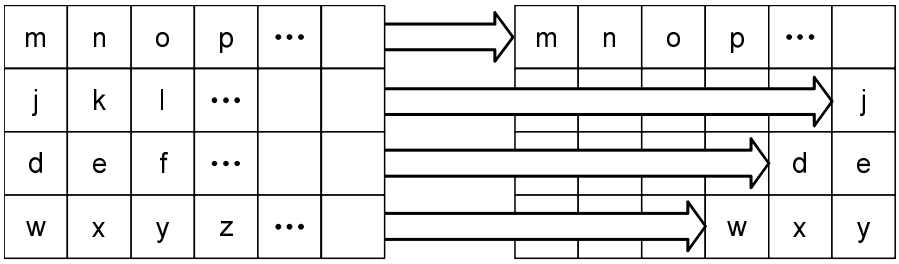


Abb. 4.26: ShiftRow-Transformation

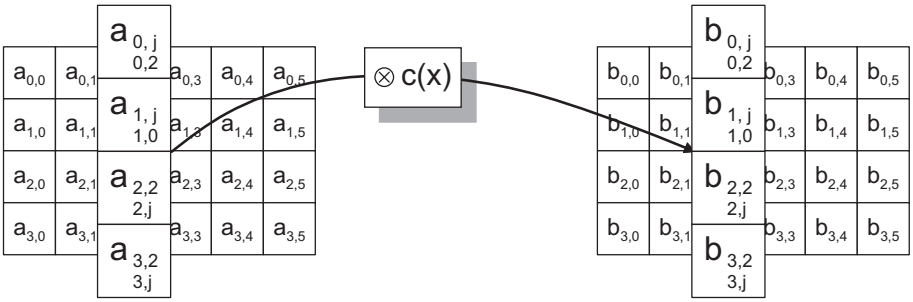


Abb. 4.27: MixColumn-Transformation

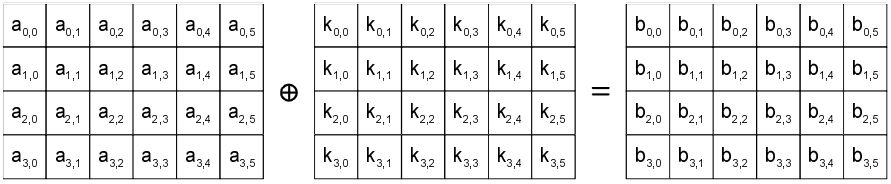


Abb. 4.28: AddRoundKey-Transformation

In der letzten Runde von Rijndael wird die MixColumn-Transformation überschlagen und direkt in die AddRoundKey-Transformation verzweigt.

Die in den einzelnen Runden benutzten Rundenschlüssel werden aus dem originalen Schlüssel durch eine Expansions-Funktion berechnet. Über XOR, zyklische Shifts und einen Tabellen-Lookup werden vor Beginn der Ver- beziehungsweise Entschlüsselung alle Rundenschlüssel berechnet. Dabei wird ein Puffer der Länge (Blocklänge in Bit) * (Anzahl der Runden +1) gefüllt, aus dem die jeweiligen Rundenschlüssel dann entnommen werden. Die ersten Ns Bits (Ns = Schlüssellänge) des Puffers entsprechen dem Schlüssel in unverfälschter Form, alle anderen jeweils Ns Bits entstehen aus den vorherigen Ns Bits durch eine zyklische Permutation und eine Transformation, die der oben angegebenen ByteSub-Transformation ähnelt.

Vor dem Beginn der ersten Runde wird eine initiale AddRoundKey-Transformation durchgeführt, die den Klartext mit dem ersten Rundenschlüssel verknüpft.

Die Entschlüsselung erfolgt analog zur Verschlüsselung, für jede der Transformationen können inverse Transformationen angegeben werden. Jede Runde wird nach folgendem Schema invertiert:

- AddRoundKey,
- InvMixColumn,
- InvShiftRow,
- InvByteSub

Analog zur Verschlüsselung entfällt in der letzten Runde die InvMixColumn-Transformation.

Bewertung der Sicherheit

AES ist der Standard für symmetrische Verschlüsselung in den nächsten Jahren. Seine Schlüssellänge von maximal 256 Bit macht ihn für die nächste Zeit gegen Brute-Force-Attacken unempfindlich. Da der Algorithmus bei dem AES-Auswahlverfahren weltweit gründlich analysiert wurde, ist ein besserer Angriff als Brute-Force nicht zu erwarten. Bei Neuanschaffungen von VPNs sollte die Verfügbarkeit von AES ein Kriterium zum Kauf sein.

4.2.3 Asymmetrische Verschlüsselungs-Verfahren

Asymmetrische Verschlüsselungs-Verfahren sind etwa um den Faktor 1000 bis 10 000 langsamer als symmetrische Verfahren, weshalb sie innerhalb von VPNs nur zur Authentikation und zum Austausch des Schlüssels für die symmetrische Datenverschlüsselung benutzt werden.

4.2.3.1 Diffie-Hellman

Diffie-Hellman war der erste Algorithmus, der auf einer Kombination von öffentlichen und privaten Schlüsseln beruht. Er wurde 1976 von Whitfield Diffie und Martin Hellman entwickelt und beruht auf der Tatsache, dass eine Potenzierung von großen Zahlen wesentlich einfacher ist als die Umkehrfunktion, der Logarithmus. Diffie-Hellman wurde ursprünglich dazu entwickelt, einen Schlüsselaustausch zwischen zwei oder mehr Parteien vorzunehmen, ohne dass dieser Schlüssel von Unbefugten aus der (abgehörten) Kommunikation zwischen den Partnern ermittelt werden kann.

Beschreibung des Verfahrens

Zunächst soll der einfache Fall eines Schlüsselaustauschs zwischen zwei Personen dargestellt werden. Beide einigen sich auf eine große Primzahl n und eine natürliche Zahl g. Diese können über ein unsicheres Netz ausgetauscht werden, ohne

dass eine Gefahr besteht. Jetzt wählen beide Partner je eine geheime Zahl, die hier als x und y bezeichnet werden.

Der Besitzer von x bildet

$X=g^x \bmod n$

und sendet X über die Leitung zu seinem Partner. Der Besitzer von y bildet

$Y=g^y \bmod n$

und sendet Y ebenfalls an den Partner. Ein potentieller Angreifer, der die gesamte Kommunikation abgehört hat, kann aus n, g, X und Y wegen der nicht trivialen Umkehrfunktion zu g^x und g^y die geheimen Zahlen x und y nicht berechnen.

Nach Empfang von X und Y berechnet der eine Partner

$k=Y^x \bmod n$,

der andere

$k'=X^y \bmod n$,

die beide gleich sind:

$k = k' = g^{xy} \bmod n$.

Also ist k bzw. k´ der gesuchte geheime Schlüssel. Analog lässt sich das Verfahren mit mehr als zwei Teilnehmern durchführen, der gesuchte Schlüssel ist beispielsweise bei vier Personen w,x,y und z

$k = g^{wxyz} \bmod n$.

Mit dieser Methode lässt sich aber auch ein übliches Schlüsselpaar aus privatem und öffentlichem Schlüssel generieren. Dabei muss die Primzahl n und die natürliche Zahl g allen potentiellen Teilnehmern bekannt sein. Jeder Benutzer wählt per Zufallsgenerator einen geheimen Schlüssel x. Der dazugehörige öffentlichen Schlüssel wird dann durch

$X = g^x \bmod n$

gebildet. Alle öffentlichen Schlüssel X´ können beispielweise über das Internet ausgetauscht bzw. von einem LDAP-Server bei Bedarf geladen werden. Will ein Teilnehmer einem anderen eine verschlüsselte Nachricht senden, ermittelt er aus seinem geheimen Schlüssel und dem öffentlichen Schlüssel des Gegenübers den zur (symmetrischen) Verschlüsselung benutzten Schlüssel k. Der Empfänger kann k ebenfalls aus seinem geheimen Schlüssel und dem öffentlichen Schlüssel des Senders generieren.

Die bei Diffie-Hellman benutzten mathematischen Operationen sind den üblichen Mikroprozessoren nicht gerade auf den Leib geschrieben, was die nicht sehr große Geschwindigkeit des Verfahrens erklärt.

Bewertung der Sicherheit

Die Sicherheit von Diffie-Hellman hängt primär von der Wahl der Primzahl n und der natürlichen Zahl g ab. Für n (und auch für die geheimen Schlüssel x) gilt »Je größer, desto besser«, denn ein Brute-Force-Angriff muss ja aus

$X=g^x \bmod n$

den Wert von x ermitteln. Die Zahl n sollte mindestens 1024 oder 2048 Bit lang sein, um eine gute Sicherheit zu gewährleisten.

Die Zahl g unterliegt nur der Einschränkung, dass sie primitiv modulo n ist. Ihre Größe trägt nichts zur Sicherheit des Verfahrens bei, so dass bei praktischen Implementierungen oft kleine g im einstelligen Bereich benutzt werden.

4.2.3.2 RSA

Der RSA-Algorithmus wurde nach seinen Entdeckern Ron Rivest, Adi Shamir und Leonhard Adleman benannt. Sie stellten ihn 1978 der Öffentlichkeit vor. RSA kann als das erste Verfahren beeichnet werden, das für Verschlüsselung und digitale Signatur innerhalb einer Public Key Infrastructure (PKI) entworfen wurde, wenngleich dieses Wort damals noch niemand in den Mund nahm. Diffie-Hellman ist zwar älter als RSA, doch wurde das Verfahren zunächst zum Schlüsselaustausch entworfen. Die oben beschriebene Möglichkeit zum Einsatz in einer PKI wurde erst später entwickelt.

Beschreibung des Verfahrens

RSA beruht ähnlich wie Diffie-Hellman auf mathematischen Operationen, deren Umkehrung extrem aufwendig ist. Hier ist es das Produkt zweier großer Primzahlen, das sich schnell bilden lässt. Die Faktorisierung eines solchen Produktes ist hingegen sehr aufwendig.

Um den öffentlichen und den privaten Schlüssel zu berechnen, werden zwei große Primzahlen p und q zufällig ausgewählt und das Produkt pq gebildet. Anschließend können p und q gelöscht werden. Der öffentliche Schlüssel besteht zum einen aus diesem Produkt n=pq, zum anderen aus dem Chiffrierschlüssel e, der wieder mittels Zufallsgenerator bestimmt wird. Es muss ein e gefunden werden, das zu dem Produkt (p-1)(q-1) prim ist, das heißt, es gibt keine gemeinsamen Teiler. Der private Schlüssel d berechnet sich dann zu

$d = e^{-1} \bmod ((p-1)(q-1))$.

Zur Verschlüsselung wird der Klartext in kleine Blöcke b zerlegt und diese werden alle nacheinander mit dem öffentlichen Schlüssel (n und e) auf die verschlüsselten Blöcke v mittels

$v = b^e \bmod n$

abgebildet. Die Entschlüsselung geschieht mit dem privaten Schlüssel d durch

$b = v^d \bmod n.$

Außer einer Verschlüsselung kann mit RSA auch eine digitale Signatur durchgeführt werden, Dazu wird zunächst einmal ein Hashwert über das zu unterzeichnende Dokument gebildet. Dieser Hashwert h wird dann mit dem privaten Schlüssel d verschlüsselt:

$v = h^d \bmod n.$

Der Empfänger bildet den Hashwert aus dem Original-Dokument und vergleicht ihn mit dem durch den öffentlichen Schlüssel (e und n) entschlüsselten Hashwert:

$h = v^e \bmod n.$

Stimmen beide überein, muss das Dokument vom Besitzer des privaten Schlüssels signiert worden sein, der in aller Regel der Absender der Datei sein sollte.

Bewertung der Sicherheit

Das Problem für einen Angreifer ist die Gewinnung des privaten Schlüssels d aus dem ihm bekannten öffentlichen Schlüssel e beziehungsweise n. Kennt er die beiden Primzahlen p und q, ist der Schlüssel geknackt. Das Knacken von RSA reduziert sich somit auf die Primzahlfaktorierung großer Zahlen. Wegen der Größe der bei RSA verwendeten Zahlen (1024 Bit, besser aber 2048 oder 4096 Bit), ist ein Brute-Force-Angriff durch Ausprobieren aller Möglichkeiten

$n = pq$

praktisch ohne Aussicht.

Es existiert jedoch ein Angriff schneller als Brute-Force. Ein schwedisches Forscherteam konnte mit Hilfe des Verfahrens »General Number Field Sieve« eine extrem schnelle Faktorierung von n durchführen und so 512 Bit RSA-Schlüssel knacken. RSA mit 512 Bit darf deshalb keinesfalls mehr zur Anwendung kommen.

Schlüsselqualität:

Die Sicherheit des RSA-Verfahrens beruht auf der Schwierigkeit, eine große Zahl in ihre Primfaktoren zu zerlegen. In der Literatur findet man mehrere Ansätze, dieses Problem zu lösen.

Beispielsweise gibt es Methoden, die auf der Kenntnis der (teilweisen) Faktorisierung von p-1 oder p+1 (gleiches gilt für q-1 und q+1) beruhen. Zahlen, die neben ihrer Primzahleigenschaft noch mehrere die Sicherheit erhöhende Merkmale wie große Primteiler in p-1 und p+1 haben und die somit diese Methoden erschweren, werden daher als »starke« Primzahlen bezeichnet.

up ...

... up ... update

Nutzen Sie den UPDATE-SERVICE des mitp-Teams bei vmi-Buch.

Registrieren Sie sich JETZT!

Unsere Bücher sind mit großer Sorgfalt erstellt. Wir sind stets darauf bedacht, Sie mit den aktuellsten Inhalten zu versorgen, weil wir wissen, dass Sie gerade darauf großen Wert legen. Unsere Bücher geben den top-aktuellen Wissens- und Praxisstand wieder.

Um Sie auch über das vorliegende Buch hinaus regelmäßig über die relevanten Entwicklungen am IT-Markt zu informieren, haben wir einen besonderen Leser-Service eingeführt.

Lassen Sie sich professionell, zuverlässig und fundiert auf den neuesten Stand bringen.
Registrieren Sie sich jetzt auf www.mitp.de oder **www.vmi-buch.de** und Sie erhalten zukünftig einen E-Mail-Newsletter mit Hinweisen auf Aktivitäten des Verlages wie zum Beispiel unsere aktuellen, kostenlosen Downloads.

Ihr Team von mitp

An die zu suchende Zahl p (bzw. q) werden folgende Forderungen gestellt /Gord84/:

- p ist eine große Zahl
- p ist eine Primzahl
- p wurde zufällig ausgewählt
- p hat eine vorher festgelegte Länge
- p-1 hat einen großen Primteiler r
- p+1 hat einen großen Primteiler s
- r-1 hat einen großen Primteiler
- s-1 hat einen großen Primteiler.

4.2.3.3 ElGamal und DSA

Der von Taher ElGamal 1993 entwickelte und nach ihm benannte Algorithmus ist eine Variante von Diffie-Hellman. Er beruht auf dem gleichen Prinzip, dass Potenzen leicht, die Umkehrfunktion Logarithmus dagegen schwer zu berechnen ist. Im Unterschied zu Diffie-Hellman wurde ElGamal direkt für den Einsatz in PKIs entwickelt. Das klassische ElGamal dient der digitalen Signatur, es gibt allerdings auch eine modifizierte Variante, mit der Verschlüsselung möglich ist. In Europa wird ElGamal nur selten eingesetzt, aber in den USA hat es durch seine Implementierung im staatlichen Signaturverfahren DSA (Digital Signatur Algorithm) eine große Verbreitung.

Beschreibung des Verfahrens

Jeder Benutzer bestimmt zunächst einen privaten und einen öffentlichen Schlüssel. Dazu werden per Zufallsgenerator eine große Primzahl p und zwei Zahlen g und x bestimmt, wobei gelten muss

$g < p$ und $x < p$.

Der private Schlüssel ist x.

Mit

$y = g^x \bmod p$

wird der öffentliche Schlüssel bestimmt, der aus dem Zahlentripel g, p und y besteht. Um ein Dokument (oder vielmehr dessen Hash) h zu signieren, wird zunächst eine weitere Zufallszahl k bestimmt, die keinen gemeinsamen Teiler mit (p-1) hat.

Der erste Teil der Signatur besteht aus der Zahl a mit

$a = g^k \bmod p$,

zur Berechnung des zweiten Teils b muss folgende Gleichung nach b ausgelöst werden:

$h = (xa + kb) \bmod (p-1)$.

Gilt dann

$y^a a^b \bmod p = g^h \bmod p$,

so ist die Unterschrift authentisch.

Bewertung der Sicherheit

Ein Brute-Force-Angriff auf ElGamal muss aus der Gleichung

$y = g^x \bmod p$

den geheimen Schlüssel x bestimmen. Werden große Zahlen benutzt (1024 oder 2048 Bit), sind diese Angriffe praktisch aussichtslos. Hier ähnelt ElGamal seinem Vorbild Diffie-Hellman stark. Es existiert aber noch ein anderer möglicher Angriff gegen das Verfahren, der weit weniger aufwändig ist. Wird die Zufallszahl k von einem schlechten Zufallsgenerator bestimmt, könnte es dem Angreifer gelingen, zwei Nachrichten-Hashwerte h und h´ mitzuschneiden, von denen er weiß, dass sie mit demselben k signiert wurden. Nachrichten mit demselben k sind daran zu erkennen, dass sie dieselbe Teilunterschrift

$a = g^k \bmod p$

tragen. Vom Gleichungssystem

$h = (xa + kb) \bmod (p-1)$

$h' = (xa + kb') \bmod (p-1)$

sind alle Größen außer x und k bekannt. Der gesuchte private Schlüssel x lässt sich daraus ohne großen Aufwand berechnen. Da eine Wiederholung von k bei den heutigen Zufallsgeneratoren durchaus im Bereich des Möglichen liegt, ist es rätselhaft, weshalb dieser Algorithmus im staatlichen Bereich in den USA vorgeschrieben ist. Vielleicht wollten sich die Geheimdienste eine zumindest theoretische Hintertür offen halten.

4.2.4 Hash-Verfahren

Ein Hashwert dient innerhalb einer VPN-Infrastruktur als Vorbereitung der digitalen Signatur einer Menge von Daten. Er komprimiert die gegebene Datenmenge auf eine feste, kleine Länge und kann als eine Art Prüfsumme bezeichnet werden. Dabei gelten aber besondere Anforderungen an den Hash-Algorithmus:

- Die Hash-Funktion ist eine Einbahnstraße, das heißt, es ist leicht, aus einer gegebenen Datenstruktur deren Hashwert zu berechnen. Umgekehrt ist es praktisch unmöglich, aus einem gegebenen Hashwert eine Datenstruktur zu berechnen, die eben diesen Hashwert hat.
- Es ist extrem schwierig, zu einer gegebenen Datenmenge eine andere Datenmenge zu berechnen, die denselben Hashwert besitzt.
- Eine kleine Änderung in der Datenmenge hat große Auswirkungen auf den Hash.

Mit diesen Anforderungen sollen Manipulationen an den Originaldaten beziehungsweise am Hashwert sofort sichtbar gemacht werden, so dass der Hashwert zur Konsistenzüberprüfung der Daten dienen kann. Wird der Hashwert zusätzlich noch signiert, kann der Absender der Daten nachvollziehbar überprüft werden. Alternativ kann der Hashwert mit einem geheimen Schlüssel manipuliert und dem Empfänger zugestellt werden. Besitzt dieser den Schlüssel ebenfalls, kann er den Hashwert kontrollieren. Diese Kombination aus Hashwert und geheimem Schlüssel wird auch als Message Authentication Code (MAC) bezeichnet.

4.2.4.1 Message Digest 4 (MD4)

Ron Rivest entwickelte Anfang der neunziger Jahre das MD4-Verfahren. Heute gilt es nicht mehr als besonders sicher, doch da Microsoft es in seiner Windows-Umgebung zur Authentikation, zum Verschlüsseln der Passworte in der SAM-Datenbank und in den Microsoft-eigenen VPNs benutzt, darf es an dieser Stelle nicht fehlen. MD4 erzeugt aus Dokumenten beliebiger Länge einen Hashwert von 128 Bit.

Beschreibung des Verfahrens

MD4 ist ein Algorithmus, der im Wesentlichen aus nichtlinearen Funktionen besteht. Diese enthalten logische Verknüpfungen der booleschen Funktionen AND, OR, NOT und XOR. MD4 zerlegt den Text in Blöcke zu 512 Bit, der letzte Block wird gegebenenfalls aufgefüllt. Vier Variablen A,B,C und D (je 32 Bit) werden mit festen Werten initialisiert und in drei Runden über nichtlineare Funktionen mit den Textblöcken verknüpft. A,B,C und D ergeben sich in den Runden 2 und 3 aus den Ergebnissen der vorhergehenden Runde. Abschließend werden die Ergebnisse der Runde 3 zu einem 128-Bit-Hashwert zusammengestellt.

Der Algorithmus im Detail:

Der Text wird zunächst auf eine Länge von n * 512 – 64 gebracht, wobei das Auffüllen (Padding) mit einer 1 und nachfolgenden 0 vorgenommen wird. Die letzten 64 Bit enthalten dann die Länge des Textes beziehungsweise nur die niederwertigen 64 Bit, falls er länger als 2^{64} ist.

Die vier Zahlen A,B,C und D werden mit Konstanten initialisiert:

A = 01 23 45 67

B = 89 ab cd ef

C = fe dc ba 98

D = 76 54 32 10

In jeder der drei Runden werden die Werte der aktuellen A,B,C und D temporären Variablen AA, BB, CC und DD zugewiesen. Anschließend werden diese Größen über eine der drei Funktionen jeweils 16-mal mit dem Text verknüpft und geshiftet:

Runde 1: F(x,y,z) = (x AND y) OR (NOT(x) AND z)

Runde 2: G(x,y,z) = (x AND y) OR (x AND z) OR (y AND z)

Runde 3: H(x,y,z) = x XOR y XOR z

Dabei ändern sich die AA, BB, CC und DD. Nach der letzten Runde werden diese Werte zu den alten Konstanten A, B, C, D addiert. Die Nebeneinanderstellung der neuen Werte von A, B, C und D ergibt dann den 128-Bit-Hashwert (Abb. 4.29).

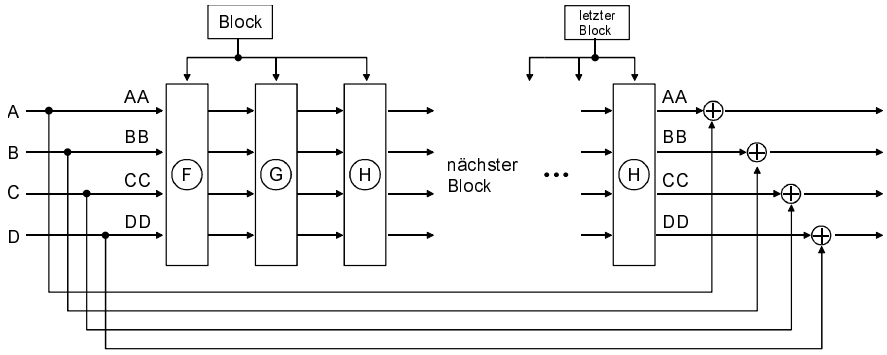


Abb. 4.29: Hashwert-Bildung mittels MD4

Bewertung der Sicherheit

Obwohl MD4 bis heute nicht gebrochen werden konnte, sind Angriffe gegen die ersten beiden Runden möglich. Die Sicherheit des Verfahrens hängt deshalb »am seidenen Faden«, an der dritten Runde.

MD4 sollte aus diesem Grund in neu konzipierten Systemen nicht mehr eingesetzt werden.

4.2.4.2 Message Digest 5 (MD5)

MD5 ist ein verbesserter Nachfolger von MD4 und wurde Anfang der neunziger Jahre ebenfalls von Ron Rivest entwickelt. Er liefert ebenfalls 128-Bit-Hashwerte und ähnelt MD4 von seinem Aufbau sehr, es wurde aber eine vierte Runde hinzugefügt. Außerdem ändern sich A, B, C, und D schon in jeder Runde.

Beschreibung des Verfahrens

Das Padding der zu hashenden Datenstruktur geschieht identisch zu MD4, also durch Auffüllen auf ein Vielfaches von 512 Bit mit einer Eins und Nullen sowie Berechnung der 64 Bit-Längenangabe.

Die Variablen A, B, C und D werden identisch zu MD4 initialisiert, die Funktionen der einzelnen Runden werden um eine vierte erweitert. Dabei wurde G modifiziert, um weniger symmetrisch als bei MD4 zu sein.

Runde 1: F(x,y,z) = (x AND y) OR (NOT(x) AND z)

Runde 2: G(x,y,z) = (x AND y) OR (y AND NOT(z))

Runde 3: H(x,y,z) = x XOR y XOR z

Runde 4: I(x,y,z) = y XOR (x OR (NOT(z))

Die entscheidende Verbesserung liegt aber in der Behandlung der A,B,C und D. Sie werden nach jeder Runde um die AA, BB, CC und DD vergrößert und anschließend den AA, BB, CC und DD für die nächste Runde zugewiesen. Der Hash ergibt sich schließlich durch die A, B, C und D der letzten Runde (Abb. 4.30).

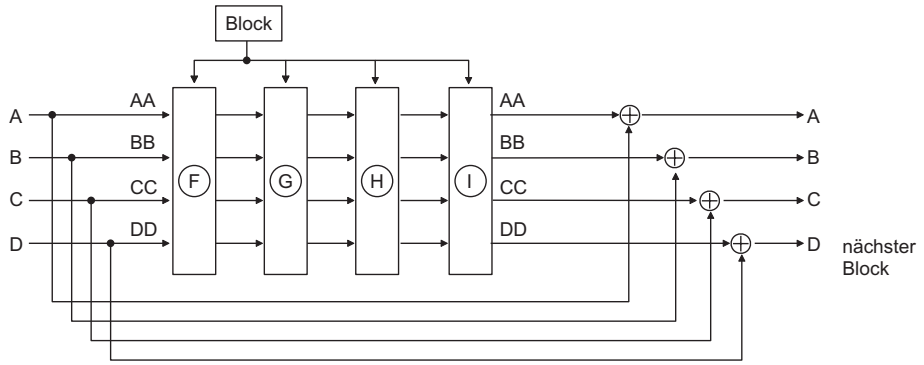


Abb. 4.30: Hashwert-Bildung mittels MD5

Bewertung der Sicherheit

MD5 ist in jedem Fall sicherer als MD4, wenngleich Kryptologen auch bei MD5 Angriffe gegen einige Runden durchführen können. Die bisher veröffentlichten Angriffe beeinträchtigen die Sicherheit von MD5 bisher nicht, doch raten einige Wissenschaftler von der Verwendung von MD5 ab.

4.2.4.3 Secure Hash Algorithm (SHA)

Unter dem Namen SHA sind verschiedene Verfahren zur Hashbildung bekannt, die ab Anfang der neunziger Jahre von den beiden US-amerikanischen Institutionen NSA und NIST entwickelt wurden. Ziel war es, eine Hashfunktion für den Signatur-Standard DSA bereitzustellen. Zusätzlich enthält DSA noch die Signatur des Hashwerts mittels ElGamal.

Der erste dieser Algorithmen, SHA-1 genannt, erzeugt einen Hashwert von 160 Bit Länge. Urmutter war auch hier der MD4-Algorithmus, wobei die Gemeinsamkeiten geringer sind als zwischen MD4 und MD5. Die Nachfolger von SHA-1 erzeugen aufgrund kleiner Modifikationen am Verfahren Hashwerte der Längen 256 Bit,

384 Bit und 512 Bit. Diese Algorithmen werden dementsprechend auch als SHA-256, SHA-384 und SHA-512 bezeichnet. Wird nur von SHA gesprochen, so ist in der Regel der alte SHA-1 gemeint.

Beschreibung des Verfahrens (SHA–1)

Das Padding der Eingangsdaten geschieht absolut identisch zu MD4 und MD5, das heißt durch Auffüllen auf ein ganzzahliges Vielfaches von 512 Bit inklusive 64 Bit Längenangabe. Wegen der Hashlänge von 160 Bit benutzt SHA–1 fünf Variablen zu je 32 Bit, die wie folgt initialisiert werden:

A = 67 45 23 01

B= ef cd ab 89

C = 98 ba dc fe

D = 10 32 54 76

E = c3 d2 e1 f0

Ein entscheidender Unterschied zwischen SHA–1 und MD4/MD5 ist eine Expansion der Nutzdaten, bei der bei jedem 512-Bit-Block nach einer Zerlegung in 16 * 32-Bit durch XOR und Shift-Operationen zusätzlich 72 weitere 32-Bit-Blöcke berechnet und in den Algorithmus eingebracht werden. Diese Funktion, die aus den 16 Wörtern insgesamt 80 Wörter macht, wird von Kryptologen als starke Verbesserung der Qualität des Verfahrens bezeichnet.

Es werden wieder 4 Runden durchlaufen, in jeder Runde aber 20 Operationen. In der ersten Runde werden dabei die ersten 20 32-Bit-Blöcke benutzt, in der zweiten Runde die Blöcke 21 bis 30 usw. In jeder Runde werden die Konstanten A, B, C, D und E wieder temporären Größen AA, BB, CC, DD und EE zugewiesen, die mit den Nutzdaten durch Shift-Operationen und nichtlineare Funktionen neue AA etc. berechnen. Diese werden dann wie bei MD5 auf die Größen A, B, C, D und E addiert. Die nichtlinearen Funktionen haben die folgende Form:

Runde 1: F(x,y,z) = (x AND y) OR (NOT(x) AND z) (identisch zu MD4 und MD5)

Runde 2: G(x,y,z) = x XOR y XOR z

Runde 3: H(x,y,z) = (x AND y) OR (x AND z) OR (y AND z)

Runde 4: I(x,y,z) = x XOR y XOR z

Die zuletzt berechneten Werte A, B, C, D und E werden analog zu MD4/MD5 zum 160 Bit-Hashwert kombiniert (Abb. 4.31).

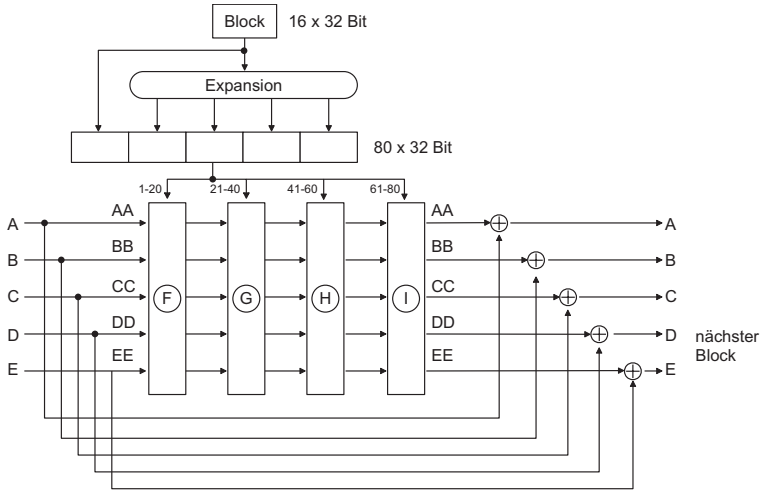


Abb. 4.31: Hashwert-Bildung mittels SHA-1

Bewertung der Sicherheit

Wegen des längeren Hashwerts sind Brute-Force-Angriffe vor allem gegen die SHA-Varianten mit 384 und 512 Bit ungleich schwieriger als gegen MD4/MD5. Angriffe gegen SHA, die bessere Möglichkeiten bieten als Brute-Force, sind bisher nicht bekannt.

Bis auf die alte 160-Bit-Variante SHA-1 wird SHA deshalb zusammen mit dem symmetrischen AES die Kryptosysteme der nächsten Jahre dominieren und auch in vielen VPN-Lösungen anzutreffen sein.

4.2.4.4 HMAC

Als Beispiel für ein Message Authentication Code-Verfahren (MAC) soll der 1997 bei IBM entwickelte Algorithmus HMAC beschrieben werden. Wie andere MAC-Verfahren kombiniert HMAC eine Hash-Funktionen mit symmetrischer Verschlüsselung. Da je nach Implementierung des VPN jedes einzelne Netzwerkpakete mittels MAC abgesichert werden muss, ist die Geschwindigkeit des Verfahrens eine wichtige Kenngröße. Eine reine Hintereinanderschaltung von Hash und Verschlüsselung wäre aus Gründen der Performance ungünstig, so dass die Entwickler von HMAC folgende Randbedingungen berücksichtigen mussten:

- Das Verfahren sollte mit möglichst vielen Hash-Funktionen zusammenarbeiten, ohne dass diese modifiziert werden mussten.
- Die Geschwindigkeit der Hash-Algorithmen sollte nur unwesentlich verlangsamt werden.
- Die Sicherheit des Hash-Verfahrens durfte durch die Manipulationen mit dem geheimen Schlüssel nicht verringert werden.

Beschreibung des Verfahrens

Ausgangspunkt von HMAC ist eine Hash-Funktion H(Text), etwa MD5 oder SHA–1. Das zu bearbeitende Dokument (Text) wird mit dem geheimen Schlüssel K und zwei internen Datenstrukturen ipad und opad nach folgender Gleichung kombiniert:

HMAC = H(K XOR opad, H(K XOR ipad, text)) mit

ipad = 0x36, 0x36, 0x36 ...

opad = 0x5C, 0x5C, 0x5C ...

Die Felder ipad und opad haben eine Länge, die der Blockgröße B des eingesetzten Hash-Algorithmus entspricht (64 Bytes bei MD5 und SHA–1). Der Schlüssel K wird durch das Anhängen von Nullen ebenfalls auf diese Länge B gebracht.

Die obige Gleichung bedeutet im Einzelnen:

- Verknüpfe den auf die Länge B gebrachten geheimen Schlüssel K mittels XOR mit der ipad-Datenstruktur.
- Stelle das Ergebnis dieser Operation vor das zu verschlüsselnde Dokument und schicke diesen so um B vergrößerten Text durch die Hash-Funktion H.
- Das Ergebnis dieser Hash-Operation hat die Länge L (16 Bytes bei MD5, 20 Bytes bei SHA–1).
- Verknüpfe den auf die Länge B gebrachten geheimen Schlüssel K mittels XOR mit der opad-Datenstruktur.
- Stelle das Ergebnis dieser Operation (Länge B) vor das Hash-Ergebnis (Länge L) und schicke diese Bytestrom der Länge L+B durch die Hashfunktion H.
- Der HMAC-Hash wird zusammen mit dem verschlüsselten Dokument an den Empfänger geschickt.

Abbildung 4.32 verdeutlicht diesen Sachverhalt.

Die Geschwindigkeit von HMAC ist bei größeren Datenstrukturen (Text) nur unwesentlich kleiner als die der verwendeten Hash-Funktion, obwohl diese zweimal aufgerufen wird. Beim ersten Hash wird der Text um das Ergebnis der XOR-Operation (Länge B) vergrößert, der zweite Hash arbeitet mit einer Länge L+B und beansprucht nur wenig Ressourcen. Soll bei einem VPN allerdings jedes Netzwerkpaket mittels HMAC abgesichert werden, entstehen relativ zu den kleinen Paketlängen große zusätzliche Aufwendungen.

Der Empfänger des (verschlüsselten) Dokuments kann den HMAC-Hash bilden, sofern er das Klartext-Dokument zurück gewinnen kann und außerdem den geheimen Schlüssel für die HMAC-Operation besitzt. Stimmt der Wert mit der mitgeschickten Größe des HMAC überein, ist das Dokument unverfälscht übertragen worden und stammt tatsächlich von einem Besitzer des geheimen HMAC-Schlüssels.

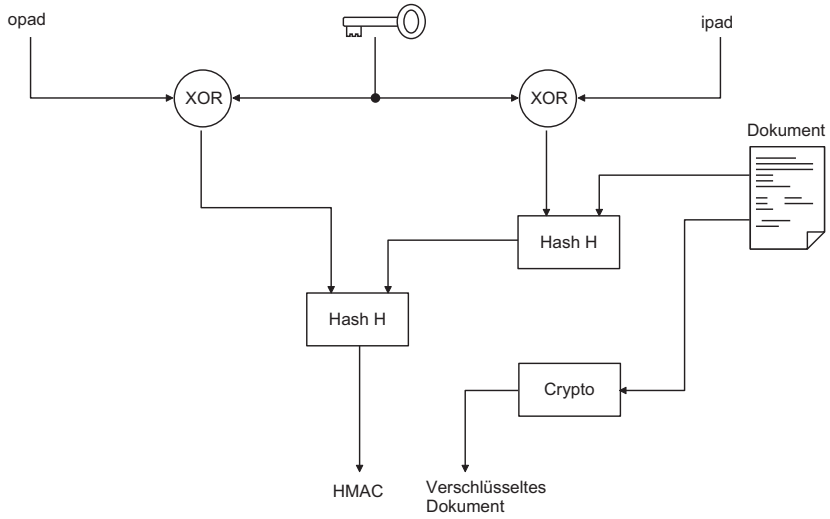


Abb. 4.32: HMAC

Bewertung der Sicherheit des Verfahrens

Der Einsatz von HMAC ist von der Sicherheit her identisch zu dem jeweils eingesetzten Hash-Verfahren.

4.3 Infrastruktur von Zertifizierungs-Systemen

Die zur Absicherung von öffentlichen Schlüsseln eingesetzten Zertifizierungs-Systeme bedürfen einer Infrastruktur, mit der in einer für den Benutzer nachvollziehbaren Weise Schlüssel und Zertifikate verwaltet und kontrolliert werden können. Eine solche Infrastruktur, die häufig als PKI (Public Key Infrastructure) bezeichnet wird, muss folgende Aufgaben erfüllen:

- Vergabe von eindeutigen elektronischen Identifikationen
- Bereitstellung und Verteilung von zertifizierten Schlüsseln
- eindeutige Zuordnung von zertifizierten Schlüsseln zu Personen oder Firmen
- Überprüfung von zertifizierten Schlüsseln
- Verwaltung von ungültigen Zertifikaten, die etwa durch Zeitablauf oder Diebstahl entstehen können

In der Praxis konnten sich eine Reihe von Verfahren etablieren, mit denen eine PKI aufgebaut werden kann. Diese unterscheiden sich vor allem im Zugriff auf die Zertifikate und in der Struktur der Vertrauensverhältnisse der beteiligten Parteien. Auf lange Sicht wird sich die im Standard X.509 festgelegte PKI durchsetzen, doch benötigt dieses Verfahren einen eigenen Verzeichnisdienst zum Zugriff auf Schlüssel und Zertifikate.

Unter den Verzeichnisdiensten, deren Aufbau und Wirkungsweise im Standard X.500 festgelegt wurden, hat sich eine etwas abgespeckte Variante mit dem Protokoll LDAP (Lightweight Directory Access Protocol) im VPN-Bereich durchgesetzt.

4.3.1 X.509-Zertifikate

Am Prozess der Ausgabe, Verwaltung und Vernichtung von Schlüsseln und Zertifikaten sind unter X.509 mehrere Parteien beteiligt.

Die Zertifizierungs-Instanz – auch Certification Authority (CA) genannt – erzeugt Zertifikate und Schlüsselpaare beziehungsweise zertifiziert bestehende (öffentliche) Schlüssel. Sie ist verantwortlich für die eindeutige Zuordnung zwischen Schlüssel, Zertifikat und dem Besitzer des Schlüssels. Der öffentliche Schlüssel ist dabei Bestandteil der Datenstruktur des Zertifikats. Die CA versieht die Zertifikate mit einer digitalen Signatur und einem Verfallsdatum, ab dem diese für ungültig erklärt werden. Falls ein Zertifikat vor diesem Datum aus dem Verkehr gezogen werden sollen, wird die Information über den Ablauf ebenfalls von der CA über einen Verzeichnisdienst bekannt gegeben. Wegen des möglichen großen Andrangs bei den CAs können diese einen Teil ihrer Aufgaben, nämlich die Kontrolle der Identität ihrer Kunden, an untergeordnete Registration Authorities (RAs) delegieren. CAs haben die Möglichkeit, sich ihrerseits über übergeordnete CAs abzusichern oder aber selbst ihre eigenen Zertifikate zu unterschreiben. CAs mit selbst unterschriebenen Zertifikaten werden auch als Root-CAs bezeichnet. Gegenüber Root-CAs kann ein Benutzer nur sein grundsätzliches Vertrauen aussprechen oder verweigern, eine Kontrolle der Integrität einer Root-CA ist nicht möglich. Abbildung 4.33 zeigt eine mögliche PKI.

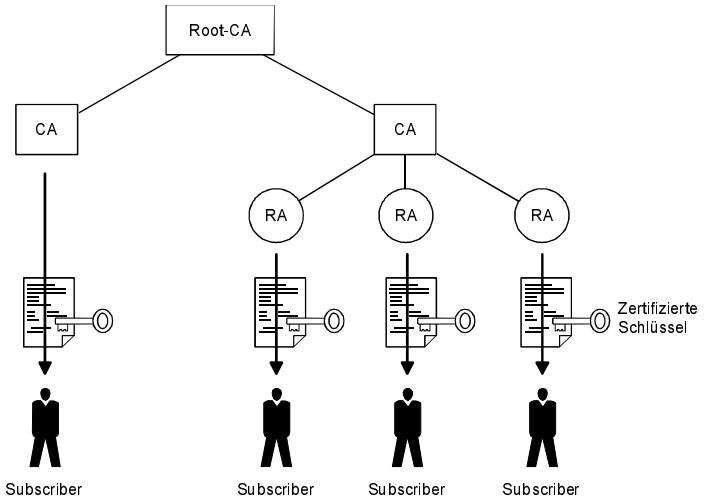


Abb. 4.33: PKI nach X.509

Der Kunde der CA – auch Subscriber genannt – erhält von der CA das Zertifikat, mit dem sein öffentlicher Schlüssel beglaubigt wird. Er muss seine Identität gegenüber der CA bzw. RA nachweisen, wobei die Qualität dieses Nachweises höchst unterschiedlich sein kann. In den meisten Fällen muss er eine Kopie seines Ausweises zur Verfügung stellen, bei so genannten Demo-Zertifikaten reicht allerdings auch die Angabe seiner E-Mail-Adresse aus. Je nach der Qualität seines Identitäts-Nachweises erhält er dann ein Zertifikat einer bestimmten Sicherheits-Kategorie.

Abbildung 4.34 zeigt als Beispiel ein Zertifikat, das von der kommerziellen CA GlobalSign ausgestellt wurde und zur Absicherung von Web- und E-Mail-Zugriffen eingesetzt werden kann. Die Sicherheitskasse 2 bedeutet bei GlobalSign, dass eine (nicht beglaubigte) Kopie des Personalausweises vorgelegt werden musste.

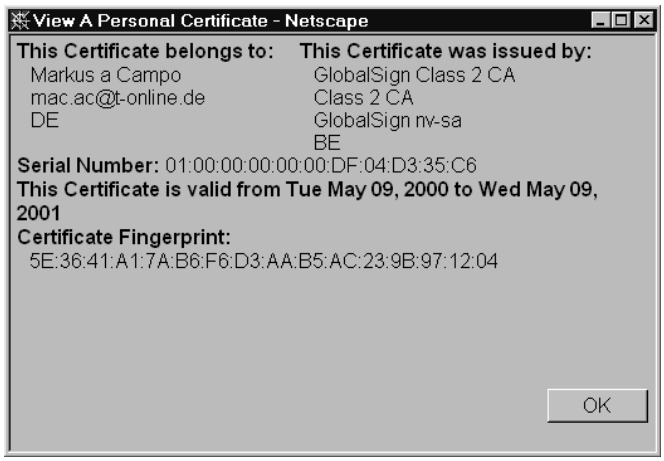


Abb. 4.34: Zertifikat nach X.509

Der Subscriber ist für die Geheimhaltung seines privaten Schlüssels selbst verantwortlich. Dieser wird in den meisten Fällen auf seinem PC abgelegt und durch eine Passphrase (eine Folge von einem oder mehreren Passworten) vor dem Zugriff Unberechtigter geschützt.

Der User schließlich ist die Instanz, die mit der Hilfe des zertifizierten öffentlichen Schlüssels dem Subscriber eine verschlüsselte Nachricht zukommen lassen will oder von diesem eine digital signierte Nachricht erhält. Er muss sich auf die Qualität des Zertifikats und dessen Gültigkeit verlassen können. In die meisten Browser ist eine Anzahl von CAs mit deren Root-CAs fest eingebaut, deren Zertifikaten dann vertraut werden kann (Abb. 4.32). Die Abbildungen 4.36 bis 4.38 zeigen die Vertrauenskette vom Subscriber-Zertifikat der Abbildung 4.34 bis zu einer Root-CA mit selbst unterschriebenem Zertifikat.

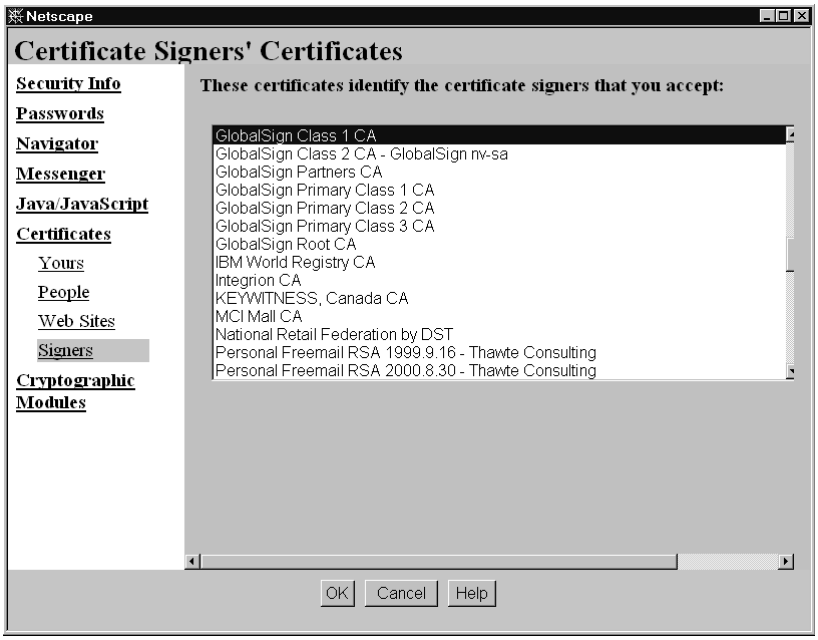


Abb. 4.35: CAs im Netscape-Browser

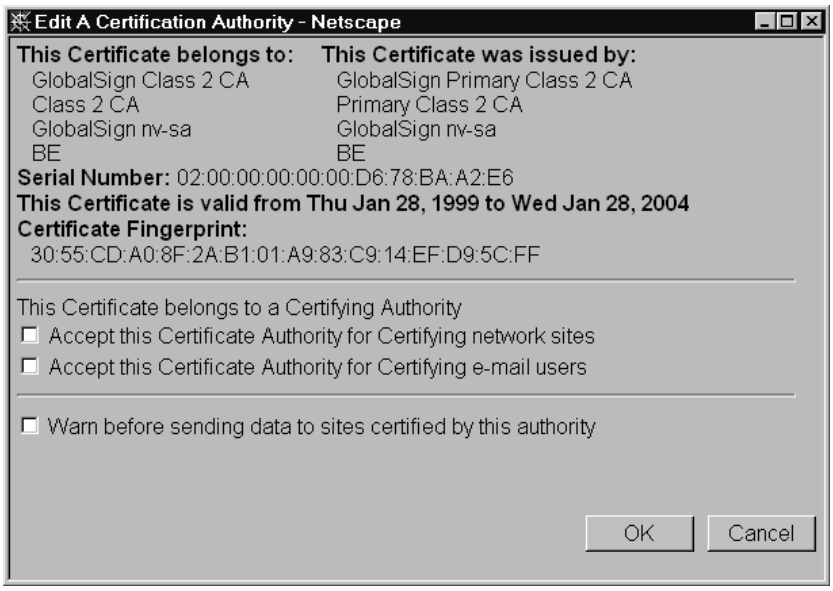


Abb. 4.36: Zertifikat von GlobalSign

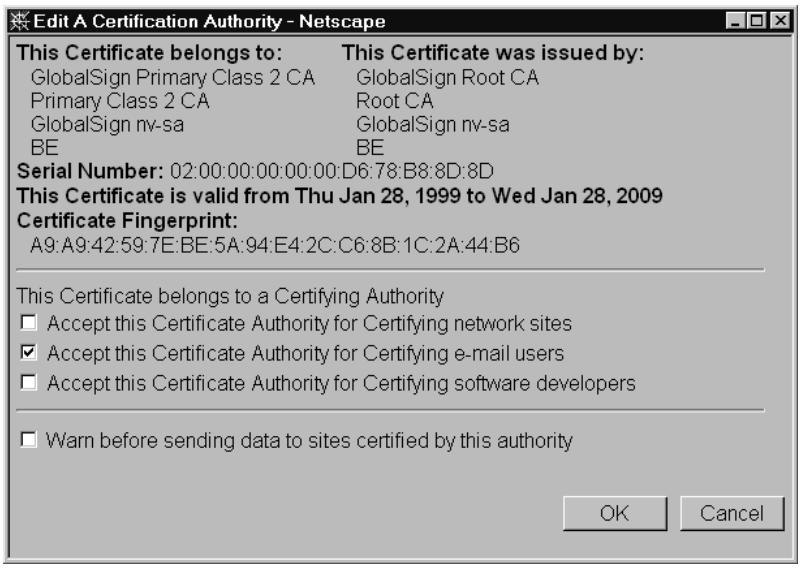


Abb. 4.37: Zertifikat von GlobalSign

Abb. 4.38: Root-Zertifikat von GlobalSign

Aufbau eines X.509-Zertifikats

X.509-Zertifikate bestehen aus drei Teilen, die in Tabelle 4.2 dargestellt werden.

Datenstruktur	Bedeutung
tbsCertificate	Zertifikat-Rumpf
signatureAlgorithm	Algorithmen, mit denen der Hash des Zertifikats gebildet und signiert wurde; mögliche Hash-Funktionen sind MD2 (veraltet!), MD5 oder SHA; signiert wird mit DSA oder RSA
signatureValue	Digitale Signatur der CA

Tabelle 4.2: Aufbau eines X.509-Zertifikats

Der Zertifikat-Rumpf hat die in Tabelle 4.3 dargestellte Struktur.

Datenstruktur	Bedeutung
version	X.509-Version (0, 1 oder 2), 2 bedeutet die aktuelle Version X.509v3
serialNumber	Eindeutige Seriennummer des Zertifikats
signature	Algorithmen, mit denen der Hashwert des Zertifikats gebildet und signiert wurde; identisch zu signatureAlgorithm in Tab. 4.1
issuer	Eindeutiger Name der Institution, die das Zertifikat ausgestellt hat
validity	Gültigkeitsbereich des Zertifikats (von / bis)
subject	Eindeutiger Name des Subscribers (Inhaber des zugeordneten Schlüsselpaars)
subjectPublicKeyInfo	Algorithmus (RSA, DSA oder Diffie-Hellman) und Wert des öffentlichen Schlüssels
issuerUniqueID	optional: eindeutige Identifikation der Institution, die das Zertifikat ausgestellt hat; wird nur benutzt, wenn der im Feld issuer angegebene Name in einem neuen Zusammenhang wieder verwendet werden soll
subjectUniqueID	optional: eindeutige Identifikation des Subscribers; wird nur benutzt, wenn der im Feld subject angegebene Name in einem neuen Zusammenhang wieder verwendet werden soll
extensions	optionale Erweiterungen des Zertifikats

Tabelle 4.3: Zertifikat-Rumpf nach X.509

Mit den im letzten Feld angegebenen optionalen Erweiterungen kann ein X.509-Zertifikat leicht an vorgegebene PKIs adaptiert werden.

Falls die CA, die das Zertifikat ausgestellt hat, sich über eine in der Hierarchie höher stehende CA legitimiert, müssen zwei Zertifikate mit den dazugehörigen Schlüsseln an den User übertragen werden usw.

4.3.2 Pretty Good Privacy (PGP)

Eins der ältesten Verfahren zur Absicherung mittels öffentlicher Schlüssel ist PGP. Der Entwickler von PGP – Phil Zimmermann – begann bereits Mitte der achtziger Jahre mit seiner Arbeit an dem Programm. Die erste lauffähige Version wurde 1991 fertiggestellt. Da PGP frei verfügbar ist, hat es eine große Verbreitung erfahren.

PGP nutzt zur Erzeugung von Schlüsseln bzw. deren Austausch die Verfahren Diffie-Hellman und RSA. Die eigentlichen Daten können wahlweise mittels AES, IDEA, Triple-DES oder CAST (in diesem Buch nicht besprochen) verschlüsselt werden. Der für die digitale Signatur erforderliche Hashwert wird nach SHA-1 oder MD5 gebildet.

Im Unterschied zu X.509 verfügt das klassische PGP nicht über eine streng hierarchische Struktur von Vertrauensverhältnissen. Statt dessen wird ein so genanntes »Web of Trust« (Abb. 4.39) installiert, bei dem sich die Teilnehmer gegenseitig vertrauen. Jeder Benutzer hat auf seinem Rechner einen Schlüsselbund installiert, dessen Elemente die öffentlichen Schlüssel seiner Partner sowie Angaben über die Gültigkeit der Schlüssel und die Vertauenswürdigkeit seiner Besitzer sind (Abb. 4.40). Die Elemente des Schlüsselbunds (Abb. 4.38) entsprechen von ihrer Funktion her den Zertifikaten aus X.509 und können per E-Mail oder über sogenannte Key-Server verteilt werden. Die kommerzielle Implementierung von PGP lässt dem Administrator die Wahl zwischen den PGP-Zertifikaten und einer X.509-konformen Struktur mit hierarchischen Vertrauensverhältnissen.

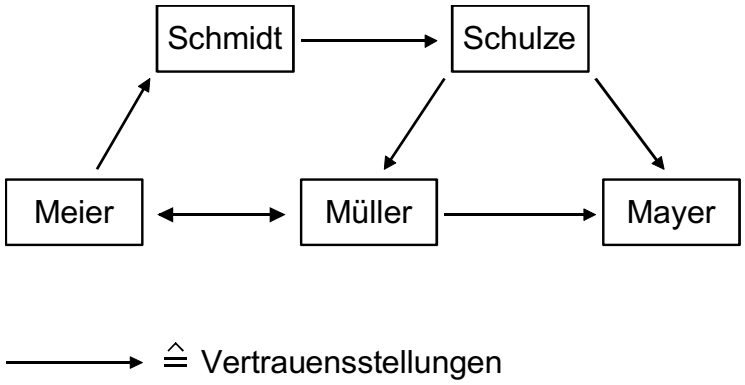


Abb. 4.39: Web of Trust

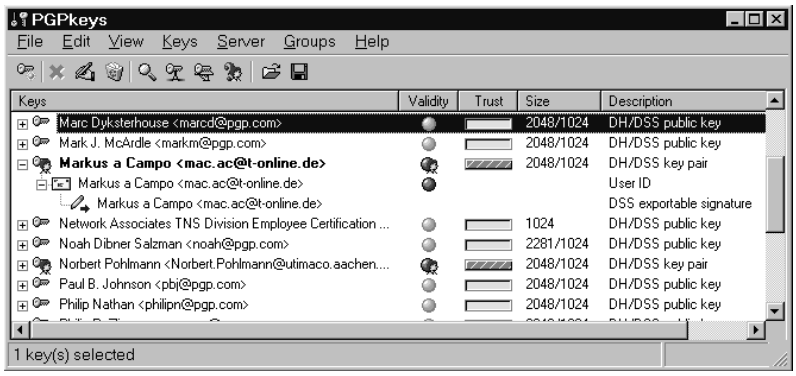


Abb. 4.40: PGP-Schlüsselbund

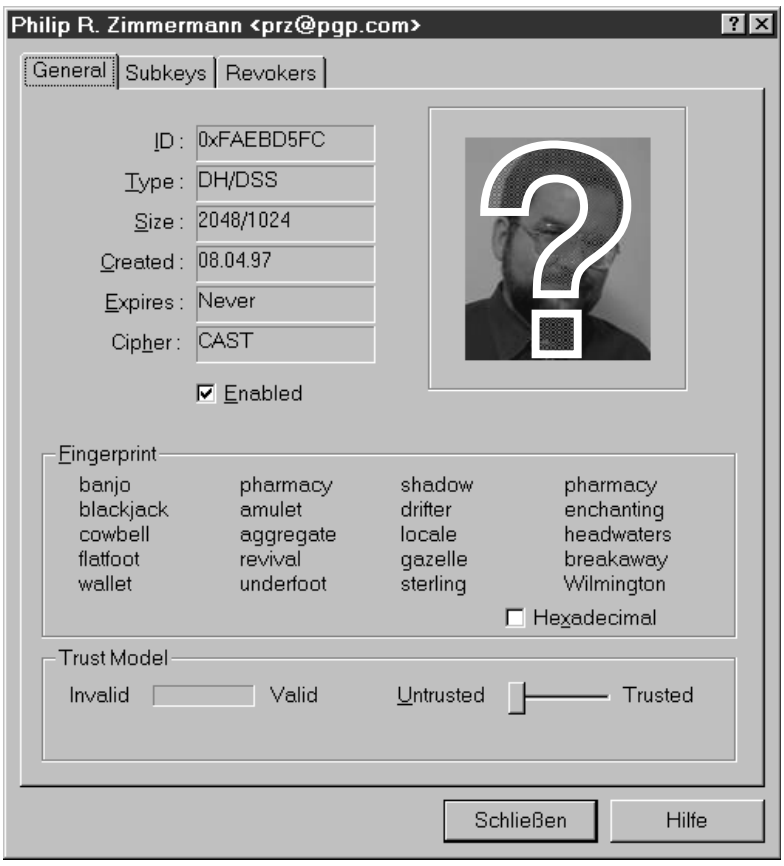


Abb. 4.41: PGP-Zertifikat

4.3.3 Verzeichnisdienste und das LDAP-Protokoll

Ein Verzeichnisdienst ist ein über Netzwerk zugänglicher Server, der über die Angabe von Namen und Attributen nach bestimmten Eigenschaften eines zugeordneten Objekts sucht. Dabei ist die Art, in der die Objekte in das Verzeichnis eingetragen werden können, in weiten Grenzen frei definierbar. In den Standards X.400 und X.500 wurde ein allgemeiner Verzeichnisdienst definiert, der sich für die Praxis im Internet allerdings als zu kompliziert erwiesen hat. Eine vereinfachte Version des Zugriff auf einen Verzeichnis-Servers wird in der LDAP-Spezifikation (Lightweight Directory Access Protocol) beschrieben. Abbildung 4.42 zeigt ein Beispiel für eine allgemein gehaltene Verzeichnis-Struktur, die mittels LDAP im Netzwerk publiziert werden könnte.

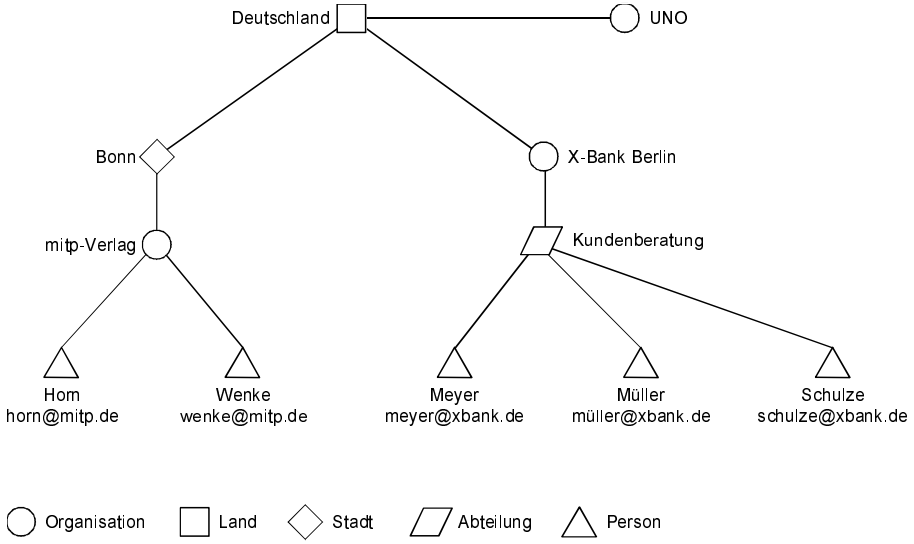


Abb. 4.42: Verzeichnis-Struktur

Die Verwaltung von zertifizierten Schlüsseln ist eine typische Anwendung für einen Verzeichnisdienst. Deshalb greifen Zertifizierungs-Systeme gerne auf diese Infrastruktur zurück. Die Zertifizierung nach dem Standard X.509 ist sogar von ihren Datenstrukturen her auf die Zusammenarbeit mit Verzeichnisdiensten abgestimmt.

Zur Unterscheidung der am Prozess der Zertifizierung und Überprüfung von Schlüsseln beteiligten Instanzen wird der so genannte Distinguished Name (DN) als Unterscheidungsmerkmal zwischen Objekten benutzt.

Diese Datenstruktur besteht ihrerseits aus verschiedenen Komponenten, die beispielsweise die ausstellende Instanz beschreiben (Tab. 4.4):

Schlüsselwort	Kürzel	Bedeutung
CommonName	CN	Name des Objekts
LocalityName	L	Ort
StateOrProvinceName	ST	US-Bundesstaat/Provinz
OrganizationName	O	Organisation
OrganizationalUnitName	OU	Organisatorische Untereinheit
CountryName	C	Staat
StreetAddress	STREET	Straßenname
Email	Email	E-Mail-Adresse

Tabelle 4.4: Komponenten des Distinguished Names (DN)

Der Distinguished Name (DN) besteht aus einer eindeutigen Zusammenstellung der in der Tabelle genannten Einträge.

Mit Hilfe dieser Begriffe kann in einem LDAP-Server der dazugehörige zertifizierte Schlüssel gesucht werden. Auch die Übertragung vorzeitig abgelaufener Zertifikate (Revocation List) geschieht über den Zugriff auf einen DN. Das X.509-Zertifikat aus Abbildung 4.43 enthält zwei DN-Strukturen, je eine für den Herausgeber des Zertifikats (Issuer) und eine für den Subscriber (Subject):

Issuer: CN=GlobalSign Class 2A CA, O=GlobalSign nv-sa, C=BE

Subject: CN=Markus a Campo, C=DE, Email=mac.ac@t-online.de

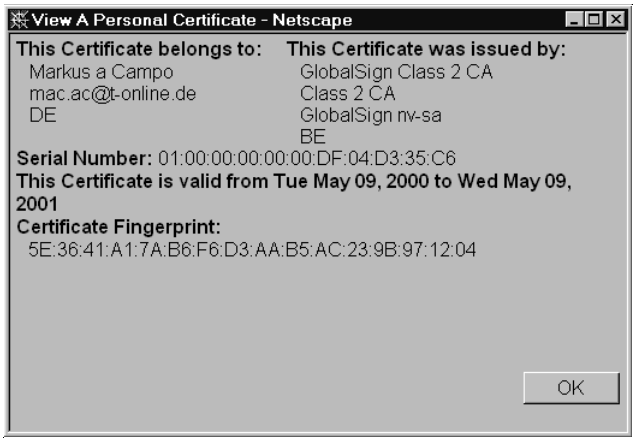


Abb. 4.43: Zertifikat nach X.509

Kapitel 5

Konzepte von Virtual Private Networks

In diesem Kapitel werden verschiedene Konzepte diskutiert, nach denen VPN-Systeme aufgebaut werden können, die zur Sicherstellung einer vertrauenswürdigen Kommunikation genutzt werden.

5.1 Ein VPN-Sicherheitssystem als transparente Lösung

Mit einer Sicherheitsschicht im Kommunikations-Stack kann aus einem »ungesicherten Netzdienst« ein »sicherer Netzdienst« gemacht werden. Hierzu wird im Rechnersystem eine geeignete Sicherheitsschicht (Security Sublayer) in die Kommunikationsarchitektur eingeführt. Eine spezielle und besonders im heterogenen Rechnerumfeld geeignete Möglichkeit, eine solche Sicherheitsschicht zu realisieren, ist zum Beispiel der Einsatz von IPSec in Black-Box-Sicherheitssystemen (siehe Abb. 5.1).

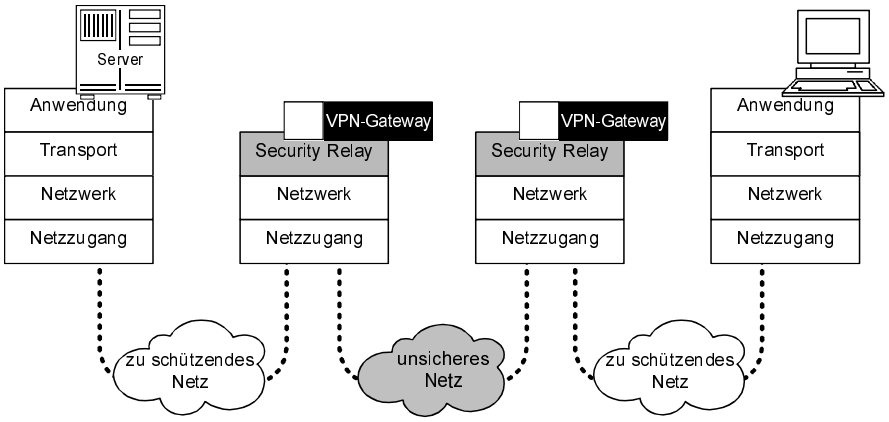


Abb. 5.1: Black-Box-Sicherheitssysteme

5.1.1 Black-Box-Lösung

Black-Box-Lösungen sind handliche Geräte, die auf einfache Weise zwischen Rechnersysteme und Netzwerkanschluss (LAN-Anschluss) geschaltet werden. Das macht sie unabhängig von den jeweiligen Endgeräten und Betriebssystemen und wegen ihrer einfachen Handhabung benutzerfreundlich. In der hochtechnisierten und »intelligenten« High-Tech Black Box spielen sich – unsichtbar für den Benutzer und ohne seine aktive Einwirkung – alle sicherheitsrelevanten Operationen ab.

Im folgenden Kapitel werden die Black Boxes als »VPN-Gateways« bezeichnet.

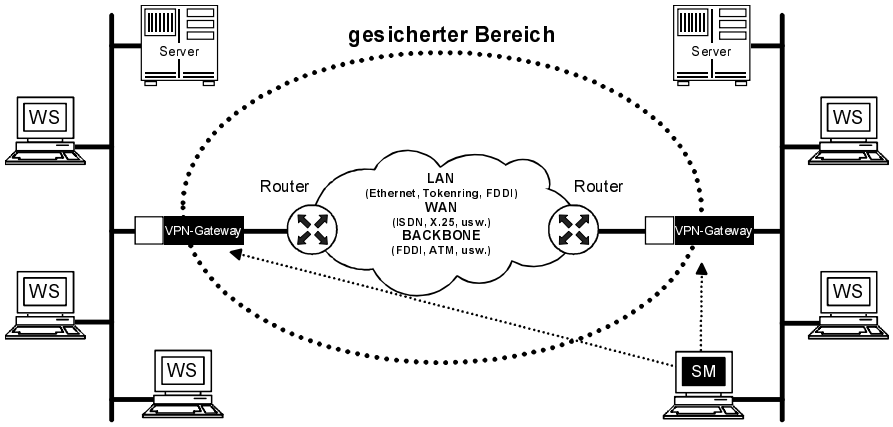


Abb. 5.2: 1:1-VPN mit Black-Box-Lösung

Alle Black Boxes eines Sicherheitssystems sollten von einem Security Management (SM) global gesteuert werden, wobei die Kommunikation – durch kryptographische Funktionen gesichert – über das Netz erfolgen muss.

Vor jedes Rechnersystem oder Subsystem, das geschützt oder über das vertrauliche Daten übertragen werden sollen, wird eine Black Box geschaltet, die sich ähnlich wie eine Bridge verhält. Die Schnittstellen sind beispielsweise zu beiden Seiten (Fast-, Giga-, ...)Ethernet oder Token Ring.

Die Security Black Boxes leisten erweiterte Sicherheitsdienste für das zu schützende Rechnersystem (siehe Abb. 5.2). In Zusammenarbeit mit einer entsprechenden Sicherheitseinrichtung auf der Gegenseite sorgen sie auch für eine kryptographische Sicherung der Kommunikation über das LAN/WAN hinweg.

Vorteile von Black-Box-Lösungen:

- Die Sicherheitseinrichtung Black Box ist unabhängig von Workstations (PCs, UNIX-Systeme, Host-Rechner, ...) und deren Betriebssystemen (Microsoft DOS, Microsoft Windows 95/98/NT/2000/..., OS/2, LINUX, VMS usw.). Das

bedeutet, dass die Black Box auch bei einem Wechsel von Endgeräten oder Workstations weiterhin verwendet werden kann.
- Die Black-Box-Lösung erlaubt die Einrichtung von Sicherheitsfunktionen zwischen Endsystemen, in die ansonsten keine Sicherheitsfunktionen integriert werden könnten (zum Beispiel Terminals oder Routern).
- Bei heterogenen Systemen (unterschiedliche Hardware, Software, Betriebssysteme, ...) kann immer die gleiche Black Box verwendet werden, wodurch sich der notwendige Aufwand verringert.
- Black Boxes sind leichter gesichert zu realisieren als spezielle Software-Lösungen in Rechnersystemen.
- Die Sicherheitseinrichtungen sind hinsichtlich der Sicherheitsqualität unabhängig von anderen Systemkomponenten.
- Die Sicherheit ist anwendungsunabhängig.

Sicherheitsdienste eines VPN-Gateway

Ein VPN-Gateway kann unterschiedliche Sicherheitsdienste bieten:

- Vertraulichkeit,
- Datenintegrität,
- Authentikation (implizit – über die Verschlüsselung – oder explizit mit einem speziellen Authentikationsprotokoll),
- Zugangskontrolle (für Pakete oder Benutzer),
- Rechteverwaltung (für Kommunikationsprotokolle und -dienste),
- Beweissicherung und
- Protokollauswertung.

Dadurch wird erreicht, dass

- Daten nicht im Klartext gelesen werden können,
- keine Manipulation der Daten stattfinden kann,
- nur logische Verbindungen zustande kommen, die erlaubt sind,
- nur Kommunikationsprotokolle und -dienste verwendet werden, die erlaubt sind,
- keine Fremden in der Lage sind, auf Rechnersysteme zuzugreifen, und
- sicherheitsrelevante Ereignisse protokolliert und ausgewertet werden können.

Es gibt gute Gründe für den Einsatz hardwarebasierter VPN-Gateways: Weil die Verschlüsselung unabhängig vom PC- und Netzwerkbetriebssystem durchgeführt wird, beeinträchtigen hardwarebasierte VPNs nicht die Effektivität des Netzwerks. Die Installation erfordert kaum Eingriffe in die vorhandene Netzwerkstruktur und verursacht keinen Aufwand für die mühsame Installation von Software auf einzelnen Rechnern. Weil die Installation relativ einfach vonstatten geht und auf Anwenderseite kaum netzwerktechnisches Know-How vorhanden sein muss, eignet sich die Einrichtung und der Betrieb hardwarebasierter VPN-Gateways auch als Service-Geschäftsmodell für Internet Service Provider.

5.1.2 Security Sublayer im Endgerät: End-to-End-Verschlüsselung

Eine weitere Möglichkeit, die notwendigen Sicherheitsfunktionen einzurichten, ist die Integration einer Sicherheitsschicht in die Rechnersysteme.

Dafür wird zum Beispiel auf den Netzwerkdienst, der von den Netzwerktreibern angeboten wird, ein sogenanntes »Security Sublayer« aufgesetzt. Dieses Security Sublayer bietet der Transportschicht alle Services des Netzwerktreibers – mit dem Unterschied, dass eine Verbindung nur bei Bedarf mit den gewünschten Sicherheitsmerkmalen versehen wird. Aus Sicht des Netzwerktreibers (Netzwerkebene) verhält sich das Security Sublayer wie eine Transportschicht, aus Sicht der Transportschicht verhält es sich wie der Netzwerktreiber. Das Security Sublayer ist somit völlig transparent gegenüber den benachbarten Schichten.

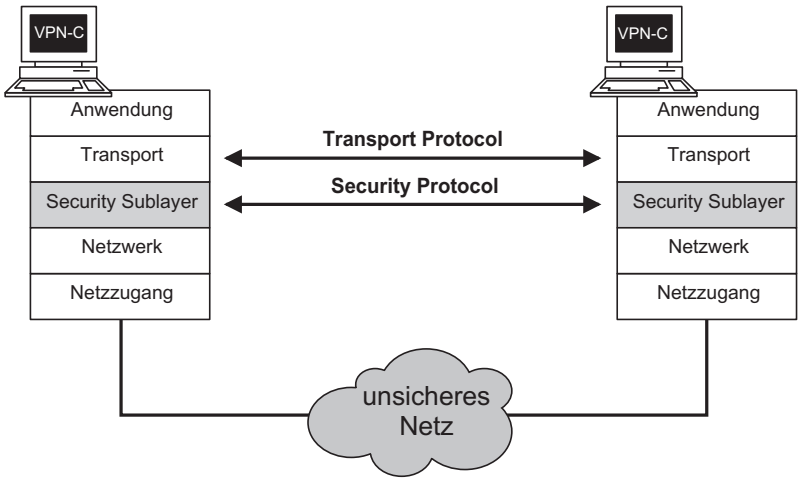


Abb. 5.3: End-to-End-Sicherheit mit PC Security Komponente

In der Praxis wird das Security Sublayer softwaremäßig als transparenter Netzwerktreiber in das Rechnersystem installiert. Wegen der höheren Sicherheit sollte bei einer solchen Lösung unterstützend eine Verschlüsselungskarte verwendet werden, in der die geheimen Schlüssel gespeichert sind.

Vorteile des VPN-Clients:

- Der VPN-Client ist kostengünstiger als die Black-Box-Lösung.
- Der VPN-Client bietet End-to-End-Sicherheit. Das bedeutet, dass nicht nur die Verbindung zwischen verschiedenen LAN-Segmenten nach außen hin abgeschottet wird, sondern auch jede einzelne Workstation (PC) gegenüber anderen.
- Eine »Person« kann authentisiert werden.

Sicherheitsdienste von PC-Security-Komponenten

Eine VPN-Client bietet unterschiedliche Sicherheitsdienste:

- Vertraulichkeit,
- Datenintegrität,
- Authentikation (implizit – über die Verschlüsselung – oder explizit mit einem speziellen Authentikationsprotokoll),
- Zugangskontrolle (für Pakete),

Dadurch wird erreicht, dass

- Daten nicht im Klartext gelesen werden können,
- keine Manipulation der Daten stattfinden kann,
- nur logische Verbindungen zustande kommen, die erlaubt sind,
- keine Fremden in der Lage sind, auf Rechnersysteme zuzugreifen.

Anwendungsmöglichkeiten und Einsatzvarianten

Mit einem VPN-Gateway und mit einem VPN-Client kann der Sicherheitsdienst Verschlüsselung in unterschiedliche Anwendungsgebiete integriert werden. In LANs können ausgewählte Segmente, bestimmte logische Bereiche oder Anwendungen geschützt werden. Bei der Kopplung von LAN-Segmenten über öffentliche Netze können mit einem VPN-Gateway Angreifer abgewehrt und kryptographisch abgesicherte, vertrauenswürdige logische Netze gebildet werden.

5.1.3 Sicherheit in LAN-Segmenten

Die Integrationsvariante »Sicherheit in LAN-Segmenten« schützt ausgewählte Segmente, logische Bereiche in einem Segment, ausgewählte Rechnersysteme oder Anwendungen innerhalb eines Segments des LAN, beispielsweise die Personalverwaltung (m:n-Topologie).

In den VPN-Gateways stehen Access-Listen und weitere sicherheitsrelevante Informationen. Außerdem stellen sie ein Logbuch zur Verfügung, in dem sicherheitsrelevante Ereignisse protokolliert werden. Die Kommunikationsbeziehungen werden in diesem Anwendungsbeispiel mit Hilfe der Adressen der Netzzugangsebene (MAC-Adressen), die möglichen höheren Protokolle mit Hilfe des Typenfelds bestimmt.

Je nach Einstellung werden die Datenpakete der Netzzugangsebene

- im Klartext durchgelassen,
- in verschlüsselter Form durchgelassen oder
- abgeblockt.

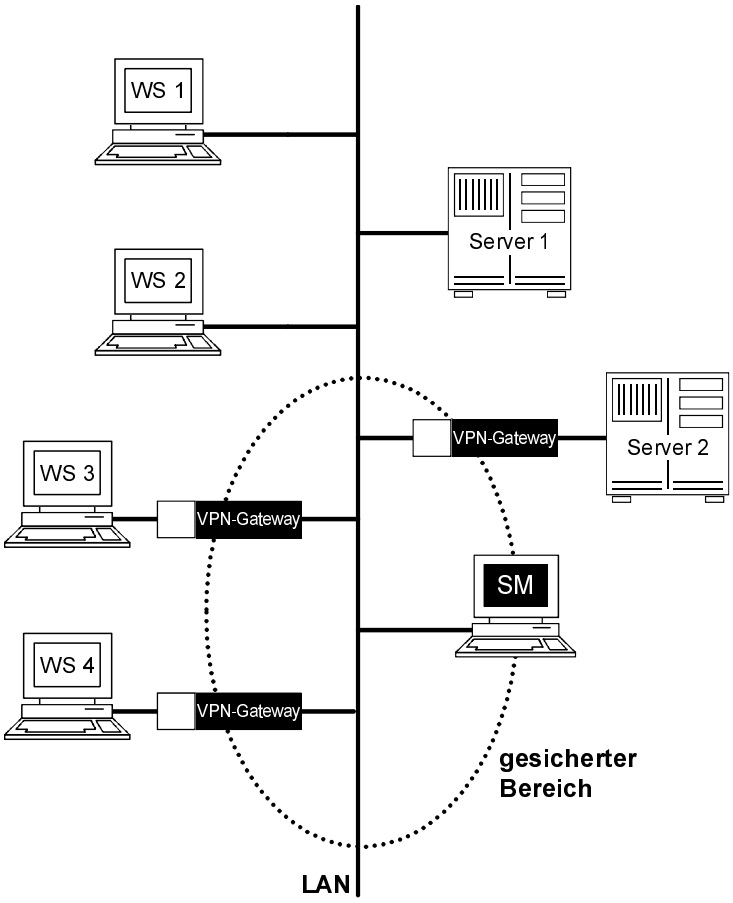


Abb. 5.4: Sicherheit in LAN-Segmenten

In diesem Beispiel (Abb. 5.4) wird dargestellt, wie die Absicherung der Kommunikation der beiden Workstations 3 und 4 mit dem Server 2 gesichert, das heißt verschlüsselt und kontrolliert werden kann. Im LAN-Segment soll niemand in der Lage sein, die übertragenen Daten im Klartext mitzulesen. Falls die Workstation 4 eine Kommunikation mit dem Server 2 durchführen möchte, wird das MAC-Paket von der Workstation 4 an das VPN-Gateway gesendet. Dieses prüft anhand der Access-Liste, ob eine Verbindung zwischen der Workstation 4 und dem Server 2 erlaubt ist (Packet-Filter-Funktion). Im vorliegenden Beispielfall ist eine verschlüsselte Kommunikation erlaubt.

Anschließend wird im VPN-Gateway der Inhalt des MAC-Paketes verschlüsselt und zur Gegenseite übertragen. Das VPN-Gateway vor dem zu schützenden Server 2 liest das MAC-Paket, stellt in seiner Access-Liste fest, dass eine verschlüsselte Kommunikation zwischen der Workstation 4 und dem Server 2 erlaubt ist, und

entschlüsselt das MAC-Paket entsprechend. Anschließend sendet das VPN-Gateway das MAC-Paket im Klartext zum Server 2. Für die Workstation 4 und den Server 2 bleiben die Sicherheitsfunktionen transparent. Die Steuerung des VPN-Gateway wird in gesicherter Form durch ein zentrales Sicherheitsmanagement realisiert.

Möchte die Workstation 4 mit Server 1 kommunizieren, sendet sie dazu ein MAC-Paket auf das LAN-Segment. Im VPN-Gateway der Workstation 4 wird das Paket angenommen. Anhand der Access-Liste wird festgestellt, dass es sich um eine erlaubte Klartextverbindung handelt. Das Paket kann daher das VPN-Gateway im Klartext passieren und gelangt über das LAN zum Server 1.

Wenn die Workstation 2 auf Server 2 zugreifen will, sendet sie das MAC-Paket im Klartext. Das VPN-Gateway von Server 2 nimmt das Paket auf und stellt fest, dass es sich um eine nicht erlaubte Verbindung handelt. Das Paket wird deshalb vom Packet Filter verworfen. Dieses sicherheitsrelevante Ereignis wird entweder im Logbuch gespeichert oder, falls dies so eingestellt ist, als »Spontane Meldung« an das Sicherheitsmanagement (SM) gesendet.

Merkmale der MAC-Verschlüsselung

- Die MAC-Verschlüsselung ist unabhängig vom Netzwerkprotokoll (wie IPX, NLSP, LLC, Netbios, Decnet, SNA usw.).
- Die Verschlüsselung ist unabhängig vom verwendeten Netzwerk-Betriebssystem.
- Die Passworte der Netzwerk-Betriebssysteme (zum Beispiel Netware) werden in verschlüsselter Form übertragen.

5.1.4 Kopplung von LAN-Segmenten mit einer Security Bridge

Bei der Integrationsvariante »Kopplung mehrerer LAN-Segmente« werden zwei LAN-Segmente verbunden (Twisted Pair, Glasfaser usw.), die über einen öffentlich zugänglichen Bereich miteinander gekoppelt sind. Die Kabel in diesem öffentlich zugänglichen Bereich (im vorliegenden Beispiel Gebäudekomplex B, siehe Abb. 5.5) werden mit einem VPN-Gateway als 1:1-VPN gesichert. Dies ist eine einfache Möglichkeit, die notwendige Sicherheit zu garantieren.

Ein Beispiel für die Kopplung mehrerer LAN-Segmente ist die Kommunikation zwischen Bürogebäude und Fertigungshalle: In den Büroräumen (Gebäudekomplex C) steht das Verwaltungssystem (Server). Aus der Fertigungshalle (Gebäudekomplex A) werden Softwarebestände, Seriennummern für die Produkte, Lieferscheine usw. benötigt. Aus diesem Grund müssen die Workstations aus der Fertigungshalle des Gebäudekomplexes A Zugriff auf das Verwaltungssystem (Server) des Gebäudekomplexes C haben.

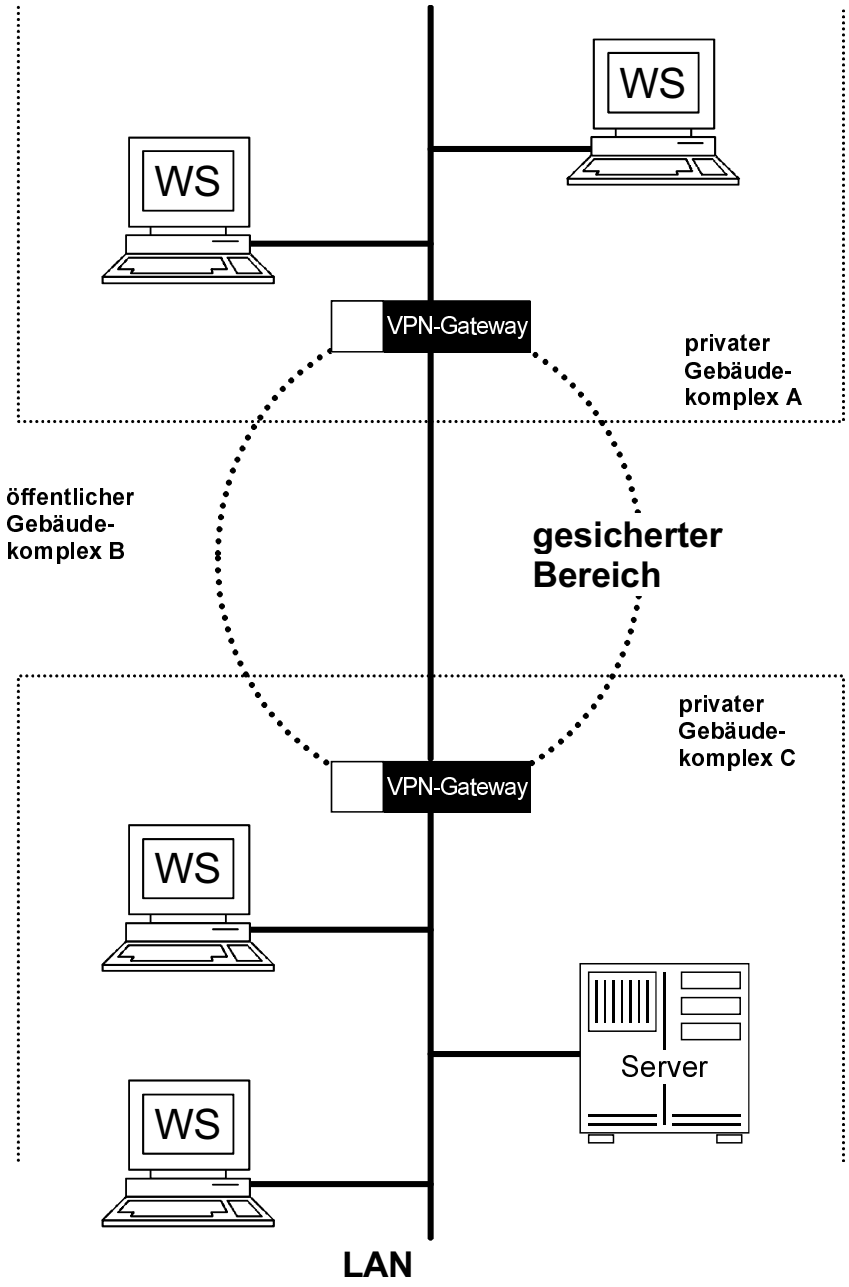


Abb. 5.5: Security Bridge für mehrere LAN-Segmente

In diesem Beispiel ist die Verwendung von VPN-Gateways eine einfache Möglichkeit, die notwendige Sicherheit zu garantieren. Die VPN-Gateways garantieren hier zusätzlich zum »Bridging« die Vertraulichkeit der Daten durch die Verschlüsselung der MAC-Pakete und verhindern, dass Fremde auf das System zugreifen können. Durch die Verschlüsselung wird eine implizite Authentikation erreicht, so dass Fremde nicht in der Lage sind, sinnvolle Pakete in das LAN zu senden.

In dieser Integrationsvariante kann eine solche VPN-Gateway auch als Security Repeater betrieben werden. Dann werden alle Pakete des VPN-Gateways auf der MAC-Ebene ver- bzw. entschlüsselt.

5.1.5 Kopplung von LAN-Segmenten über öffentliche Netze

Mit den folgenden Integrationsvarianten kann die Kommunikation auf der Netzwerkebene, der IP-Ebene, geschützt werden. Dies entspricht zum Beispiel der Bildung von Virtual Private Networks (VPN) nach dem IPSec-Standard.

Anwendungsmöglichkeiten dafür sind

- die Kommunikation aller Rechnersysteme in einem LAN,
- die Kommunikation ausgewählter Rechnersysteme in einem LAN oder
- die Kommunikation über öffentliche Netze beziehungsweise über ein Backbone.

In der folgenden Abbildung 5.6 ist eine Integrationsvariante dargestellt, bei der die Kommunikation über ein öffentliches Netz (ISDN, X.25, Leased Line oder ähnliches), Satellitenübertragung oder ein Backbone (FDDI, ATM usw.) gesichert wird.

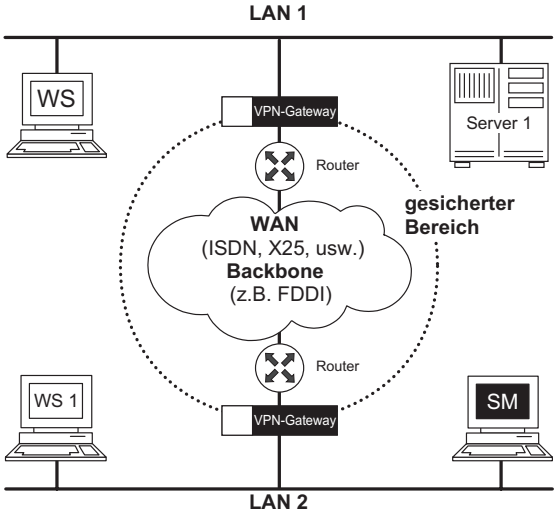


Abb. 5.6: Kopplung von LAN-Segmenten über öffentliche Netze

Die VPN-Gateways werden zur Netzwerksicherung vor den Routern positioniert.

In dieser Integrationsvariante werden die Kommunikationsbeziehungen mit Hilfe der IP-Adressen bestimmt. Je nach Einstellung werden die IP-Pakete von den VPN-Gateways im Klartext oder verschlüsselt durchgelassen oder abgeblockt.

Möchte die Workstation 1 auf Server 1 zugreifen, sendet die Workstation 1 das IP-Paket im Klartext in das LAN. Das VPN-Gateway vor dem Router empfängt das IP-Paket und überprüft in den Access-Listen die Regeln. Falls eine verschlüsselte Verbindung zwischen Workstation 1 und Server 1 erlaubt ist, verschlüsselt das VPN-Gateway das IP-Paket. Der Header des IP-Paketes bleibt unverschlüsselt, damit er vom Router vermittelt werden kann.

In diesem Konzept spielt es aus Sicht des VPN-Gateway keine Rolle, ob die Kommunikation über ISDN, über Satellit, oder über andere Wege erfolgt. Das VPN-Gateway führt in jedem Fall die gleichen Sicherheitsfunktionen aus.

Auf der Gegenseite empfängt das VPN-Gateway das IP-Paket und erkennt in der Access-Liste, dass es sich um eine erlaubte verschlüsselte Kommunikation handelt. Das VPN-Gateway entschlüsselt dann das IP-Paket entsprechend und sendet es im Klartext zum Server 1. Auch hier bleibt die Sicherheit für die beteiligten Komponenten (Workstations, Server, Router usw.) transparent. Die Rechteverwaltung wird zentral von einem Sicherheitsmanagement (SM) realisiert. In einer solchen Konfiguration ist es auch möglich, die Rechteverwaltung sehr einfach zu gestalten. So kann zum Beispiel über die Sub-Adressen der LANs die einfache Regel »Verschlüsselung aller Pakete, die zu den entsprechenden LANs gehören« definiert werden.

Ein besonderer Vorteil dieser Lösung ist, dass sie auch die Sicherheitsanforderungen für Backup und flexible Bandbreiten erfüllt. Weil die Sicherheit unabhängig vom Übertragungsmedium ist, kann immer ein gleich hohes Maß an Sicherheit garantiert werden, auch wenn beispielsweise im Normalbetrieb über eine Standleitung kommuniziert und im Backup-Fall das ISDN-Netz verwendet wird.

Die Funktion eines VPN-Gateways und eines Routers sollte aus sicherheitstechnischer Sicht und aus Gründen der Performance immer von getrennten Komponenten ausgeübt werden.

Router mit IPSec-Funktionalität zeigen meist starke Leistungseinbrüche und bilden daher einen »Flaschenhals«. Aus diesem Grunde stellt der Router die Verbindung zum WAN7-Backbone dar. Zwischen Router und dem LAN-Segment wird das VPN-Gateway positioniert.

Tunneling

Beim Tunneling wird jedes zu sendende Paket in ein neues Paket verpackt. Dazu wird ein zusätzlicher neuer Header vorgeschaltet. So wird beispielsweise für IP-basierte Netze ein IP-Header vorangestellt. Weiterhin kommen zusätzliche Informationen oder Kennzeichen im Body-Teil des Pakets dazu.

Die vorgeschalteten Header charakterisieren die Endpunkte des Tunnels; die »eingepackten« Header beschreiben die eigentlichen IP-Adressen (Rechnersysteme), zwischen denen die Kommunikation stattfinden soll. Die Adressbereiche können auch unterschiedlich sein. Mit Tunneling kann aber auch ein beliebiges Paket (zum Beispiel IP oder IPX) verpackt übertragen und am Ziel wieder entpackt werden. Die dazwischenliegenden Router »wissen« nichts von diesen Mechanismen / Pohl99d/.

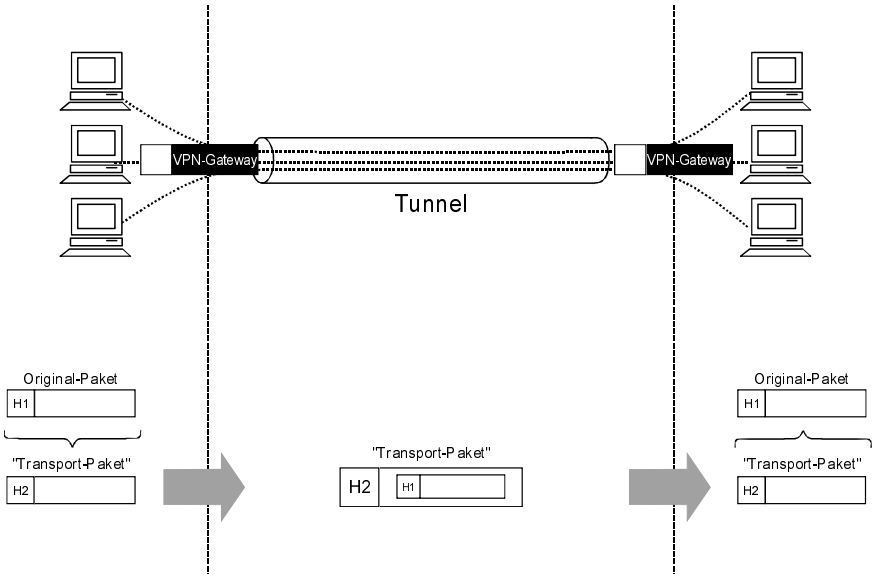


Abb. 5.7: Tunneling

Ein Vorteil von Tunneling ist, dass bei der Kommunikation über eine öffentliche Infrastruktur – beispielsweise zwischen zwei Organisationen – immer nur zwei IP-Adressen verwendet werden, unabhängig davon, über welchen Weg die Kommunikation tatsächlich stattfindet. Im Tunnel können auch nicht routbare Protokolle eingepackt werden.

Falls die getunnelte Verbindung verschlüsselt wird, kann auch ein gewisser Schutz vor einer Verkehrsflussanalyse gewährleistet werden, da die Quell- und Ziel-Adressen im getunnelten Header verschlüsselt sind und nur die Adressen der Komponenten, die das Tunneling realisieren, sichtbar werden. Andererseits können dann Features wie Prioritätensteuerung nicht mehr verwendet werden.

5.1.6 Bildung von kryptographisch gesicherten logischen Netzen (VPN)

VPN-Gateways können auch vor bestimmten Rechnersystemen platziert werden. Hierdurch wird eine höhere »Tiefe« der »End-to-End-Sicherheit« erreicht.

Mit dieser Integrationsvariante können sichere logische Netze in einem Gesamtnetz realisiert werden. Es ist auch möglich, mehrere logische Netze parallel oder geschachtelt zu betreiben. Ein VPN-Gateway kann dann auch zu mehreren logischen Netzen gehören.

Damit können bestimmte, besonders sicherheitsrelevante Bereiche (der arbeitsmedizinische Bereich, die Personalabteilung, Geschäftsführung, Forschungs- oder Marketing-Abteilung) geschützt werden (m:n-Topologie). Alle Daten, die zwischen den Rechnersystemen ausgetauscht werden, sind verschlüsselt.

In den beschriebenen Virtual Private Networks (VPNs) können verschiedene Strategien verfolgt werden. So kann zum Beispiel festgelegt werden, dass die Kommunikation zwischen den Workstations 1, 2 und 3 immer verschlüsselt wird und alle anderen Kommunikationsverbindungen im Klartext ablaufen. Eine andere Strategie könnte vorsehen, dass nur eine Kommunikation zwischen den Workstations 1, 2 und 3 möglich ist, und das auch nur in verschlüsselter Form.

Merkmale der IP-Verschlüsselung

Die IP-Verschlüsselung ist unabhängig vom Übertragungsmedium und bietet daher einen hohen Investitionsschutz. Die Vertraulichkeit der Daten wird gewährleistet, auch die der Passworte wie beispielsweise bei Telnet, FTP oder rlogin.

Der Zugriff von Angreifern aus öffentlichen Netzen auf Rechnersysteme wird abgewehrt. Außerdem ist es mit einem solchen Sicherheitssystem möglich, Security Domains zu bilden.

5.1.7 VPN-Client

Ein VPN -Client kann eine Softwarelösung oder eine Kombination aus Software- und Hardwarelösung sein, die in das Rechnersystem integriert wird. Es handelt sich um ein Security Sublayer, das erweiterte Kommunikationssicherheitsdienste wie Verschlüsselung und Zugangskontrolle zur Verfügung stellt. Durch die Verwendung sicherer Hardware kann die vertrauliche Speicherung von geheimen

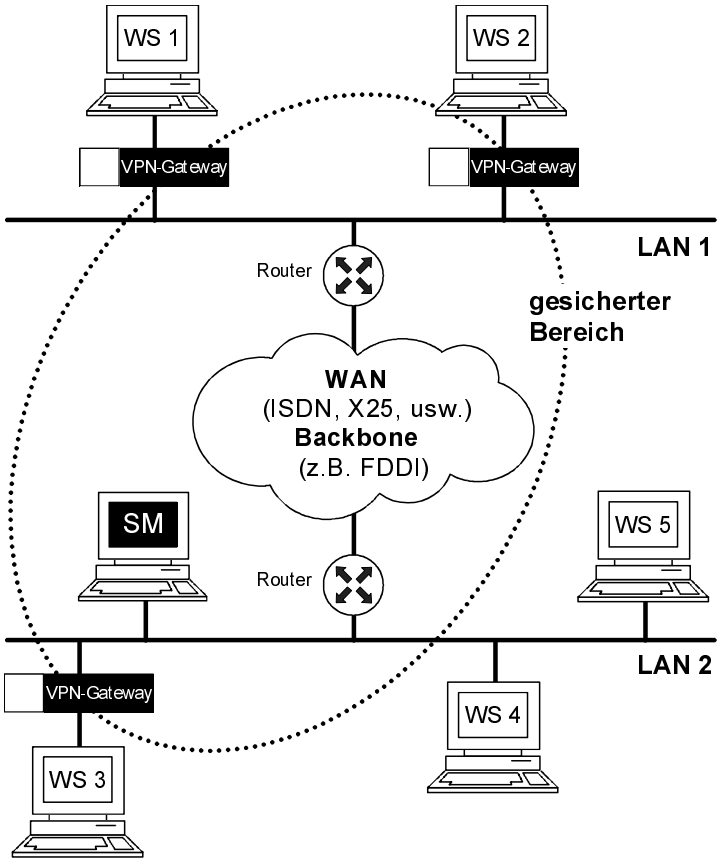


Abb. 5.8: End-to-End-Sicherheit

Schlüsseln gewährleistet werden. Mit Hilfe eines VPN-Clients kann die Verschlüsselung zwischen PCs, aber auch die Verschlüsselung zwischen einem PC und einem VPN-Gateway realisiert werden.

Wenn eine Workstation ohne VPN-Client mit dem Server-System 1 kommuniziert, kann dies über das Packet Filter anhand der festgelegten Protokolle und Dienste kontrolliert werden. Mit Hilfe des Sicherheitsmanagements können der VPN-Client sowie die VPN-Gateways gesteuert und verwaltet werden.

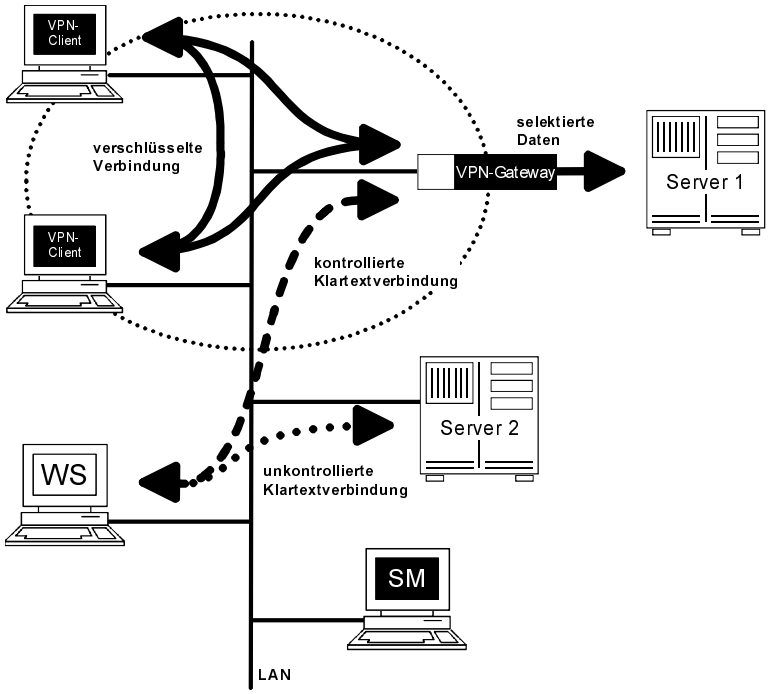


Abb. 5.9: VPN-Client

5.1.8 Anwendungsfälle

Die Notwendigkeit, Rechnersysteme »remote« an das lokale Netz einer Organisation anzukoppeln, wird zunehmend größer. Für Außendienstmitarbeiter wird es immer wichtiger, direkt auf Preislisten und Lieferzeiten zugreifen und Bestellungen eingeben zu können, damit der Arbeitsvorgang effektiv und ohne Medienbruch durchgeführt werden kann. Im Hinblick auf gesellschaftspolitische Entwicklungen und die Verfügbarkeit von Know-how wird es immer dringlicher, auch Heimarbeitsplätze anzubieten, die »remote« an das System angekoppelt sind. Die Eintrittswahrscheinlichkeit eines Angriffs ist aber gerade in der Umgebung von Remote-Rechnern besonders hoch einzustufen, so dass bei der Remote-Ankoppelung eine hohe Gefahr des Missbrauchs besteht.

Kopplung von mobilen Rechnersystemen (Notebooks)

Notebooks können z. B. mit einem Modem über die Telefonleitung oder mit einem Mobiltelefon über das Mobilfunknetz (z. B. GSM, GPRS, UMTS) an ein Server-System gekoppelt werden. Die Kombination von VPN-Client und VPN-Gateway bietet ein einfaches Konzept, das die notwendige hohe Sicherheit zur Verfügung stellt.

Im folgenden Beispiel (Abb. 5.10) werden die IP-Pakete vom Notebook in verschlüsselter Form über das Fernsprechnetz oder Mobilfunknetz gesendet und vom VPN-Gateway entsprechend entschlüsselt.

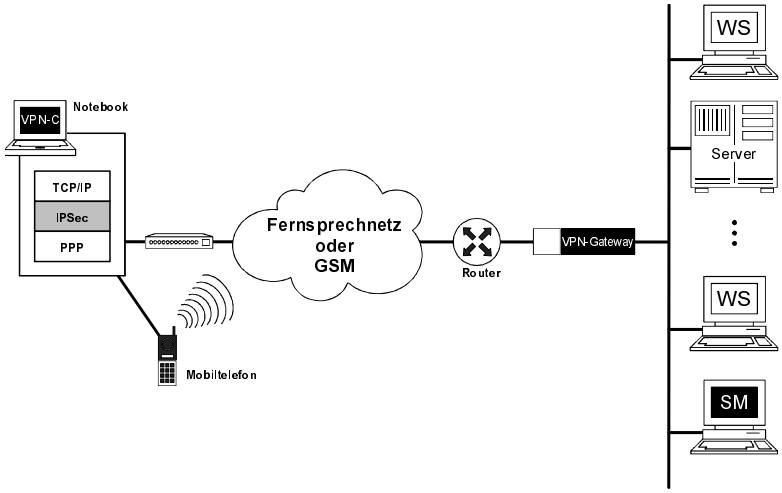


Abb. 5.10: Kopplung mobiler Rechnersysteme

Durch das VPN-Gateway kann bestimmt werden, welcher Benutzer auf welches Rechnersystem zugreifen darf, um beispielsweise Arbeiten abzuliefern oder neue Aufträge zu holen.

Kopplung von Tele-Arbeitsplätzen

Für die Einrichtung von Telearbeitsplätzen ist die Ankopplung über ISDN besonders interessant. ISDN ist in Deutschland flächendeckend verfügbar und inzwischen sind viele Millionen Anschlüsse darauf umgestellt; die Akzeptanz ist so hoch wie in keinem anderen Land.

Über das ISDN-Netz können IP-Pakete verschlüsselt und in gesicherter Form übertragen und auf der Seite der Zentrale durch das VPN-Gateway entschlüsselt werden. Das VPN-Gateway sorgt für eine effektive Abschottung, so dass kein Hacker in der Lage ist, auf die zu schützenden Rechnersysteme zuzugreifen.

Tele-Arbeitsplätze können so nicht nur durch die Verschlüsselung, sondern auch durch Überwachung und Kontrolle mit Packet-Filter-Funktionalität geschützt werden.

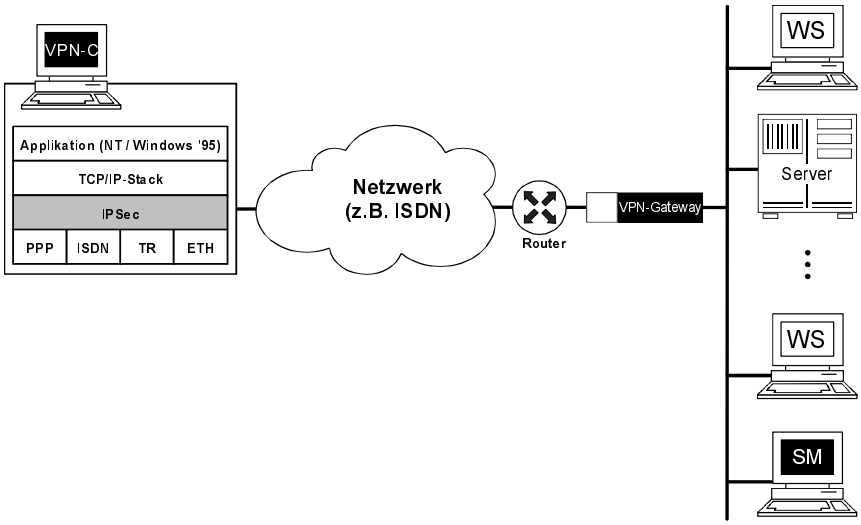


Abb. 5.11: Kopplung von Tele-Arbeitsplätzen

Mit Hilfe der Packet-Filter auf der zentralen Seite kann kontrolliert werden, auf welches Server-System und mit welchen Protokollen die Tele-Arbeitsplätze zugreifen dürfen. Außerdem kann genau festgelegt werden, zu welcher Zeit der Zugriff erlaubt wird.

VPN-Realisierungen

Hinsichtlich der Realisierung von VPNs existieren unterschiedliche Lösungsansätze. Einige Hersteller haben spezielle Sicherheitsprotokolle verwirklicht, die mit einem geschwindigkeitsoptimierten Ansatz arbeiten.

Vorteile eines solchen Ansatzes sind

- absolute Transparenz,
- sehr geringe Verzögerungszeiten in allen Phasen der Kommunikation,
- kein Overhead während der Kommunikation und
- keine Notwendigkeit irgendwelcher Reaktionen seitens der Komponenten, die in den einzelnen Netzen integriert sind.

Dieser Ansatz ist besonders bei echtzeitorientierten Anwendungen und bei Terminal-Anwendungen von besonderer Bedeutung.

5.2 Topologien von VPNs

Ein VPN fasst eine Menge von Netzwerk-Knoten zu einem Netzwerk zusammen, das durch krytographische Methoden vor dem Zugriff Außenstehender abgeschottet ist. Dabei spielt es keine Rolle, ob die Kommunikations-Strecken über öffentli-

che Netze (Telefon, Internet) geführt werden oder ob Teile eines internen LAN miteinander kommunizieren sollen. Abhängig davon, zwischen wie vielen Partnern die Verschlüsselung aufgebaut werden muss, kommen VPN-Strukturen 1:1, 1:n und m:n zur Anwendung.

Die Entscheidung, welche dieser Topologien zum Einsatz kommt, ergibt sich aus der Anforderungs-Analyse der über das Netzwerk abzuwickelnden Aufgaben und ihres Sicherheitsbedarfs. Da ein späterer Wechsel auf eine andere VPN-Topologie oft nur mit erheblichen Aufwand möglich ist, kommt dieser grundsätzlichen Auswahl eine besondere Bedeutung zu.

5.2.1 Die 1:1-Topologie

Bei dieser Topologie sind nur zwei Systeme an der Bildung eines VPN beteiligt. Zwischen ihnen wird die verschlüsselte Kommunikation abgewickelt, die von Unbefugten nicht abgehört werden kann. Fast immer handelt es sich bei diesen Systemen um VPN-Gateways, die verschiedene Standorte einer größeren Firma oder Institution miteinander verbinden. Will ein Rechner am Standort A über das VPN mit einem Rechner am Standort B kommunizieren, gelangen seine Netzwerkpakete zunächst unverschlüsselt über das lokale Netz A bis zum VPN-Gateway. Von dort gehen sie über den verschlüsselten und authentisierten Tunnel bis zum VPN-Gateway B auf der anderen Seite. Ab da bewegen sie sich wieder unverschlüsselt durch das Netz B zum Zielrechner. Da im Normalfall mehrere Rechner aus Netz A gleichzeitig mit Rechnern aus Netz B kommunizieren wollen, können über den VPN-Tunnel mehrere logische Kanäle geöffnet werden, die jeweils den einzelnen Kommunikations-Strecken zugeordnet sind. Bei den VPN-Gateways kann es sich um dezidierte Systeme oder auch um Firewall-Systeme oder Router handeln, bei denen eine zusätzliche VPN-Software installiert wurde. Abbildung 5.12 zeigt ein Beispiel.

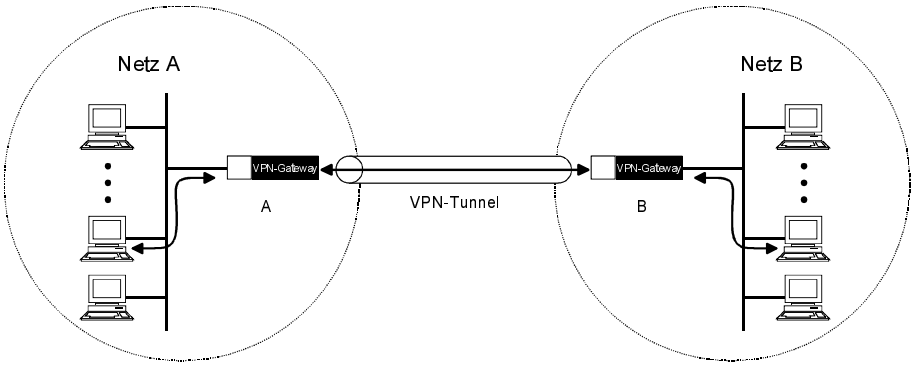


Abb. 5.12: VPN in der 1:1-Topologie

Charakteristisch für ein 1:1-VPN ist die starre Zuordnung der Tunnel zu den VPN-Gateways und ihren festen IP-Adressen. Deshalb wird auch die in Abbildung 5.13 angegebene Topologie aus drei gekoppelten Netzwerken als (in diesem Fall: dreifaches) 1:1-VPN bezeichnet. Es sind insgesamt drei Tunnel vorhanden, über die die Kommunikation zwischen den Standorten A, B und C abgewickelt wird.

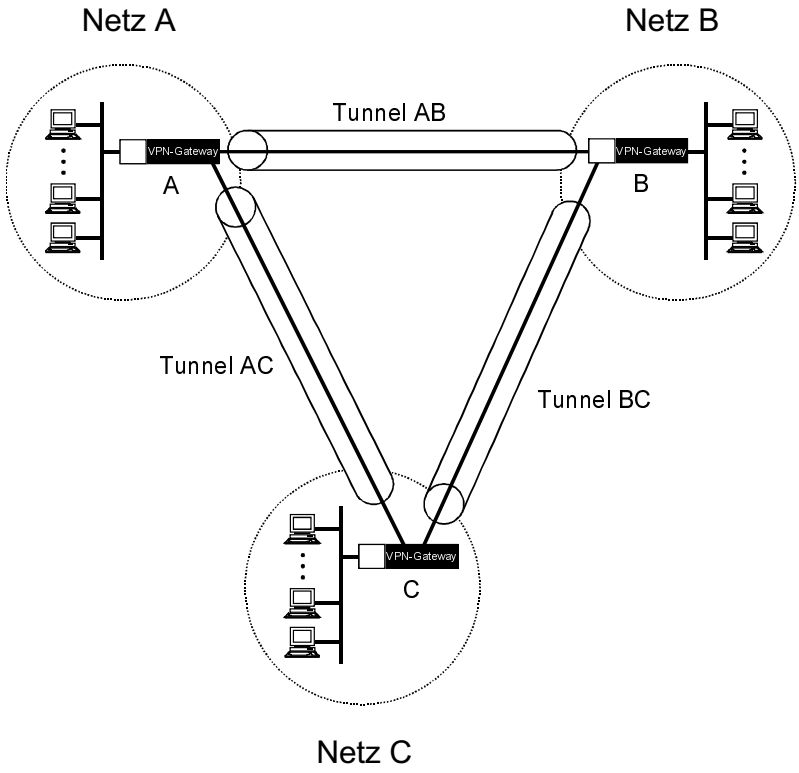


Abb. 5.13: Drei Standorte mit 1:1-Topologie

5.2.2 Die 1:n-Topologie

In vielen Fällen reicht die Zuordnung von VPN-Strecken zu festen Tunneln nicht aus. Geschäftsreisende wie zum Beispiel Außendienst-Mitarbeiter müssen sich von beliebigen Standorten aus über unterschiedliche Provider in das interne Netz einwählen können. Geschieht diese Kommunikation über ein öffentliches Netz wie das Internet, haben sie praktisch keinen Einfluss auf die ihnen vom Provider zur Verfügung gestellte Netzwerk-Adresse. Das VPN-Gateway auf der anderen Seite muss nach erfolgter Authentikation eine VPN-Strecke zu der jeweiligen (temporären) Adresse des Benutzers aufbauen. Hinter dem VPN-Gateway befindet sich wieder das firmeninterne Netz, über das die weitere Kommunikation mit dem Ziel-

rechner unverschlüsselt abgewickelt wird. Da die gesicherten Verbindungen jeweils vom VPN-Gateway zu den diversen Netzknoten reichen, trägt diese Topologie den Namen 1:n-VPN.

Im Gegensatz zu den sicheren Tunneln bei einem 1:1-VPN, über die jeweils mehrere Rechner durch unterschiedliche logische Kanäle miteinander kommunizieren können, besteht beim 1:n-VPN eine gesicherte Peer-to-Peer-Verbindung zwischen den Endknoten der Kommunikation. Abbildung 5.14 gibt ein Beispiel.

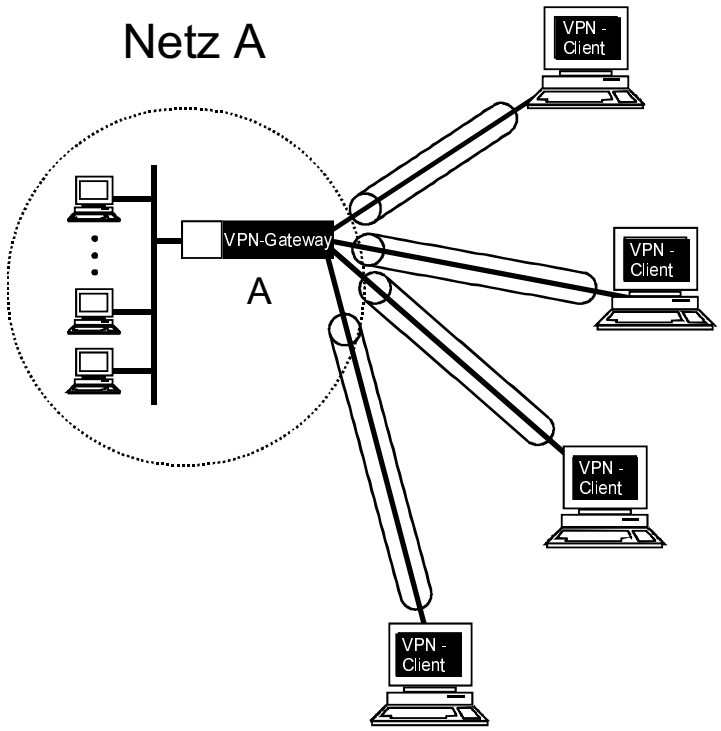


Abb. 5.14: VPN in der 1:n-Topologie

5.2.3 Die m:n-Topologie

Die beiden bisher beschriebenen Topologien decken die meisten VPN-Anwendungsfälle ab. Insbesondere die Kommunikation über das Internet lässt sich fast immer durch eine der beiden Varianten implementieren. Dennoch gibt es Anforderungen, bei denen eine mehr oder weniger willkürliche Gruppierung von Netzwerk-Knoten zu logischen Netzen mit erhöhtem Sicherheitsbedarf erforderlich ist.

So könnte es beispielsweise nötig sein, die über das gesamte Firmennetz verteilten Rechner einer Forschungs-Abteilung logisch vom Rest des Netzwerks abzukop-

peln, obwohl die Pakete physikalisch ganz oder teilweise über dieselben Leitungen gesendet werden. Auch die Zusammenstellung dezidierter Rechner aus verschiedenen physikalischen Netzwerken (beispielsweise Zulieferer und Endfertiger) zu einem »privaten« Netz ist denkbar. Bei einem solchen Konzept ist die beliebige Zusammenstellung der einzelnen Rechner zu einem oder mehreren VPNs möglich, was die Bezeichnung m:n-VPN erklärt (Abb. 5.15).

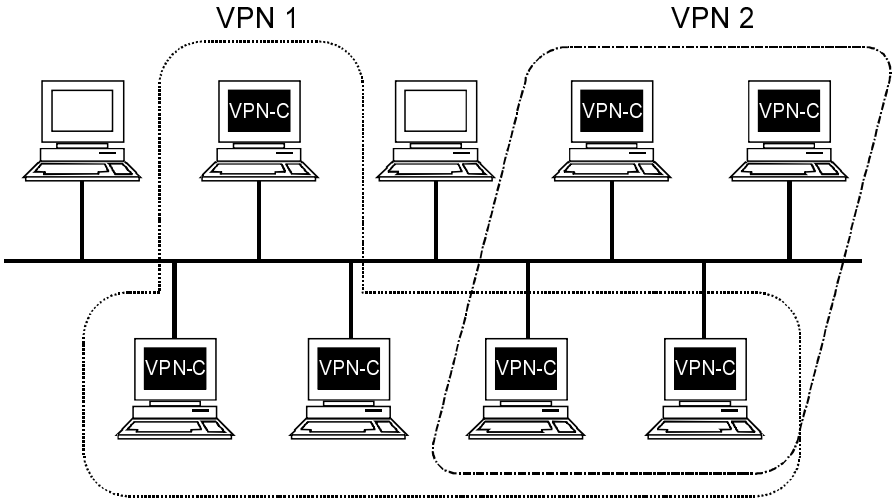


Abb. 5.15: VPN in der m:n-Topologie

Der organisatorische Aufwand zur Implementierung und Wartung der m:n-Topologie ist deutlich größer als bei den anderen Varianten, da sich durch die im Betrieb üblichen organisatorischen Maßnahmen die Zuordnung der einzelnen Rechner zu den VPNs häufiger als bei den anderen Topologien ändert und die VPN-Struktur tagesaktuell nachgezogen werden muss.

5.3 Sicherheitsmanagement für VPN-Systeme

Mit Hilfe eines Sicherheitsmanagements sollte eine einfache, zuverlässige und nachprüfbare Verwaltung eines VPN-Systems möglich sein.

5.3.1 Anforderungen an ein Sicherheitsmanagement

Das Sicherheitsmanagement muss selbst gegen Angriffe resistent sein, weil sonst Angreifer über das Sicherheitsmanagement die Sicherheitsfunktionen der VPN-Gateways und VPN-Clients ausschalten können. Dazu sollte das Sicherheitsmanagement selbst Sicherheitsmechanismen wie Identifikation und Authentikation,

Rollen-Verteilung, Protokollierung mit Audit-Möglichkeiten sowie Verschlüsselung der sicherheitsrelevanten Informationen im Sicherheitsmanagement bieten.

Ein Sicherheitsmanagement für VPN-Systeme soll mindestens die Voraussetzungen »Benutzerfreundlichkeit« und »Widerspruchsfreiheit von Regeln« erfüllen.

- Benutzerfreundlichkeit: Die Menüführung des Sicherheitsmanagements soll einfach und zuverlässig sein. Außerdem sollen keine redundanten Eingaben notwendig sein.
- Widerspruchsfreiheit der Regeln: Fehleingaben in den Eingabefeldern (zum Beispiel für IP-Adressen) sollten nicht möglich sein. Hier sollte eine syntaktische Überprüfung stattfinden.
- Filterregeln sollten nur für die entsprechende Protokollschicht einstellbar sein. Benutzer sollten beispielsweise nicht gleichzeitig als »aktiv« und als »gesperrt« für einen Dienst eingetragen werden können. Mehrfach-Einträge sollen eliminiert werden. Ferner sollte eine semantische Überprüfung der Filterregeln erfolgen.

Damit eine hohe Gesamtsicherheit des gesamten VPN-Systems gewährleistet werden kann, müssen zusätzlich die Sicherheitsfunktionen Zugangskontrolle, Rechteverwaltung, Verschlüsselung und Protokollierung zur Verfügung gestellt werden.

- Zugangskontrolle im Sicherheitsmanagement: Hier soll eine Identifikation und Authentikation der Benutzer durchgeführt werden, damit Unberechtigte das Sicherheitsmanagement nicht nutzen können.
- Rechteverwaltung (Rollen) im Sicherheitsmanagement: Um einen sicheren Betrieb des Sicherheitsmanagement zu gewährleisten, sollten möglichst die folgenden Rollen im Sicherheitsmanagement angeboten werden: Security Administrator, Operator, Editor, Observer und Auditor.
  - Der Security Administrator ist beispielsweise für die Personalisierung des Sicherheitsmanagements, die Vergabe der Zugriffsrechte für das Sicherheitsmanagementnd für das Erstellen und Wiedereinspielen von Backups verantwortlich.
  - Der Operator hat die Aufgabe, die Nutzungsrechte gemäß der Sicherheitspolitik seiner Organisation einzugeben.
  - Ein Editor ist für die Datenerfassung von nicht sicherheitskritischen Daten wie Benutzernamen, Rechnersystemen, Profilen etc. verantwortlich. Er kann keine Rechte vergeben oder entziehen.
  - Der Observer hat die Aufgabe, den Betrieb des VPN-Systems zu beobachten und gegebenenfalls Probleme zu analysieren. Er kann keine Rechte vergeben oder entziehen.
  - Der Auditor übernimmt die Aufgabe, die Logbuchdaten des Sicherheitsmanagement auf sicherheitskritische Aktionen zu überprüfen. Er kann keine Rechte vergeben oder entziehen.

Für besonders sicherheitskritische Aktionen im Sicherheitsmanagement kann ein Mehr-Augen-Prinzip verlangt werden, bei dem zwei oder mehr Personen nur gemeinsam, beispielsweise durch die Eingabe ihres Passworts, eine Aktion auslösen dürfen.

Die sicherheitsrelevanten Informationen, zum Beispiel Passworte oder Schlüssel für die Authentikation, sollten im Sicherheitsmanagement in verschlüsselter Form abgespeichert werden, damit kein Missbrauch dieser Informationen stattfinden kann.

Die verschiedenen Funktionen im Sicherheitsmanagement sollten in separaten Logbüchern protokolliert werden. Zu diesem Zweck sollte das Sicherheitsmanagement beispielsweise folgende Logbücher zur Verfügung stellen:

- Funktions-Logbuch: Hierin werden alle Aktionen festgehalten, die mit Hilfe des Sicherheitsmanagement durchgeführt werden, zum Beispiel die Vergabe der Rechte für die Benutzer, das Löschen von Logbüchern usw. In diesem Logbuch können die Handlungen der Benutzer des Sicherheitsmanagements (Security Administrator, Operator usw.) festgehalten werden.
- Login-Logbuch: Dort werden alle Logins in das Sicherheitsmanagement festgehalten.
- Fehler-Logbuch: Darin werden alle Fehler festgehalten, die im Sicherheitsmanagement erkannt werden.
- Backup-Logbuch: Es werden alle Backup-Aktionen festgehalten, die der Security Administrator im Sicherheitsmanagement durchführt.

Weitere Anforderungen

- Kopplung an ein Netzwerkmanagement-System (NMS):
  Die besonders hohe Verfügbarkeit von VPN-Systemen macht es in der Regel erforderlich, bestimmte »Spontane Meldungen« der VPN-Gateways oder VPN-Clients, die Auskunft über die Verfügbarkeit des Systems geben, an das Netzwerkmanagement zu senden, weil dieses in größeren Organisationen häufig eine 24-Stunden-Besetzung hat und bei Ausfällen schnell reagieren kann. Dazu sollte das Sicherheitsmanagement in der Lage sein, SNMP-Traps und einfache Get-Befehle mit Hilfe eines SNMP Proxy mit dem Netzwerkmanagement auszutauschen.

- Kommunikationsschutz für das Sicherheitsmanagement:
  In vielen Systemanordnungen ist es sinnvoll, das Sicherheitsmanagement mit Hilfe eines Firewall-Systems abzuschotten. Dies kann dann der Fall sein, wenn in den unterschiedlichen Organisationseinheiten lokale Security Manager tätig sind, die auf ein zentrales Sicherheitsmanagement zugreifen

5.3.2 Systeme zum Sicherheitsmanagement

Das Sicherheitsmanagement größerer VPNs wird in der Regel mit Hilfe von zentralen Software-Systemen durchgeführt. Kommerzielle Management-Systeme sind proprietäre Produkte einzelner Hersteller, der mit ihnen gebotene Komfort liefert starke Argumente für den Kauf eines bestimmten Systems.

Ein Management-System besteht im Allgemeinen aus drei Komponenten (Abb. 5.16):

- Der Management-Server ist ein dezidierter Rechner, dessen Kernstück eine Datenbank mit der gesamten Konfiguration des VPN ist. Er dient als zentrales Logging-System und bedient die externen Schnittstellen zu anderen Systemen, wie etwa einem Netzwerkmanagement-System.
- Die eigentliche Administration findet über ein grafisches Benutzer-Interface statt, das auf dem Management-Server oder den Arbeitsplatz-Rechnern der verschiedenen Administratoren laufen kann. Dieses Interface wird meist als Graphical User Interface (GUI) bezeichnet (Abb. 5.17)
- Die unterste Ebene in der Hierarchie wird durch die VPN-Gateways beziehungsweise VPN-Clients gebildet, die ihre Konfigurations-Daten vom Management-Server erhalten.

Die Kommunikation zwischen den einzelnen Komponenten verlangt ein Höchstmaß an Sicherheit, so dass starke Verfahren zu Authentikation und Verschlüsselung zum Einsatz kommen. Bei VPN-Clients, die in der Regel offline sind (zum Beispiel Desktops, Notebooks), ist eine automatische Konfiguration über den Management-Sever nicht möglich. Änderungen der Konfiguration müssen manuell übertragen beziehungsweise eine automatische Re-Konfiguration manuell gestartet werden.

Firewall-Systeme mit intergriertem VPN bieten ein gemeinsames Sicherheitsmanagement beider Komponenten. Die VPN-Strecke erscheint dann sehr übersichtlich als »Filterregel« in der Firewall-Konfiguration.

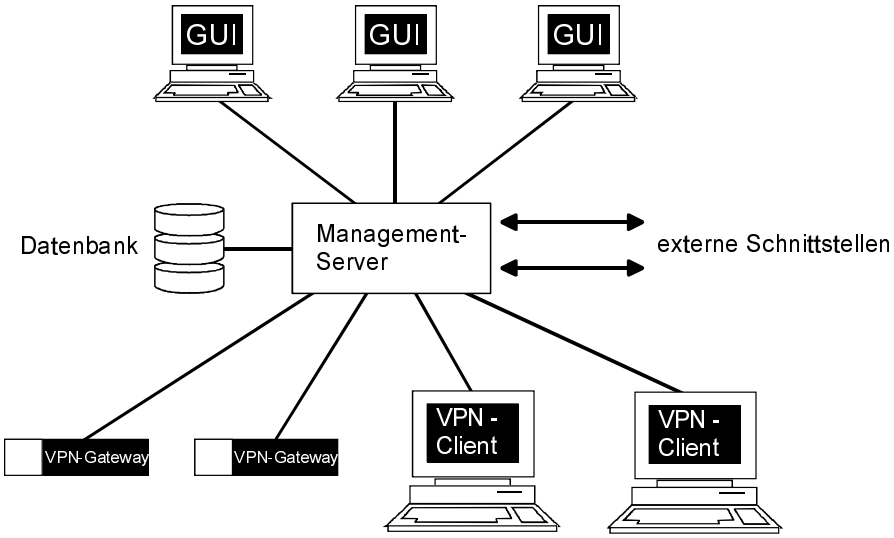


Abb. 5.16: Sicherheitsmanagement

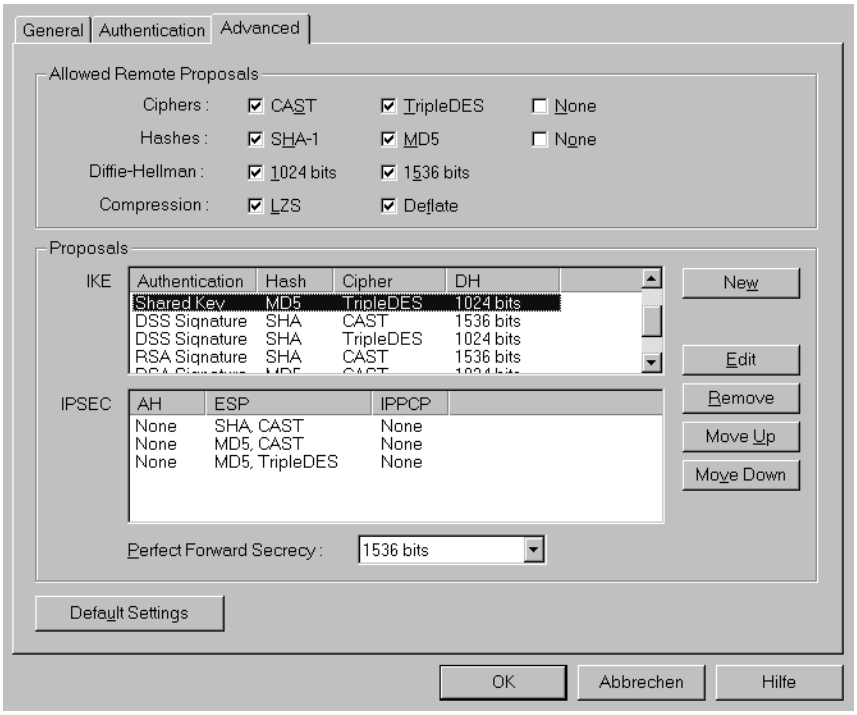


Abb. 5.17: Konfiguration eines VPN

5.3.3 Zertifizierungs-Systeme

Ein zentrales Element von VPN-Systemen ist die gegenseitige Authentikation. Damit belegt jeder Teilnehmer, dass er tatsächlich der angegebene Kommunikationspartner ist. Nur bei kleinen VPNs ist es möglich, die mit der Authentikation verbundenen Aufgaben manuell zu lösen. Eine automatische Authentikation bedarf einer Infrastruktur, die in der Praxis durch die in Kapitel 4 beschriebenen Zertifizierungs-Systeme geschaffen wird. Da Zertifikate neben dem Nachweis der Authentizität durch eine digitale Signatur auch kryptographische Verfahren und die dazu benötigten Schlüssel enthalten, sind die zu ihrer Verwaltung implementierten Systeme hochkomplexe und von der Administration her oft gewöhnungsbedürftige Produkte.

Ein Zertifizierungs-System enthält folgende Komponenten:

- Mit einem PKI-Editor (Public Key Infrastructure) wird die in Kapitel 4 angesprochene hierarchische Struktur aus Certification Authorities (CA) und Registration Authorities (RA) definiert.
- Mit dem Policy-Editor wird für einen Typ von Zertifikaten verbindlich festgelegt, wie der Nachweis der Identität erfolgt, welche kryptographischen Algorithmen benutzt werden und wie die Gültigkeit des Zertifikates geregelt werden soll.
- Grafische Frontends (GUIs) stellen die Schnittstelle für die Personen dar, die innerhalb der CAs und RAs mit der Erstellung und Administration der Zertifikate betraut sind.

In komplexen Zertifizierungs-Systemen findet eine Arbeitsteilung zwischen den Institutionen CA, RA sowie den dort arbeitenden Personengruppen CA-Operatoren (CAO) und RA-Operatoren (RAO) statt. Die Beziehungen zwischen diesen sind wie folgt definiert (Beispiel Abb. 5.18):

- Die Aufgabe einer Certification Authority CA ist die Bearbeitung von Anfragen der RA nach Zertifikaten, die innerhalb der CA erstellt, in einer Datenbank abgespeichert und schließlich ausgeliefert werden.
- Ein CAO definiert die ihm zugeordneten RA und RAO, definiert die für die verschiedenen Typen von Zertifikaten benötigten Policies, leitet diese an seine RAs weiter und ruft Zertifikate zurück, die vorzeitig aus dem Verkehr gezogen werden müssen.
- Innerhalb der RA werden die (Benutzer-)Anfragen nach Zertifikaten angenommen und an die zugeordnete CA weitergeleitet.
- Ein RAO setzt die vom CAO definierte Policy um, das heißt, er kontrolliert die Authentizität der Personen oder Systeme, die ein Zertifikat erhalten sollen, signiert die Anfrage und sendet sie an seine CA weiter.

PKI-Editor

Der erste Schritt bei der Erstellung einer Zertifizierungs-Infrastruktur ist die Definition der beteiligten Instanzen und ihrer Abhängigkeiten. Dabei wird ein grundsätzlicher Rahmen für die Erstellung von Zertifikaten definiert, der Algorithmen, Verfahren zum Schlüsselaustausch, Regelungen für die Gültigkeitsdauer von Zertifikaten und Mechanismen zum vorzeitigen Zurückziehen von Zertifikaten über Sperrlisten (Certification Revocation List, CRL) enthält.

Da bei der Erstellung der Infrastruktur eine Fülle von Aufgaben zu bewältigen ist, wurden Software-Systeme entwickelt, die Unterstützung leisten können. Abbildung 5.18 zeigt einen PKI-Editor mit grafischer Benutzeroberfläche.

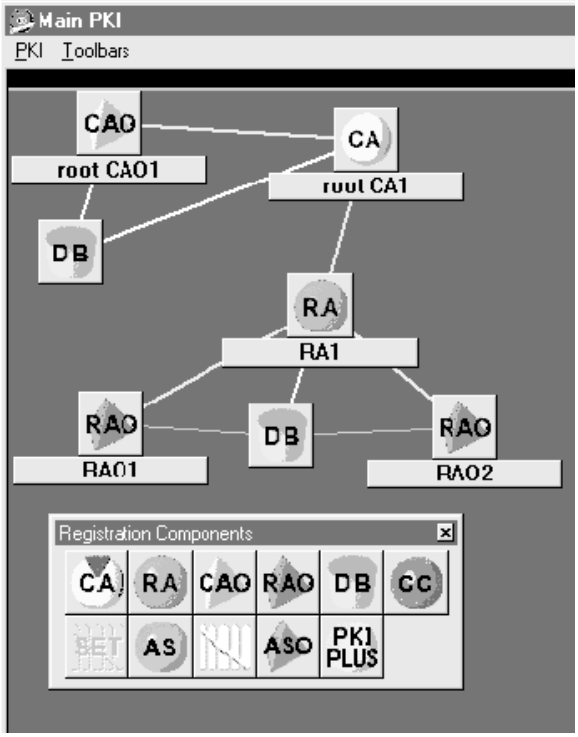


Abb. 5.18: PKI-Editor

Anschließend werden die so definierten CAs, CAOs, RAs und RAOs konfiguriert. Abbildung 5.19 gibt ein Beispiel.

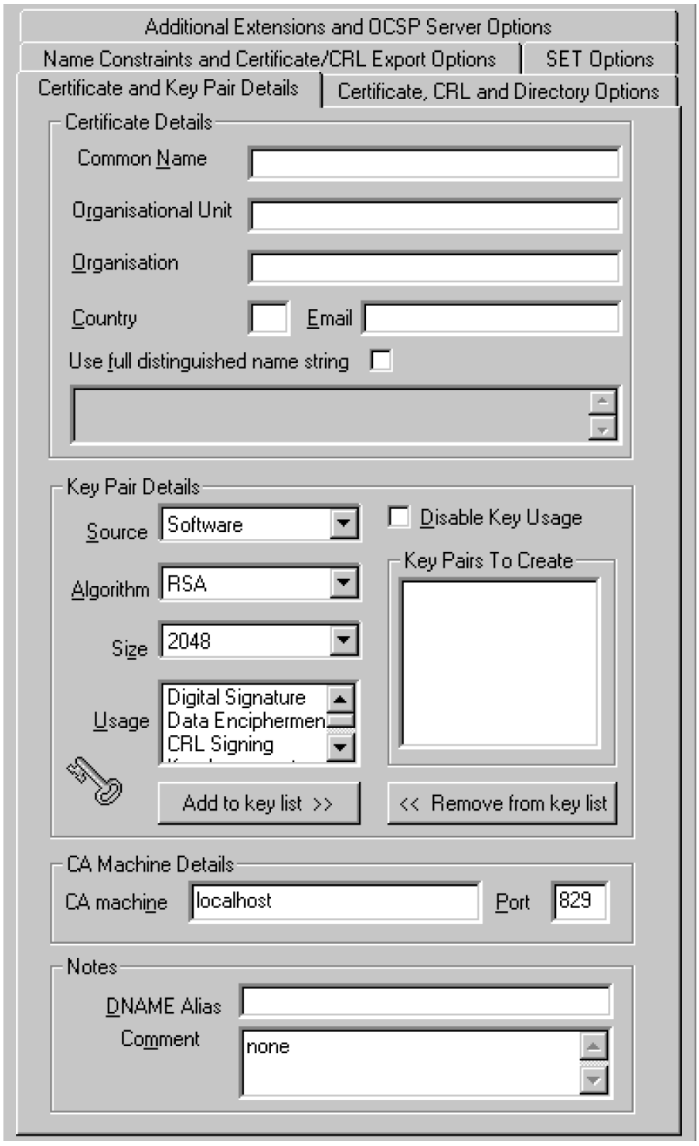


Abb. 5.19: Konfiguration einer CA

Policy-Editor

Mit diesem Tool werden die Mechanismen festgelegt, nach denen der Antrag für ein Zertifikat bearbeitet wird. Abhängig von der Sicherheits-Klasse des Zertifikats sind dabei bestimmte Anforderungen zu erfüllen. Mit der Definition einer Policy werden die bei der Definition der PKI festgelegten Rahmenbedingungen für Verfahren usw. »mit Leben erfüllt«. Auch hier existieren grafische Oberflächen (Abb. 5.20). Der CAO legt hier wie auf einem Formblatt die Randbedingungen für die Ausstellung von Zertifikaten fest.

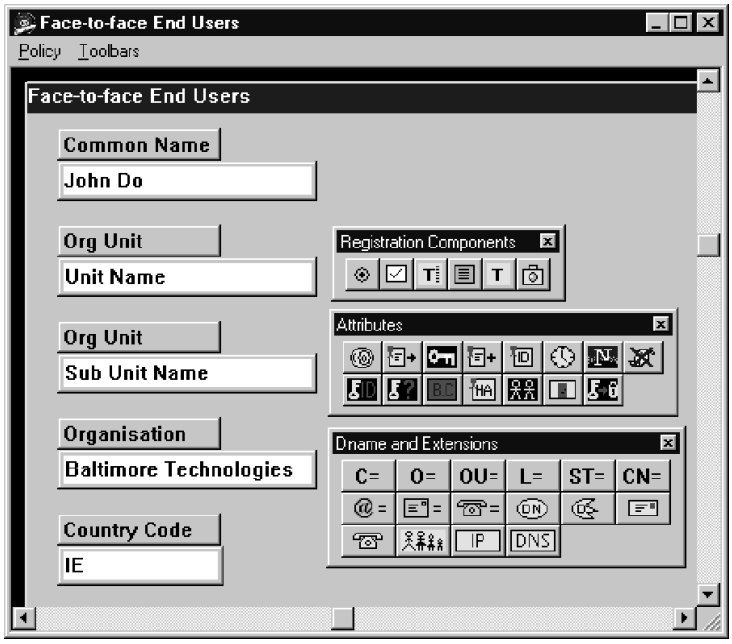


Abb. 5.20: Policy-Editor

5.3.4 Directory-Service

Innerhalb einer VPN-Infrastruktur spielt der schnelle Zugriff auf Sicherheitsinformationen eine entscheidende Rolle. Da die Verhandlungen der an der Kommunikation beteiligten Partner online ablaufen, muss auch der Zugriff auf Zertifikate und Listen mit abgelaufenen Zertifikaten mit einer adäquaten Geschwindigkeit erfolgen. Bei kleinen VPNs können Änderungen manuell auf die einzelnen Komponenten übertragen werden. In den meisten Fällen muss ein Verzeichnis-Dienst (Directory-Service) eingerichtet werden, der die automatische Verteilung von Informationen und den Zugriff darauf regelt.

Ein VPN-Verzeichnis-Dienst ist im Grunde nichts anderes als eine Datenbank, in der Informationen über Zertifikate und die in diesen abgelegten öffentlichen Schlüsseln verwaltet werden. Der Zugriff auf die Datenbank geschieht über die Angabe von Namen, IP-Adressen oder anderen eindeutigen Kriterien. Verzeichnis-Dienste sind meist hierarchisch aufgebaut, so dass die Verbreitung der Informationen (Replikation) innerhalb der Hierarchie transparent und effizient erfolgt. Die Software der VPN-Gateways oder VPN-Clients greift beim Aufbau einer neuen Verbindung auf den Verzeichnis-Dienst zu, falls die gewünschten Informationen nicht lokal verfügbar sind. Moderne VPN-Management-Systeme verfügen über eine Verzeichnis-Schnittstelle nach der LDAP-Spezifikation. Die anfallenden Konfigurations-Arbeiten können dann wahlweise auf dem LDAP-Server oder innerhalb des VPN-Management-Systems durchgeführt werden.

Zur Konfiguration und Administration eines Verzeichnis-Dienstes existieren grafisch orientierte Tools, die den Administratoren die Arbeit erleichtern (Abb. 5.21).

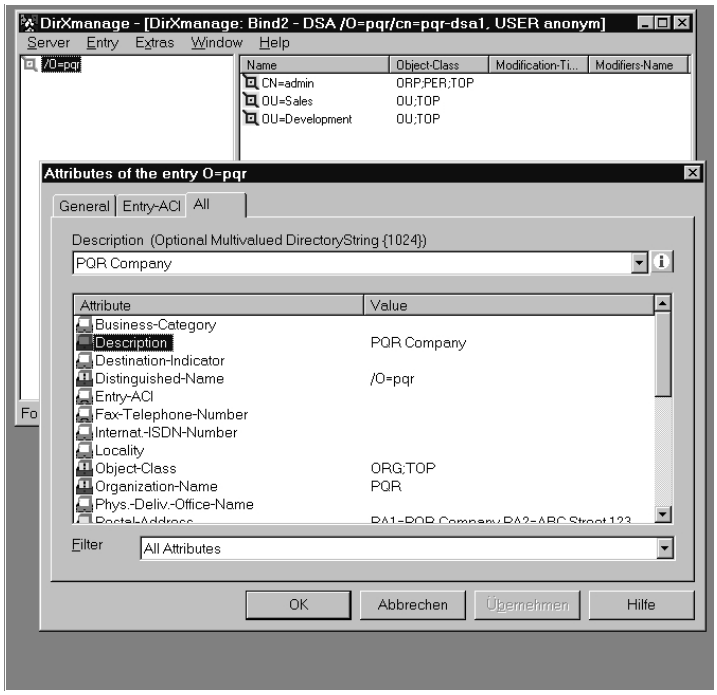


Abb. 5.21: Konfiguration eines Verzeichnis-Dienstes

5.3.5 Schlüssel-Management

VPNs nutzen die hybride Verschlüsselungstechnik: Für die Übertragung der Nutzdaten wird symmetrische Verschlüsselung genutzt, für die Übertragung des symmetrischen Schlüssels hingegen asymmetrische Verschlüsselung. Während die symmetrischen Schlüssel meist von Zufallsgeneratoren erzeugt werden, müssen die für die asymmetrische Verschlüsselung benutzten Paare aus privaten und öffentlichen Schlüsseln vor Beginn der Kommunikation bereit stehen. Dabei muss von der eingesetzten Infrastruktur sowohl die Geheimhaltung des privaten Schlüssels als auch die Authentizität des öffentlichen Schlüssels garantiert werden.

Kommt ein Zertifizierungs-System mit Verzeichnis-Dienst (z. B. LDAP) zum Einsatz, wird das Management der Schlüssel über diesen vorgenommen. Von der CA gelangt der private Schlüssel abgesichert zum Empfänger, oft wird er auch direkt beim Empfänger erzeugt. Die Echtheit des öffentlichen Schlüssels wird über ein Zertifikat oder eine Kette von Zertifikaten nachgewiesen. Sollen Schlüsselpaare zurückgezogen werden, wird das dazugehörige Zertifikat in die Certification Revocation List (CRL) eingetragen. Die Veröffentlichung neuer Schlüssel beziehungsweise Zertifikate geschieht über einen Verzeichnis-Dienst, ebenso wie die Bekanntgabe ungültiger Schlüssel.

Der Einsatz eines kompletten Zertifizierungs-Systems ist allerdings keine notwendige Bedingung zum Betrieb eines VPN. Im Extremfall können die öffentlichen Schlüssel manuell auf die an der Kommunikation beteiligten Systeme gebracht werden. Bei größeren VPNs scheidet diese Variante allerdings wegen des hohen administrativen Aufwands aus. Als Mittelweg zwischen manuellem Schlüsselaustausch und Zertifizierungs-System kann der Einsatz eines Key-Servers angesehen werden, auf den die öffentlichen Schlüssel nach ihrer Erstellung kopiert werden. Von diesem Rechner beziehen dann alle am VPN beteiligten Knoten die benötigten öffentlichen Schlüssel, der Einsatz eines komplexen Verzeichnis-Dienstes erübrigt sich.

Sind an der Bildung eines VPNs nur wenige Knoten beteiligt (z. B. 1:1-Topologie mit drei Standorten), ist der manuelle Schlüsselaustausch die geeignete Methode. Sind aber remote Benutzer (1:n-Topologie) zu versorgen oder ist in der nächsten Zeit mit einem Wachstum der am VPN beteiligten Rechner zu erwarten, sollte konsequent auf einen LDAP Verzeichnis-Dienst gesetzt werden. Für große VPNs stellt sich die Frage nach dem Verzeichnis-Dienst nicht, dieser wird außer für das VPN auch für die Administration von Firewalls oder Authentikations-Systemen benötigt.

Kapitel 6

VPN-Verfahren

Um die drei Ziele einer vertrauenswürdigen Daten-Übertragung – Vertraulichkeit, Authentikation und Integrität – mit einem VPN zu realisieren, müssen eine Reihe von Überlegungen durchgeführt werden. Dieses Kapitel hilft bei der Auswahl von Protokollen, die den gesicherten Transport von Daten und den Austausch der Schlüssel durchführen. Mit dem Protokoll IPSec wurde ein in die Zukunft weisender Standard geschaffen, doch die Eignung von IPSec für eine große Anzahl von Algorithmen macht eine sorgfältige Recherche der Fähigkeiten von VPN-Produkten vor dem Kauf erforderlich. Sonst sind bei IPSec-fähigen Produkten unterschiedlicher Hersteller Probleme vorprogrammiert. Insbesondere beim (automatischen) Austausch geheimer Schlüssel kann IPSec mit sehr unterschiedlichen Verfahren kombiniert werden.

Neben IPSec sind noch eine ganze Reihe anderer Verfahren innerhalb von VPNs implementiert. Microsoft ist mit seinen Produkten erst ab Windows 2000 auf den IPSec Standard umgestiegen – genauer gesagt: hat sich dem IPSec-Standard angenähert, aber eigentlich eine proprietäre Lösung geschaffen – und zahllose VPN-Realisierungen nutzen noch das alte PPTP-Protokoll, trotz seiner Unzulänglichkeiten und Risiken. In der Unix-Welt, wo IPSec in modernen Implementierungen der Standard ist, wurden ältere VPNs häufig mit dem Protokoll Secure Shell (SSH) realisiert. Die Zukunft gehört aber IPSec mit dem Schlüsselaustausch über IKE (Internet Key Exchange), so dass moderne VPN-Implementierungen IPSec und IKE in jedem Falle zur Verfügung stellen müssen.

6.1 VPN-Protokolle

6.1.1 IPSec

Die Grundideen des VPN-Standardprotokolls IPSec wurden im Zusammenhang mit dem neuen Internet-Protokoll IPv6 entwickelt. IPSec wurde von der Internet Engineering Task Force (IETF) definiert. Im Gegensatz zur bisherigen IP-Version 4 können hier optionale zusätzliche Header angegeben werden, mit denen eine erweiterte Funktionalität auf Protokollebene realisiert werden kann.

Zwei dieser Header wurden zu Zwecken der Authentikation und Verschlüsselung definiert. Ihre Namen sind »Authentication Header« (AH) und »Encapsulated Security Payload« (ESP). IPSec kann aber ebenso in Netzwerken nach dem bishe-

rigen IPv4-Standard implementiert werden. Statt der zusätzlichen Header findet dann eine Erweiterung des normalen IP-Header statt. In diesem Fall sind AH und ESP Datenstrukturen innerhalb des Headers. Da die Absicherung der Kommunikation mit IPSec auf IP-Ebene stattfindet, stehen die zusätzlichen Datenstrukturen zwischen dem IP-Header und dem Header für die nächsthöhere Netzwerk-Ebene (TCP oder UDP). AH und ESP können einzeln oder auch gemeinsam eingesetzt werden, wobei dann innerhalb des Netzwerkpakets der AH-Header vor dem ESP-Header stehen muss. Die beiden Header selbst enthalten keine Informationen über die zur Absicherung eingesetzten Algorithmen und Schlüssellängen, sondern nur einen Verweis (Security Parameter Index, SPI) auf eine Datenstruktur mit diesen Informationen (Security Association, SA).

Mit der AH-Datenstruktur kann gewährleistet werden, dass eine eventuelle Manipulation von Daten auf dem Weg durch das Netzwerk entdeckt wird. Außerdem findet die Authentikation des Absenders der Pakete statt. Beim ausschließlichen Einsatz des AH-Headers findet keine Verschlüsselung über IPSec statt. Vertraulichkeit kann dann nur über eine Verschlüsselung außerhalb des IPSec-Protokolls ermöglicht werden.

Mit Hilfe von ESP können Vertraulichkeit der Übertragung, Authentikation des Absenders und Integrität der Daten garantiert werden, da neben der Verschlüsselung auch ähnliche Mechanismen wie in AH definiert werden können. Im Unterschied zu ESP bezieht sich die Authentikation von AH auch auf den IP-Header, so dass die Kombination von AH und ESP Vorteile im Sicherheitsbereich bietet, allerdings mehr Ressourcen auf den beteiligten Rechnern benötigt.

Kryptographische Verfahren in IPSec

IPSec ist von seinem Ansatz her flexibel und zur Zusammenarbeit mit praktisch jedem kryptographischen Verfahren bereit. In der Praxis haben sich allerdings bestimmte de-facto-Standards herausgebildet, die von den meisten IPSec-Implementierungen unterstützt werden:

- Verschlüsselungsalgorithmus: DES im CBC-Modus, Triple-DES im CBC-Modus, AES
- Hash-Algorithmus: SHA-1 oder MD5, jeweils mit HMAC
- Authentikation: durch RSA-Signaturen mit X.509-Zertifikaten, RSA ohne Zertifikate (öffentliche Schlüssel wurden zuvor ausgetauscht) oder durch Pre-Shared Keys
- Austausch von Session-Keys: mittels Diffie-Hellman

Transport- und Tunnelmodus

IPSec kann im Transport- oder im Tunnelmodus betrieben werden. Im Transportmodus wird der IP-Header des ungesicherten IP-Pakets übernommen und nur sein Datenteil verändert. Bis auf das Feld »Länge des IP-Paketes« und die Prüf-

summe bleibt der alte IP-Header unverändert. Im Tunnelmodus hingegen wird das gesamte IP-Paket in die Nutzdaten des IPSec-Pakets übernommen, so dass die alte IP-Adresse nicht mehr notwendigerweise sichtbar sein muss. Bei 1:1-VPNs, die beispielsweise zwischen zwei Firewall-Systemen eingerichtet werden, wird der Tunnelmodus genutzt. Damit bleiben die echten IP-Adressen der Kommunikations-Partner einem Angreifer verborgen. Bei 1:n- oder m:n-VPNs kommt in der Regel der Transportmodus zum Einsatz. In den Abbildungen 6.1 und 6.2 werden die beiden Modi jeweils für die Versionen IPv4 und IPv6 am Beispiel eines TCP-Paketes dargestellt.

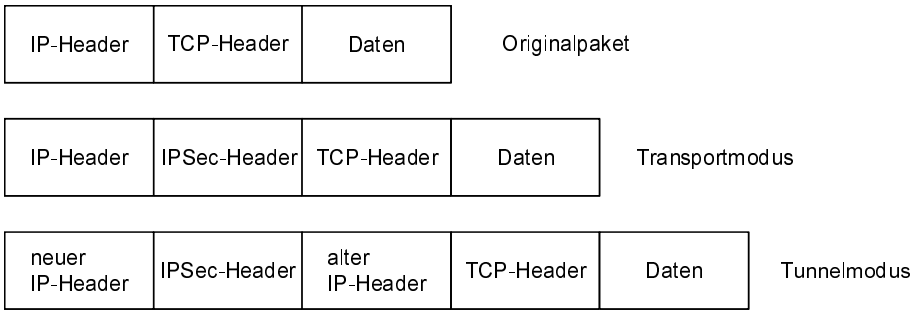


Abb. 6.1: IPSec-Modi bei IPv4

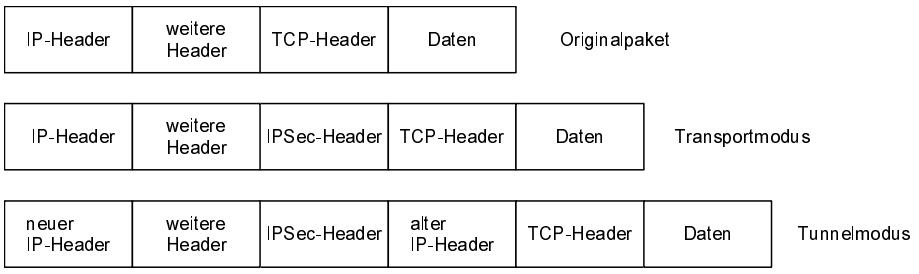


Abb. 6.2: IPSec-Modi bei IPv6

Security Association (SA)

Die Security Associations (SAs) können anschaulich als Definitionen von Filtern verstanden werden, durch die die IP-Pakete beim Versand beziehungsweise beim Empfang geleitet werden. Die Zuordnung zwischen Paket und SA erfolgt über den Pointer »Security Parameter Index« (SPI). Abgehende Pakete werden mit den gewünschten Authentikations- beziehungsweise Verschlüsselungsalgorithmen abgesichert, ankommende Pakete wieder in den allgemein lesbaren Zustand (ohne AH und ESP) gebracht. Werden ESP und AH kombiniert, müssen auch zwei SAs

angegeben werden. Alle SAs eines Rechners werden in einer Datenbank abgelegt, die »Security Associations Database« (SAD) genannt wird. SAs für ankommende und abgehende Pakete sind wegen der zumeist eingesetzten asymmetrischen Verfahren stets getrennt anzugeben. Beim Aufbau einer IPSec-Verbindung werden die SAs zwischen den beiden Partnern ausgehandelt und in der SAD abgelegt (Abb. 6.3). Dabei hat jeder Rechner intern eine Sammlung von möglichen Parametern als Anforderungs-Policies abgelegt, die er mit denen des Partners abgleicht und woraus er die Parameter mit der höchstmöglichen (vordefinierten) Priorität wählt.

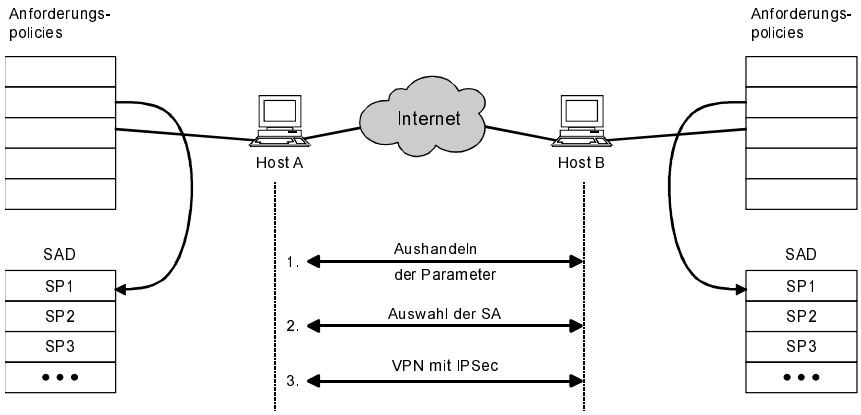


Abb. 6.3: Aushandeln von Security Associations

Jede SA besteht aus einer Datenstruktur, in der die Adresse des Kommunikationspartners, die ausgehandelten Verfahren zur Verschlüsselung, Authentikation, Hashwert-Bildung, die bei der Verschlüsselung beziehungsweise Authentikation eingesetzten kurzlebigen Session-Keys sowie die Gültigkeitsdauer der SA angegeben werden. Ein Beispiel für eine AH-SA zeigt Tabelle 6.1.

IP-Adresse des Partners	205.48.34.263
Security Parameter Index	7B750AC6
Filter-Transformation	AH, MD5 mit HMAC
Session-Key (hier für HMAC)	73DA6710BC651801
weitere SA-Attribute (z. B. Gültigkeitsdauer)	5 Minuten oder 100 KByte

Tabelle 6.1: Beispiel für eine Security Association

Die »Security Policy Database« (SPD) ist eine Sammlung von Regeln, ähnlich denen von Paketfiltern. Für alle Klassen von ankommenden und abgehenden Paketen muss angegeben werden, ob die Pakete mittels IPSec behandelt sind

beziehungsweise behandelt werden müssen (Verweis auf eine SA in der SAD), ob es sich um IP ohne IPSec handelt oder ob die Pakete verworfen werden müssen. Die Einträge in der SPD müssen geordnet sein, da der erste auf das Paket passende Eintrag verwendet wird. Alle im Regelwerk nicht explizit behandelten Pakete werden verworfen.

Der AH-Header

Der AH-Header sichert das gesamte IP-Paket mittels eines MAC ab, einschließlich der unveränderlichen Header-Daten. Flaggen, die sich auf dem Weg des Pakets durch das Internet ändern können, sind vom Schutz durch AH ausgenommen. Abbildung 6.4 zeigt den Einbau des AH-Headers in IP-Pakete am Beispiel eines TCP-Pakets im IPv4-Standard, die Struktur des AH-Headers selbst kann der Abbildung 6.5 entnommen werden.

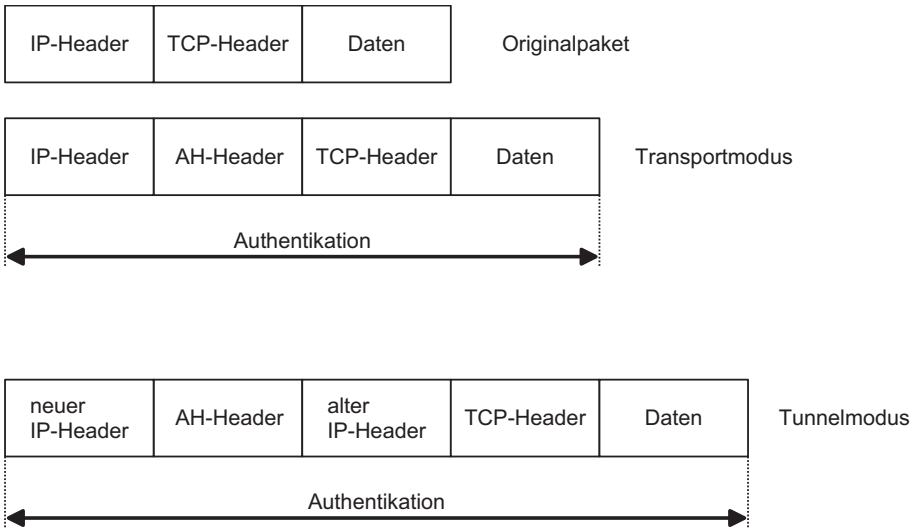


Abb. 6.4: AH-Header im Transport- und Tunnelmodus (IPv4)

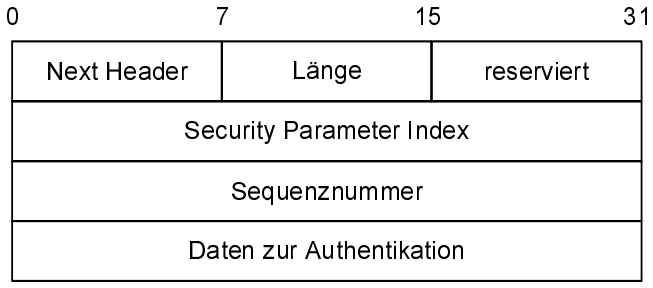


Abb. 6.5: Struktur des AH-Headers

Dabei bedeuten die einzelnen Felder:

- »Next Header« (8 Bit) gibt den Typ der Daten an, die hinter dem AH-Header folgen.
- Die Länge (8 Bit) gibt die Gesamtlänge des AH-Headers an.
- Der reservierte Bereich (16 Bit) ist bis zu einer späteren Verwendung stets zu 0 zu setzen.
- Der Security Parameter Index (SPI, 32 Bit) ist zusammen mit der IP-Zieladresse und der Tatsache der AH-Authentikation ein eindeutiger Verweis auf die für dieses Paket verwendete Security Association (SA).
- Die Sequenznummer (32 Bit) ist ein Zähler, mit dem Replay-Angriffe (böswillige Wiederholung von Paketen) erkannt werden können. Sie wird mit jedem gesendeten Paket um eins erhöht. Die Auswertung der Sequenznummer ist optional und wird in der dazugehörigen SA angegeben.
- Die Authentikationsdaten AD (32 Bit) schließlich enthalten einen verschlüsselten Hashwert oder ähnliches, um die Integrität der Daten überprüfen zu können.

Der AH-Header hat den IP-Protokolltyp 51.

Der ESP-Frame

Mittels des ESP-Frames wird der gesamte auf ESP folgende Teil des Pakets verschlüsselt und authentisiert, unter IPv6 einschließlich etwaiger nachfolgender Header. Die Authentikation über ESP bezieht sich allerdings nur auf den Bereich zwischen dem ESP-Header und dem am Ende des Pakets stehenden ESP-Trailer, wie Abbildung 6.6 am Beispiel eines TCP-Paketes zeigt. Die Struktur des ESP-Frames (Header, Nutzdaten, Trailer) ist in Abbildung 6.7 angegeben.

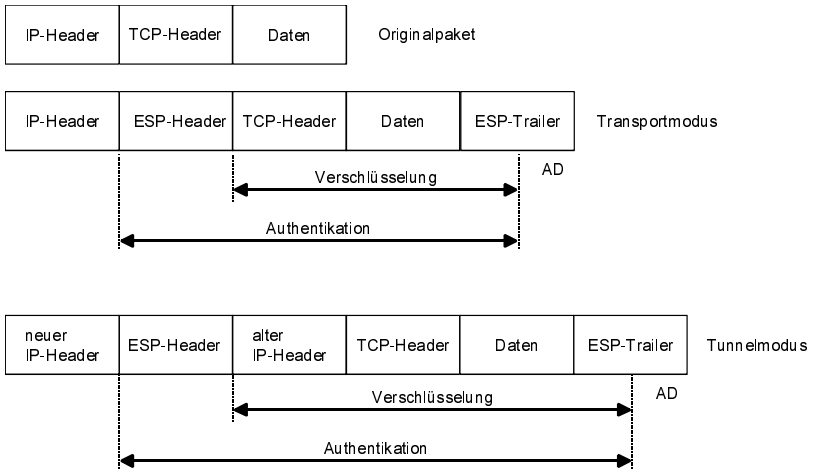


Abb. 6.6: ESP-Header im Transport- und Tunnelmodus (IPv4)

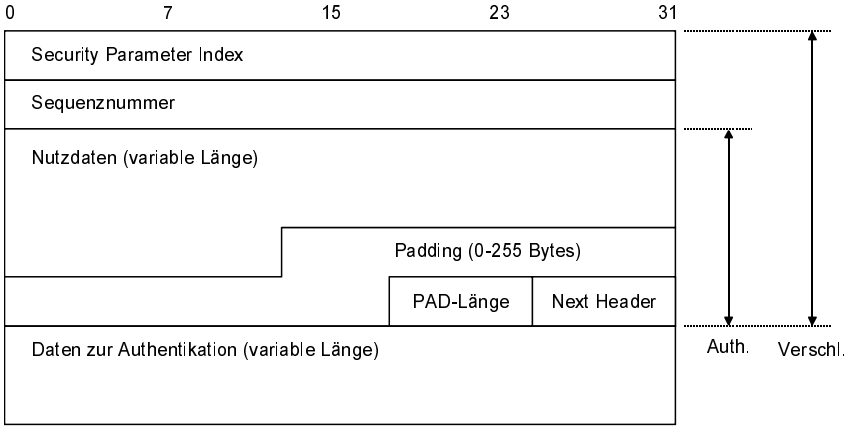


Abb. 6.7: Struktur des ESP-Frames

Dabei haben die einzelnen Felder die folgenden Bedeutungen:

- Der Security Parameter Index (SPI, 32 Bit) hat dieselbe Bedeutung wie beim AH-Header.
- Die Sequenznummer (32 Bit) hat dieselbe Bedeutung wie beim AH-Header.
- Die Nutzdaten (TCP/UDP-Header, Applikationsdaten) können bei Bedarf um etwaige Initialisierungsvektoren für die Entschlüsselung erweitert werden.
- Die Padding-Daten füllen die Nutzdaten bei Bedarf auf, wenn zum Beispiel ein Entschlüsselungsalgorithmus eine feste Blocklänge verlangt.
- Die PAD-Länge gibt die Länge der Padding-Daten an.
- Im Next-Header-Feld ist (wie beim AH-Header) vermerkt, von welchem Typ die Nutzdaten sind.
- Die Authentikationsdaten (AD) haben – im Gegensatz zum AH-Header – eine variable Länge. Die Länge dieses Felds ist implizit durch den verwendeten Algorithmus vorgegeben, der in der zugehörigen SA vermerkt ist.

Der ESP-Header hat den IP-Protokolltyp 50.

Werden AH und ESP kombiniert, so ergibt sich die in Abbildung 6.8 angegebene Paketstruktur.

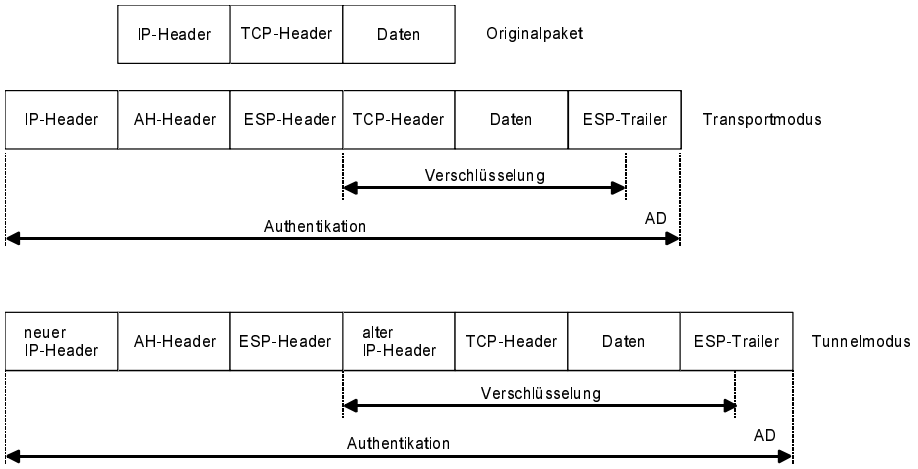


Abb. 6.8: AH/ESP-Header im Transport- und Tunnelmodus (IPv4)

Verarbeitung von abgehenden Netzwerkpaketen

Soll eine Netzwerkverbindung unter IPSec aufgebaut werden, wird zunächst in der Security Policy Database (SPD) nachgeforscht, wie die dazugehörigen Pakete zu verarbeiten sind. Als Suchkriterien dienen dabei die gewünschte Verarbeitung (AH, ESP oder beides), die Ziel-IP-Adresse sowie der Security Parameter Index (SPI). Wird in der Datenbank eine passende Security Association (SA) gefunden, findet mit Hilfe dieses Filters der Umbau des Pakets gemäß dem IPSec-Standard statt. In bestimmten Fällen (beispielsweise AH und ESP) kann auch ein Set von SAs gefunden und angewandt werden.

Falls noch keine passende SA im Zugriff ist, muss diese ermittelt und in der Datenbank abgelegt werden. Dazu müssen unter Umständen Verhandlungen mit anderen Rechnern vorgenommen, Schlüssel ausgetauscht und Algorithmen festgelegt werden. Am Ende dieser Operationen liegt bei beiden Partnern die passende SA (beziehungsweise ein Set von SAs) vor. Von diesem Punkt an werden die Netzwerkpakete umgewandelt wie in der SA beschrieben.

Verarbeitung von ankommenden Netzwerkpaketen

Ankommende IP-Fragmente von Netzwerkpaketen werden zunächst zusammengesetzt. Dann wird, ebenso wie bei abgehenden Verbindungen, zunächst nach einer passenden SA gesucht. Wird keine gefunden, wird das Paket verworfen und ein Eintrag in eine Fehler-Logdatei vorgenommen.

Wird eine SA oder ein Set von SAs gefunden, wird das Paket durch die damit definierten Filter geschleust und erhält seine ursprüngliche Form zurück. Dann findet nochmals ein Vergleich mit der Security Policy Database (SPD) statt, ob das Paket gemäß seinen dort festgelegten Spezifikationen korrekt verarbeitet wurde. Anschließend wird das Paket dem normalen Netzwerkstack zur Verfügung gestellt. Handelt es sich beim Empfänger um ein VPN-Gateway oder ein Firewall-System und befindet sich das Paket im Tunnelmodus, wird es an den endgültigen Empfänger weitergesendet.

6.1.2 Point-to-Point Tunneling Protocol (PPTP)

Bei der Implementierung von VPNs in der »Microsoft-Welt« hat das als veraltert geltende PPTP noch immer einen großen Stellenwert, ist es doch das einzige Protokoll, das von Microsoft vor der Einführung von Windows 2000 offiziell unterstützt wurde. PPTP ist eine Erweiterung des älteren »Point-to-Point Protocol« (PPP), mit der ein Tunneln von PPP-Paketen über IP-Netze wie das Internet möglich wird. Dabei werden bezüglich Authentikation und Verschlüsselung keine neuen Verfahren definiert, da PPP beziehungsweise seine Erweiterungen selbst schon diese Punkte abdecken. Die Aufgabe von PPTP beschränkt sich im Wesentlichen auf den Aufbau und Betrieb des Tunnels, über den eine oder mehrere PPP-Verbindungen gesendet werden (Multilink). Zur Unterscheidung der einzelnen Links wurde ein weiterer Header (GRE) eingebaut. Den gesamten Header bis hin zu den Nutzdaten zeigt Tabelle 6.2.

MAC-Header (Ethernet, Token-Ring, FDDI etc.)
IP-Header
GRE-Header
PPP-Header der getunnelten Verbindung(en)
IP-Header der getunnelten Verbindung(en)
TCP/UDP-Header der getunnelten Verbindung(en)
Nutzdaten der getunnelten Verbindung(en)

Tabelle 6.2: PPTP-Paketaufbau

Außer dem eigentlichen Tunnel mit den verschlüsselten und authentisierten Nutzdaten wird beim Aufbau einer PPTP-Verbindnung eine zweite Steuerverbindung auf TCP-Basis genutzt. Über den TCP-Port 1723 wird eine Client-Server-Verbindung aufgebaut; die an dieser Verbindung beteiligten Systeme werden »PPTP Access Concentrator« (PAC) und »PPTP Network Server« (PNS) genannt (Abb. 6.9). Bei Multilink-Verbindungen können mehrere PPP-Verbindungen über einen PAC geführt werden, zum Beispiel wenn zwei Netze über Firewalls und PPTP miteinander gekoppelt werden.

Folgende Funktionen werden von der TCP-Steuerverbindung wahrgenommen:

- Auf- und Abbau des PPTP-Tunnels
- Kontrolle der ordnungsgemäßen Arbeit des Tunnels durch »keep alive«-Pakete
- Auf und Abbau von physikalischen Verbindungen, zum Beispiel Telefonverbindungen
- Steuerung des PPP-Verkehrs und Fehlerbehandlung

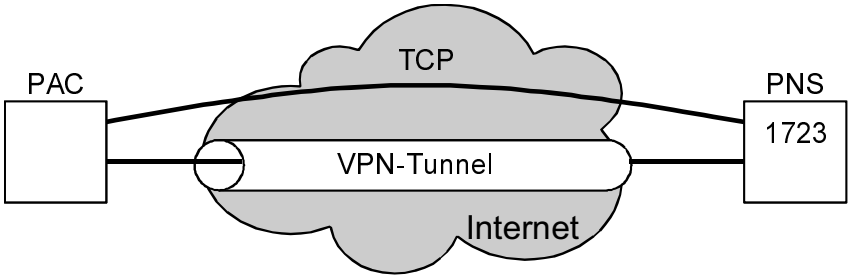


Abb. 6.9: PPTP-Verbindung

PPP-Protokoll

PPP wurde entwickelt, um unterschiedliche Protokolle über Punkt-zu-Punkt-Verbindungen zu schicken. In der Praxis wird meist IP in die PPP-Pakete »eingepackt«, doch können auch andere Protokolle wie zum Beispiel IPX eingesetzt werden.

PPP ist im OSI-Schichtenmodell in Ebene 2 (Media Access Control MAC) eingeordnet. Ebenso wie bei seinen »Kollegen« Ethernet oder Token Ring können mehrere Verbindungen gleichzeitig über eine Kommunikations-Strecke übertragen werden. PPP unterstützte in seiner ursprünglichen Version nur die Authentikation über die nachfolgend beschriebenen Protokolle PAP und CHAP, die aktuelle Variante erlaubt eine Verschlüsselung nach DES-CBC.

Authentikation

Die Authentikation über das »Password Authentication Protocol« (PAP) kann heutigen Sicherheitsanforderungen nicht genügen. Es erhält von der Zugangssoftware die Kennung und das Passwort des Benutzers und übermittelt diese mit PPP-Paketen im Klartext an den Partner, und zwar so lange, bis eine positive oder negative Quittung erhalten wird oder die Verbindung vom Partner beendet wird.

Das »Challenge Handshake Authentication Protocol« (CHAP) hingegen ist ein Challenge-Response-Verfahren, bei dem die Windows-Passwörter in Form eines bei jeder Anmeldung wechselnden MD4-Hashs übertragen werden. Replay-Attacken sind somit unmöglich. In den meisten Implementierungen von CHAP

authentisiert sich der Client am Server, doch eine zusätzliche Authentikation des Servers kann problemlos in die Kommunikation integriert werden.

Bewertung der Sicherheit

Obwohl sich PPTP im Bereich der Microsoft-Netzwerke allgemein durchgesetzt hat, muss das Design des Protokolls als kritisch eingeschätzt werden. Die TCP-Steuerverbindung zwischen PNS und PAC ist weder authentisiert noch verschlüsselt, so dass hier ein breites Spektrum von Angriffen denkbar ist. Diese reichen von der Übernahme der Verbindung (Hijacking) bis zur Störung durch manipulierte oder eingestreute Pakete. Wenn auch die im VPN-Kanal getunnelten PPP-Pakete sicher sind, kann der Netzwerkverkehr durch Angriffe auf die Steuerverbindung (Denial of Service, DoS) empfindlich gestört werden.

Die Authentikation über einen MD4-Hash entspricht ebenso wie eine gewöhnliche DES-Verschlüsselung nur dem Stand der Technik vor einigen Jahren, so dass die Zukunftsaussichten von PPTP nicht rosig sind. Microsoft hat in seinem Betriebssystem Windows 2000 als Alternative eine Absicherung über IPSec implementiert. Microsoft erfüllt leider nicht den vollständigen Standard, sondern hat sich ihm lediglich angenähert, was aber – wie schon erwähnt – eigentlich eine proprietäre Lösung ist.

6.1.3 Secure Shell (SSH)

Die von der finnischen Firma SSH entwickelte »Secure Shell« ist von ihrer Grundkonzeption her eine Applikation, die unter UNIX als Ersatz für das wegen seiner Klartext-Übermittlung von Passworten und Daten als unsicher einzustufende Telnet dient. Seit der Einführung von IPSec ist die Bedeutung von SSH als VPN-Protokoll stark gesunken. Außer dem Unix-SSH sind auch zahlreiche Windows-Implementierungen verfügbar (Abb. 6.10). Analog zu einer Telnet-Verbindung nimmt ein SSH-Client eine Verbindung zu einem SSH-Server auf, allerdings werden bei der Authentikation der Verbindung und bei der nachfolgenden Datenübertragung kryptographische Verfahren aktiviert. Im Unterschied zu Telnet (Port 23) wartet der Server bei SSH an Port 22 auf die Verbindungsaufnahme eines Clients. Als Weiterentwicklung von Telnet hat sich SSH bei der Fernadministration beispielsweise von Routern oder Servern längst durchgesetzt.

Die Entwickler von SSH haben das Protokoll mit einer großen Flexibilität ausgestattet, so dass im Prinzip jedes beliebige Protokoll über eine SSH-Verbindung getunnelt werden kann. Dadurch entsteht allerdings ein gewisser Verwaltungs-Overhead, da sich das SSH-Protokoll im IP-Stack oberhalb der TCP-Ebene ansiedelt. Dennoch hat SSH wegen der einfachen Möglichkeit der Realisierung von VPNs eine große Verbreitung auch in diesem Bereich gefunden.

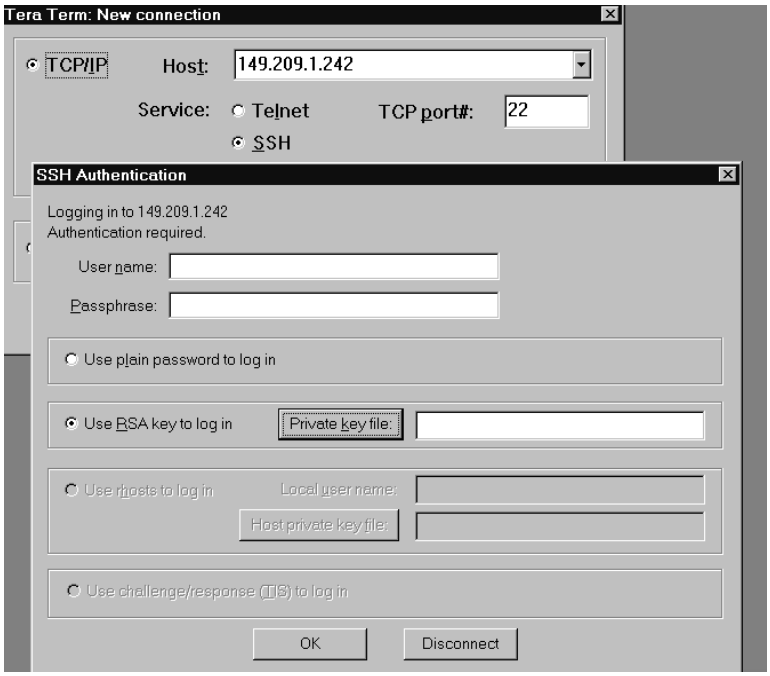


Abb. 6.10: SSH-Client unter Windows

Der Verbindungsaufbau bei SSH arbeitet dreistufig. Zunächst wird unter Benutzung des »SSH Tranport Layer Protocols« eine einseitig authentisierte Verbindung vom Client zum Server aufgebaut, bei der nur der Server seine Authentizität nachweist. Steht diese Verbindung, authentisiert sich auch der Client mittels des SSH Authentication Layer Protocols.

Damit steht ein authentisierter und verschlüsselter Tunnel zwischen Client und Server zur Verfügung, über den sich dann mittels des »SSH-Connection Protocols« beliebige andere Protokolle einspeisen lassen (Abb. 6.11).

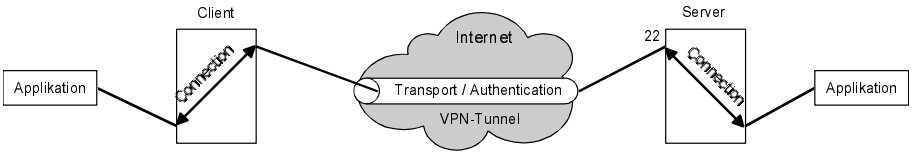


Abb. 6.11: Die Elemente einer SSH-Verbindung

Kryptographische Verfahren in SSH

In den aktuellen Implementierungen von SSH kommen folgende kryptographischen Verfahren zum Einsatz:

- Verschlüsselungsalgorithmus: Triple-DES im CBC-Modus, Blowfish (CBC), Twofish (CBC), ARCFOUR, IDEA (CBC), CAST
- Hash-Algorithmus: SHA-1 oder MD5, jeweils mit HMAC
- Authentikation: durch Diffie-Hellman oder Zertifikate nach X.509, SPKI oder PGP
- Austausch von Schlüsseln: mittels Diffie-Hellman

Die Implementierung von AES ist nur eine Frage der Zeit.

SSH-Transport Layer Protocol

Dieses Protokoll ist das allgemeine Transportmedium für SSH-Verbindungen. Es umfasst, ähnlich wie IPSec, die verschlüsselten und authentisierten Daten. Im Unterschied zum Security Parameter Index (SPI) von IPSec werden bei einer schon aufgebauten SSH-Verbindung keine Pointer auf die eingesetzten Algorithmen mehr übertragen; die gesamte »Buchführung« für die gesendeten und empfangenen Pakete müssen Client und Server unabhängig voneinander erledigen. Den Aufbau des Transport Layer Protocols zeigt Tabelle 6.3.

MAC-Header (Ethernet, Token-Ring, PPP, FDDI etc.)
IP-Header
TCP-Header
SSH-Paketlänge in Bytes
Padding-Länge in Bytes
Nutzdaten
Padding
Message Authentication Code (MAC)

Tabelle 6.3: SSH-Transport Layer Protocol

Das eigentliche SSH-Paket beginnt bei der Angabe der SSH-Paketlänge und endet mit dem MAC-Feld. Wie bei IPSec dienen die Padding-Daten dazu, feste Blocklängen für Blockverschlüsseler zu erzeugen. Verschlüsselung und Authentikation umfassen das gesamte SSH-Feld mit Ausnahme des MAC-Felds.

Zum Schutz von Replay-Attacken durch das Wiederholen bereits gesendeter Pakete wird in die Berechnung des MAC eine Sequenznummer eingebaut, die bei jedem gesendeten Paket um eins erhöht wird:

MAC = HMAC (Sequenznummer++, unverschlüsseltes SSH-Paket)

Beim Vergleich von SSH und IPSec fällt auf, dass sich die Sicherungsmechanismen von SSH nur auf das SSH-Paket beziehen. Aus der Sicht des TCP-Pakets handelt es sich um einen reinen Schutz der Nutzdaten, IP- und TCP-Header bleiben unverändert.

Das erste Byte der Nutzdaten ist eine SSH-Kennung und gibt den Typ des Pakets gemäß Tabelle 6.4 an.

SSH-Message-Number (dezimal)	Bedeutung
Transport Layer Protocol:	
1-19	Basisfunktionen des Transport-Layers (Disconnect, Ignore, Debug etc.)
20-29	Verhandlung über Algorithmen
30-49	Pakete für den Schlüsselaustausch
User Authentication Protocol:	
50-59	Basisfunktionen des User Authentication Protocol
60-79	Pakete für die User-Authentikation
Connection Protocol:	
80-89	Basisfunktionen des Connection Protocols
90-127	Nachrichten, die den einzelnen Kanälen des Tunnels zugeordnet sind
Reserviert für Client-Protokolle:	
128-191	reserviert
Erweiterungen:	
192-255	Erweiterungen

Tabelle 6.4: SSH-Message-Numbers

SSH-Authentication Protocol

Schon beim Aufbau einer SSH-Verbindung hat sich der Server authentisiert. Über das Authentication Protocol muss sich jetzt auch der Client authentisieren. Dazu sendet ihm der Server eine Liste mit Authentikations-Verfahren, die er beherrscht. Der Client kann diese Liste »nach Lust und Laune« abarbeiten. Die Bandbreite der möglichen Verfahren ist groß, sie reicht von der Angabe eines einfachen Passworts bis hin zu zertifizierten Schlüsseln.

SSH-Connection Protocol

Nach dem Aufbau eines zweiseitig authentisierten Tunnels können nun Applikationen einen Übertragungs-Kanal in diesem Tunnel eröffnen, Nutzdaten übertragen und den Kanal wieder schließen. Diese Funktionen werden über das Connection Protocol realisiert. Eine Reihe von Kanälen sind vordefiniert (Tabelle. 6.5).

Kanal-Typ	Bedeutung
session	Öffnen einer interaktiven Session
pty-req	UNIX-Pseudoterminal
x11	X-Windows
auth-agent	Client-Authentikation ohne SSH
auth-ssh1-agent	Client-Authentikation über die alte SSH-Version 1
env	Übermittlung einer UNIX-Environment-Variablen
shell	Start einer Shell
exec	Ausführung eines Programms
subsystem	Ausführung eines vordefinierten Subsystems (z. B. FTP-Transfer)
tcp-ip-forward	Tunneln von beliebigen Client-Server-Verbindungen

Tabelle 6.5: SSH-Kanäle

Zum Aufbau eines VPN bietet sich der TCP/IP-Forwarding-Kanal an, das Tunneling von UDP-Paketen ist jedoch nicht möglich. Das schränkt den Einsatzbereich von SSH etwas ein. Es gibt allerdings eine Erweiterung der aktuellen Version 2 von SSH, die alle UNIX RPC-Dienste in die Absicherung einbezieht. Damit kann ein Teil der UDP-Dienste doch noch in das SSH-Protokoll integriert werden.

6.2 Schlüsselaustausch – Methoden/Protokolle

Eine zentrale Frage bei der Implementierung von symmetrischen Verschlüsselungs-Algorithmen, wie sie auch in einem VPN zum Einsatz kommen, ist der Austausch des geheimen Schlüssels. Dieser muss beiden Seiten bekannt sein, darf aber keinesfalls in die Hände von Angreifern geraten. Eine Übertragung des Schlüssels im Klartext über das Internet scheidet damit von vorneherein aus. Beide Seiten müssen sich über einen gemeinsamen Schlüssel einig werden, ohne dass ein »Lauscher an der Wand« aus den über die Kommunikationsstrecke gesendeten Informationen einen Hinweis auf den Schlüssel enthält, der es ihm erlaubt, den Schlüssel schneller als mit einem Brute-Force-Verfahren zu ermitteln.

Da beim Aufbau einer VPN-Stecke nicht jedes Mal ein menschlicher Eingriff erfolgen kann, müssen die beteiligten Rechner automatisch nach einem vorgegebenen Key-Management-Protokoll arbeiten und mit diesem den gemeinsamen Schlüssel ermitteln und übertragen. Ist ein automatischer Austausch des Schlüssels nicht möglich, bleibt als (mühevolle) Alternative nur der manuelle Austausch. Für den automatischen Schlüsselaustausch wurden zwei grundlegend unterschiedliche Konzepte entwickelt, die jedoch beide in gängigen VPN-Implementierungen zu finden sind:

- Die Schlüsselinformation wird im IP-Paket selbst übertragen, aber natürlich so, dass ein Angreifer mit den aufgefangenen Daten den Schlüssel nicht rekonstruieren kann. Diese Form des Schlüsselaustauschs wird als geschlossenes Sicherheitssystem bezeichnet und hat den (akademischen?) Vorteil, dass sie innerhalb der IP-Ebene und somit in der zugeordneten Ebene des TCP/IP-Stack stattfindet. Für die Ebene der TCP/UDP-Protokolle oder gar der Applikationen ist dieser Schlüsselaustausch völlig transparent.
- Die Schlüsselinformation wird außerhalb der eigentlichen Kommunikation der beteiligten Applikationen übertragen. Dazu müssen eigene Hilfsapplikationen installiert werden, die das Key-Management-Protokoll »out-of-band« abwickeln und dafür sorgen, dass eine Applikation erst dann mit der Kommunikation beginnt, wenn beide Seiten den Schlüssel kennen. Der praktische Vorteil solcher Verfahren ist die mögliche Integration in eine offene Infrastruktur und die dadurch entstehenden Synergieeffekte.

Ein wichtiger Begriff beim Key-Management ist die »Perfect Forward Secrecy«. Mit ihr kann erreicht werden, dass nach dem Knacken eines Schlüssels oder Verfahrens nur zukünftige Nachrichten von einem Unbefugten entschlüsselt werden können. Die in der Vergangenheit abgesetzten verschlüsselten Nachrichten können hingegen nicht in Klartext verwandelt werden. Perfect Forward Secrecy wird durch die Verwendung kurzlebiger, von einem (Pseudo-)Zufallsgenerator erzeugter und mittels Diffie-Hellman ausgetauschter Schlüssel erreicht, die nach Gebrauch gelöscht werden. Wird ein Schlüssel oder das Verfahren der Schlüsselgenerierung später gebrochen, kennt der Angreifer die früheren Zufalls-Schlüssel nicht und sieht sich einem (erneuten) Brute-Force-Problem gegenüber gestellt.

Der VPN-Standard IPSec arbeitet mit einer Reihe von Algorithmen zum Schlüsselaustausch zusammen. Das am weitesten verbreitete Verfahren ist IKE, es sind aber auch Implementierungen mit SKIP oder manuellem Schlüsselaustausch vorhanden.

6.2.1 Pre-Shared key

Von einem Pre-Shared Key wird gesprochen, wenn der gemeinsame Schlüssel nicht erst beim Aufbau der Verbindung ermittelt und ausgetauscht wird, sondern sich bereits auf den beteiligten Rechnern befindet:

- Die Schlüssel wurden manuell übertragen (zum Beispiel per Diskette oder verschlüsselter E-Mail). Diese Methode wird auch als »Manual keying« bezeichnet.
- Die Schlüssel sind in die Geräte fest eingebaut (zum Beispiel ins EPROM).

Pre-Shared Keys haben gravierende Nachteile. Zum einen ist es bei einer größer werdenden VPN-Infrastruktur kaum noch möglich, die benötigten Schlüssel zu verteilen und einzuspielen. Sieht man einmal von der äußerst leichtsinnigen Vari-

ante ab, allen beteiligten Geräten den selben Schlüssel für die gesamte Kommunikation untereinander mitzugeben, lassen sich die bei n VPN-Knoten erforderlichen Schlüssel K zu

$K = n(n-1)/2$

berechnen. Eine Firma mit nur 10 Standorten, bei der jeder Standort mit den anderen über ein VPN kommunizieren soll, benötigt schon 45 verschiedene Schlüssel. Auf jedem der 10 Gateways ins Internet müssen die benötigten 9 Schlüssel gepflegt und gegebenenfalls ersetzt werden. Bei 50 Standorten sind schon 1225 Schlüssel erforderlich und auf jedem der 50 Gateways befinden sich 2450 Schlüssel, was von keinem Administrator mehr zu verwalten ist.

Ein weiterer Nachteil von Pre-Shared Keys ist der nur relativ seltene Schlüsselwechsel. Moderne Verschlüsselungs-Verfahren wechseln ihren Schlüssel oft schon nach Minuten (oder einigen 100 KByte), um selbst bei einem erfolgreichen Angriff auf einen der Schlüssel eine Entschlüsselung der VPN-Daten zu verhindern. Ohne besondere Maßnahmen ist ein schneller Schlüsselwechsel mit dem Pre-Shared-Key-Verfahren nicht möglich.

Pre-Shared-Key-Verfahren kommen daher nur in kleinen VPN-Strukturen zum Einsatz, oder wenn aus organisatorischen oder technischen Gründen keine andere Lösung möglich ist. Ein klassischer Einsatzfall für Pre-Shared Keys sind Geräte unterschiedlicher Hersteller, die zwar vom eingesetzten Protokoll her, nicht aber vom Verfahren des Schlüsselaustauschs her zueinander kompatibel sind.

6.2.2 Simple Key Management for Internet Protocols (SKIP)

SKIP ist ein von Sun Microsystems entwickeltes Verfahren, das den gerade aktuellen Schlüssel im Paket selbst verschickt. Dieser Schlüssel wird deshalb auch Paketschlüssel genannt. Theoretisch könnte jedes Paket mit einem anderen Schlüssel bearbeitet werden, so dass ein Knacken von SKIP aussichtslos erscheint. Der Paketschlüssel darf natürlich nicht im Klartext übertragen werden. Er wird mit einem zweiten Schlüssel (Master Key) verschlüsselt, der aber niemals über die Leitung gesendet wird. Eine Folge von Master Keys wird aus einem geheimen »Superschlüssel« berechnet, der mittels Diffie-Hellman oder aber nach einem Pre-Shared-Key-Verfahren zu den beiden Partnern übertragen werden kann.

Die Länge der IP-Pakete vergrößert sich drastisch, da zusätzlich der verschlüsselte Paketschlüssel mit übertragen werden muss und, falls der Verschlüsselungs-Algorithmus eine bestimmte Blocklänge voraussetzt, ein Padding-Feld vorhanden sein muss. Durch diese Maßnahmen kann eine Fragmentierung der IP-Pakete nötig werden, was bei korrekter Konfiguration der Netzwerkinterfaces aber keine Probleme bereiten sollte.

Bei einem n:m-VPN müssen an der gesicherten Kommunikation mehr als zwei Partner teilnehmen. Unter SKIP ist deshalb die Angabe einer Namespace-ID (NSID) möglich, die einen Namensraum mit allen beteiligten Rechnern angibt. Alle Knoten mit gleicher NSID können ohne Einschränkung gleichgewichtig die SKIP-Pakete bearbeiten.

Kryptographische Verfahren im SKIP-Protokoll

SKIP macht keine Vorgaben oder Annahmen über die zur Authentikation bzw. Verschlüsselung der Pakete eingesetzten Algorithmen, so dass im Prinzip der Einbau beliebiger Verfahren möglich ist.

SKIP im Detail

SKIP ist von seiner Definition her flexibel, der Einsatz in IPv4 und IPv6 ist möglich. Es arbeitet mit IPSec zusammen, so dass die dort definierten Header AH und ESP genutzt werden können. Durch das Mitsenden des Schlüssels in jedem Paket vereinfacht sich die Verarbeitung in den beteiligten Hosts und Gateways ganz enorm. Dabei ist der Paketschlüssel Kp nicht direkt der für die Authentikation oder Verschlüsselung genutzte Schlüssel. Aus Kp lassen sich nach einem in SKIP definierten Verfahren zwei Schlüssel ableiten, von denen einer zur Authentikation, der andere zur Verschlüsselung genutzt wird.

Abbildung 6.12 zeigt die Verwandlung eines Pakets vom Typ IPv4 in ein SKIP-Paket.

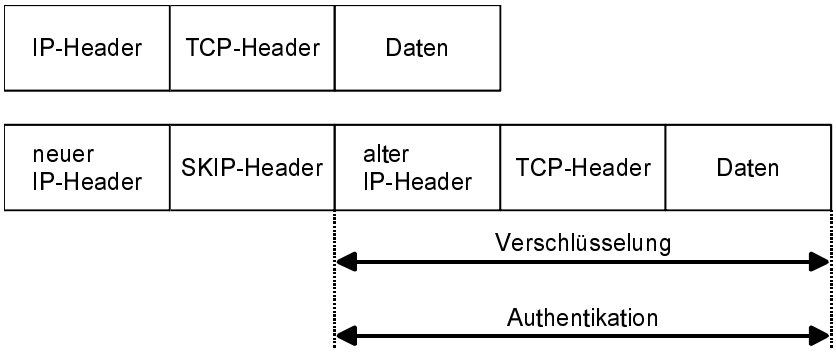


Abb. 6.12: SKIP unter IPv4

Da das gesamte ursprüngliche IP-Paket verschlüsselt wird, arbeitet SKIP immer im Tunnelmodus. Der Transportmodus kann aber durch die Umsetzung

neuer IP-Header = alter IP-Header (Modifikation von Länge und Prüfsumme)

leicht emuliert werden. Der SKIP-Header selbst hat den in Abb. 6.13 angegebenen Aufbau:

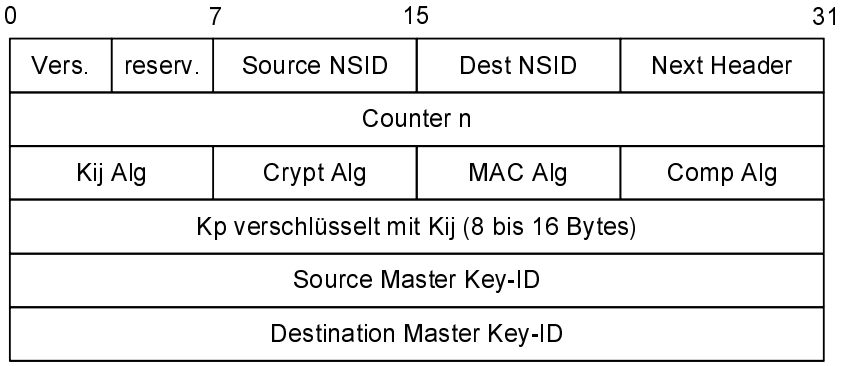


Abb. 6.13: Der SKIP-Header

Dabei haben die einzelnen Felder folgende Bedeutung:

- Die Version gibt die Versionsnummer des SKIP-Protokolls an.
- Die reservierten Bits werden zur Zeit alle auf Null gesetzt.
- Die NSID (Namespace-ID) wird eingesetzt, wenn der »Superschlüssel« mehr als nur zwei Netzwerkknoten bekannt ist. Dann bezieht sich der jeweilige Master Key nicht mehr nur auf bestimmte Rechner, sondern auf einen »Namensraum« von Rechnern. Dieser Namensraum wird durch die NSID spezifiziert. Falls eine oder beide NSID nicht angegeben sind, sind die Werte zu Null gesetzt.
- Das »Next Header«-Feld gibt – wie üblich – den Typ des nächsten Headerfelds an, beispielsweise AH oder ESP.
- Der Zähler n entspricht den Sequenznummern von AH oder ESP und dient der Bekämpfung von Replay-Attacken.
- Die nächsten Felder spezifizieren die eingesetzten Algorithmen zur Ermittlung der Master Keys Kij, zur Verschlüsselung und Authentikation (MAC) sowie zur Komprimierung.
- Es folgt der Paketschlüssel Kp, verschlüsselt mit dem Master Key Kij.
- Die letzten Felder (Master-Key-ID) werden nur benötigt, wenn die dazugehörige NSID ungleich Null ist, wenn also theoretisch mehr als zwei Partner in die Kommunikation eingebunden sein können. Dann steht in diesen Feldern ein Verweis auf den endgültigen Empfänger beziehungsweise den tatsächlichen Sender.

Der SKIP-Header hat den IP-Protokolltyp 57.

Durch die Kombination der MSID und NSID ist es möglich, auf dem Weg eines Pakets bestimmte Netzwerkknoten (Gateways, Firewalls etc.) in die Überprüfung der Pakete einzubinden, ohne dass diese die wirkliche Absenderadresse beziehungsweise die endgültige Zieladresse sind. Sie müssen lediglich zum gleichen Namensraum wie der Absender beziehungsweise Empfänger gehören.

Versand von SKIP-Paketen

Beim Versand eines SKIP-Paketes sind folgende Operationen erforderlich:

- Der aktuelle Master Key Kij wird aus dem beiden Seiten per Diffie-Hellman (oder auch durch manuelle Übertragung) bekannten »Superschlüssel« und einem Inkrement berechnet.
- Der aktuelle Paketschlüssel Kp wird beispielsweise mit einem Zufallsgenerator ermittelt.
- Aus Kp werden die Teilschlüssel für Authentikation und Verschlüsselung berechnet.
- Das Paket wird mit diesen Schlüsseln authentisiert und verschlüsselt.
- Kp wird mit dem gerade aktuellen Master Key verschlüsselt.
- Der neue Header wird gebildet und das Paket wird versendet.

Dabei sollte der Paketschlüssel Kp häufig geändert werden, zum Beispiel alle 5 Minuten oder nach 100 KBytes Daten. Der Master Key kann etwa jede Stunde geändert werden, abhängig vom Geheimhaltungsgrad und Verkehrsaufkommen. Durch das Inkrement wird gewährleistet, dass niemals derselbe Master Key ein zweites Mal eingesetzt wird.

Empfang von SKIP-Paketen

Der Empfänger verfährt folgendermaßen:

- Der aktuelle Master Key wird berechnet
- Der aktuelle Paketschlüssel Kp wird mit dem Master Key entschlüsselt
- Aus Kp werden die Teilschlüssel für Authentikation und Verschlüsselung berechnet
- Das Paket wird entschlüsselt und authentisiert
- Die Nutzdaten werden den höheren Schichten im Netzwerkstack zugeführt

Zusammenarbeit von SKIP und IPSec

Da SKIP neben dem reinen Schlüsselaustausch Möglichkeiten zur Authentikation und Verschlüsselung bietet, ist eine Integration von SKIP und IPSec kein großes Problem. Dabei steht der SKIP-Header jeweils vor den AH- bzw. ESP-Headern. Die AH- und ESP-Header selbst bleiben unverändert. Mit SKIP sinkt der Verwaltungs-Overhead für IPSec. Die Filterfunktionen SA brauchen weniger komplex zu sein, da die Authentikations- und Verschlüsselungsfunktionen ja bereits in SKIP enthalten sind.

Bewertung von SKIP

Beim Einsatz von SKIP ist die Bedrohung durch Hacker gering. Das Knacken eines einzelnen Paketschlüssels Kp bringt so gut wie nichts, und die Berechnung des Master Keys aus einer Reihe entschlüsselter Kp ist praktisch ausgeschlossen. Ein

Problem könnte der mögliche Diebstahl des »Superschlüssels« sein, der allerdings nur auf sehr wenigen Netzwerkknoten abgelegt ist und niemals über das Netz übertragen wird – auch nicht in verschlüsselter Form.

Brute-Force-Attacken sind durch den raschen Schlüsselwechsel praktisch unmöglich. Auch ein Angriff auf die Algorithmen hat nur eine begrenzte Wirkung, es sein denn, der gewählte Algorithmus ist so schwach, dass eine Echtzeit-Entschlüsselung möglich ist.

6.2.3 Internet Key Exchange (IKE)

IKE ist ein Verfahren, das auf den beiden Standards »Internet Security Association Key Management Protocol« (ISAKMP) und »Oakley« basiert. IKE, ISAKMP und Oakley wurden von der Internet Egeneering Task Force (IETF) definiert (siehe RFC 2408, 2409 und 2412 unter www.ietf.org).

ISAKMP stellt einen Protokoll-Rahmen für einen Schlüsselaustausch in zwei Phasen zur Verfügung. Oakley ist ein Perfect-Forward-Secrecy-Ansatz zum Austausch von Schlüsseln auf Basis von Diffie-Hellman. IKE ist das Standardverfahren zum Schlüsselaustausch bei IPSec.

In der ersten Phase wird ein gesicherter und authentisierter Kanal zwischen den beiden Partnern aufgebaut. Dabei besteht die Möglichkeit, alternativ ein besonders schnelles (Aggressive Mode) oder ein besonders sicheres (Main Mode) Verfahren einzusetzen. Im Main Mode werden zunächst Pre-Authentikations-Token – genannt Cookies – ausgetauscht. Diese Datenstrukturen sind kurze Hash-Werte und benötigen zu ihrer Generierung und Versendung kaum Ressourcen. Dabei muss das Cookie zunächst vom Client angefordert und anschließend dessen Empfang explizit bestätigt werden. So können Denial-of-Service-Angriffe durch die bloße Wiederholung von Anmeldeversuchen (Flooding) bekämpft werden. Danach werden über Diffie-Hellman Schlüssel ausgetauscht, die über Zertifikate abgesichert werden können. Anschließend einigen sich die Partner über ein gemeinsames Verfahren zur Verschlüsselung. Diese Festlegung wird – wie bei IPSec – Security Association (SA) genannt. Der schnellere Aggressive Mode überspringt den Austausch der Cookies, die Verbindungsaufnahme wird dadurch anfälliger gegen Angriffe.

Zwischen der ersten und der zweiten Phase kann ein Zwischenschritt eingebaut werden, der den Betrieb von IKE zusammen mit einer Gruppe von Netzwerkknoten (n:m-VPN) ermöglicht. Im »New Group Mode« kann eine Diffie-Hellman-Gruppe gebildet werden, deren Mitglieder sich dann untereinander verständigen können.

In der Phase 2 werden weitere Security Associations (SA) ausgehandelt, auf die IPSec dann unmittelbar zugreifen kann.

Kryptographische Verfahren in IPSec

IKE unterstützt eine große Anzahl kryptographischer Verfahren:

- Verschlüsselungsalgorithmus: DES, Triple-DES, IDEA, Blowfish, RC5, CAST (alle im CBC-Modus), ECP, EC2N, AES
- Hash-Algorithmus: Tiger, SHA-1 oder MD5
- Authentikation: durch DSS-Signaturen (ElGamal), RSA-Signaturen mit X.509-Zertifikaten, RSA ohne Zertifikate, Pre-Shared Keys
- Austausch von Session-Keys: mittels Diffie-Hellman

IKE im Detail

Da IKE ein sehr flexibles Protokoll ist, haben die hin und her geschickten Pakete einen komplexen Aufbau. Deshalb wird an dieser Stelle auf die Wiedergabe des Aufbaus der kompletten Pakete verzichtet. Statt dessen wird eine schematische Darstellung der einzelnen Kommunikationsschritte gegeben.

Zunächst wird (optional) vom Initiator der Verbindung ein Cookie erzeugt und gesendet. Dieser besteht im wesentlichen aus einem Hashwert, der aus einer geheimen Zahl, den IP-Adressen sowie den Portnummern der beiden Partner generiert wird. Der Empfänger des Cookies, Responder genannt, prüft, ob er schon bestehende Anforderungen des Initiators hat (Flooding?) und antwortet mit einem ähnlich gearteten Hash. Das Austauschen der Cookies hat keinerlei kryptographische Funktion, es dient nur dazu, Ressourcen beim Responder zu schonen.

Phase 1 des IKE-Protokolls baut eine abgesicherte und authentisierte Verbindung zwischen Initiator und Responder auf. Je nach dem Authentikations-Mechanismus und dem gewählten Modus ergeben sich unterschiedliche Abfolgen von Paketen, die in den folgenden Tabellen leicht vereinfacht dargestellt sind.

Initiator	Richtung	Responder
ein oder mehrere Vorschläge für eine Security Association (SA)	→	
	←	Auswahl einer SA
Diffie-Hellman-Austausch	→	
	←	Diffie-Hellman-Austausch
digitale Signatur (ggf. mit Zertifikat)	→	
	←	digitale Signatur (ggf. mit Zertifikat)

Tabelle 6.6: Main-Modus mit Authentikation über digitale Signatur

Initiator	Richtung	Responder
ein oder mehrere Vorschläge für eine SA, Diffie-Hellman-Austausch	→	
	←	Auswahl einer SA, Diffie-Hellman-Austausch, digitale Signatur (ggf. mit Zertifikat)
digitale Signatur (ggf. mit Zertifikat)	→	

Tabelle 6.7: Aggressive-Modus mit Authentikation über digitale Signatur

Initiator	Richtung	Responder
einer oder mehrere Vorschläge für eine SA	→	
	←	Auswahl einer SA
Diffie-Hellman-Austausch, Zufallszahl n mit dem öffentlichen Schlüssel des Responders verschlüsselt	→	
	←	Diffie-Hellman-Austausch, Zahl n mit dem öffentlichen Schlüssel des Initiators verschlüsselt
Message Authentication Code (MAC)	→	
	←	MAC

Tabelle 6.8: Main-Modus mit Authentikation über öffentliche Schlüssel

Initiator	Richtung	Responder
ein oder mehrere Vorschläge für eine SA, Diffie-Hellman-Austausch, Zufallszahl n mit dem öffentlichen Schlüssel des Responders verschlüsselt	→	
	←	Auswahl einer SA, Diffie-Hellman-Austausch, Zahl n mit dem öffentlichen Schlüssel des Initiators verschlüsselt, MAC
MAC	→	

Tabelle 6.9: Aggressive-Modus mit Authentikation über öffentliche Schlüssel

Initiator	Richtung	Responder
ein oder mehrere Vorschläge für eine SA	→	
	←	Auswahl einer SA
Diffie-Hellman-Austausch	→	
	←	Diffie-Hellman-Austausch
MAC	→	
	←	MAC

Tabelle 6.10: Main-Modus mit Authentikation über Pre-Shared Key

Initiator	Richtung	Responder
einer oder mehrere Vorschläge für eine SA, Diffie-Hellman-Austausch	→	
	←	Auswahl einer SA, Diffie-Hellman-Austausch, MAC
MAC	→	

Tabelle 6.11: Aggressive-Modus mit Authentikation über Pre-Shared Key

Alle weiteren IKE-Operationen (New Group, Phase 2) werden über diesen sicheren Kanal abgewickelt und können daher auf rechenaufwändige Public-Key-Operationen verzichten. Wird Perfect Forward Secrecy benötigt, ist (mindestens) ein weiterer Diffie-Hellman-Schlüsselaustausch erforderlich.

Die über das Netz geschickten Pakete ähneln von ihrer Struktur denen in Phase 1, wenn alle Operationen mit öffentlichem Schlüssel ausgelassen werden.

Bewertung von IKE

IKE ist durch die Verwendung von gut bekannten und analysierten Standard-Verfahren als sicher zu bezeichnen. Ein Nachteil ist der komplizierte Ablauf der Verhandlungen zwischen den beiden Partnern, der »out-of-band« abgewickelt wird. Dennoch ist IKE der Standard der Zukunft, vor allem wegen seiner problemlosen Integration in das IPSec-Verfahren.

6.2.4 Schlüsselaustausch bei SSH

Die Secure Shell (SSH) nutzt zum Austausch der Algorithmen und Schlüssel ein proprietäres Protokoll. Als Ergebnis dieser Prozedur entsteht ein geheimer Schlüssel, der beiden Seiten bekannt ist, und ein Hash-Wert, der als Identifikation für die Session dient. Als Standard-Verfahren sind Diffie-Hellman und SHA-1 implementiert, doch auch andere Algorithmen sind denkbar.

Zunächst müssen die Algorithmen über den Austausch mit bestimmten Netzwerk-Paketen ausgehandelt werden. Tabelle 6.12 zeigt den schematischen Aufbau.

Wert	Bedeutung
SSH_MSG_KEXINIT	Identifikation aus Abb. 6.15
cookie	Zufallszahl
kex_algorithms	Liste von Algorithmen für den Schlüsselaustausch
server_host_key_algorithms	Liste von Algorithmen für den öffentlichen Schlüssel des Servers
encryption_algorithms_client_to_server	Liste von Algorithmen für die Verschlüsselung vom Client zum Server
encryption_algorithms_server_to_client	Liste von Algorithmen für die Verschlüsselung vom Server zum Client
mac_algorithms_client_to_server	Liste von Algorithmen für die Berechnung des MAC vom Client zum Server
mac_algorithms_server_to_client	Liste von Algorithmen für die Berechnung des MAC vom Server zum Client
compression_algorithms_client_to_server	Liste von Algorithmen für die Daten-Kompression vom Client zum Server
compression_algorithms_server_to_client	Liste von Algorithmen für die Daten-Kompression vom Server zum Client
languages_client_to_server	Liste von sprachabhängigen Angaben (nach RFC 1766) für die Kommunikation vom Client zum Server
languages_server_to_client	Liste von sprachabhängigen Angaben (nach RFC 1766) für die Kommunikation vom Server zum Client
first_key_packet_follows	Flagge, die angibt, ob das erste Paket für den Schlüsselaustausch im Anschluss folgt
0	für Erweiterungen reserviert

Tabelle 6.12: Aufbau der Pakete für die Ermittlung von Algorithmen

Dabei können jeweils mehrere Verfahren (mit abnehmender Priorität) angegeben werden, die durch Kommata voneinander getrennt werden müssen. Haben sich die beiden Rechner über die Verfahren geeinigt, werden geheimer Schlüssel und Hashwert ermittelt.

Bewertung des Schlüsselaustauschs bei SSH

Da der Schlüsselaustausch bei SSH fest vorgegeben ist, besteht keine Alternative zu dem Verfahren. Seine Komplexität liegt zwischen SKIP und IKE, wegen des Einbaus bekannter Verfahren ist eine hohe Sicherheit gewährleistet.

Kapitel 7

Praktischer Einsatz von Virtual Private Networks

Dieses Kapitel behandelt den praktischen Einsatz von VPN-Systemen. Neben Umsetzungsbeispielen von VPNs für verschiedene Anwendungsfälle wird exemplarisch die Konfiguration zweier gängiger VPN-Lösungen beschrieben.

7.1 Fallstudien

In diesem Abschnitt wird anhand von Praxisbeispielen vorgestellt, wie verschiedene Organisationen mit sehr unterschiedlichen Anforderungen Virtual Private Networks aufgebaut haben, um eine vertrauenswürdige Kommunikation zu gewährleisten.

7.1.1 Sichere Ankopplung von Außendienstmitarbeitern eines Versicherungsunternehmens

Anforderungen

Die Außendienstmitarbeiter greifen auf einen zentralen Server der Versicherung zu, um an aktuelle Informationen zu gelangen. Dies erspart Zeit und ermöglicht den Versicherungsmaklern vor Ort, immer auf aktuelle Daten und Berechnungen zugreifen zu können. Da diese Daten, beispielsweise für Lebensversicherungen (Angaben über Krankheiten des Kunden usw.), sehr sensibel sind, muss die Kommunikation vertrauenswürdig realisiert werden, damit die Versicherung keinen Image-Schaden durch Angriffe erleidet.

Lösung

Zentral wurde ein redundantes, hochverfügbares VPN-Gateway aufgebaut, das über einen X.500-Directory-Service die Zertifikate und Zertifikats-Revokationslisten (CRLs) der einzelnen Außendienstmitarbeiter abrufen kann. Außerdem steht zentral eine PKI für Schlüssel und Zertifikatsmanagement zur Verfügung.

Die einzelnen Außendienstmitarbeiter haben auf ihrem Rechnersystem (Notebook oder Desktop) einen VPN-Client installiert.

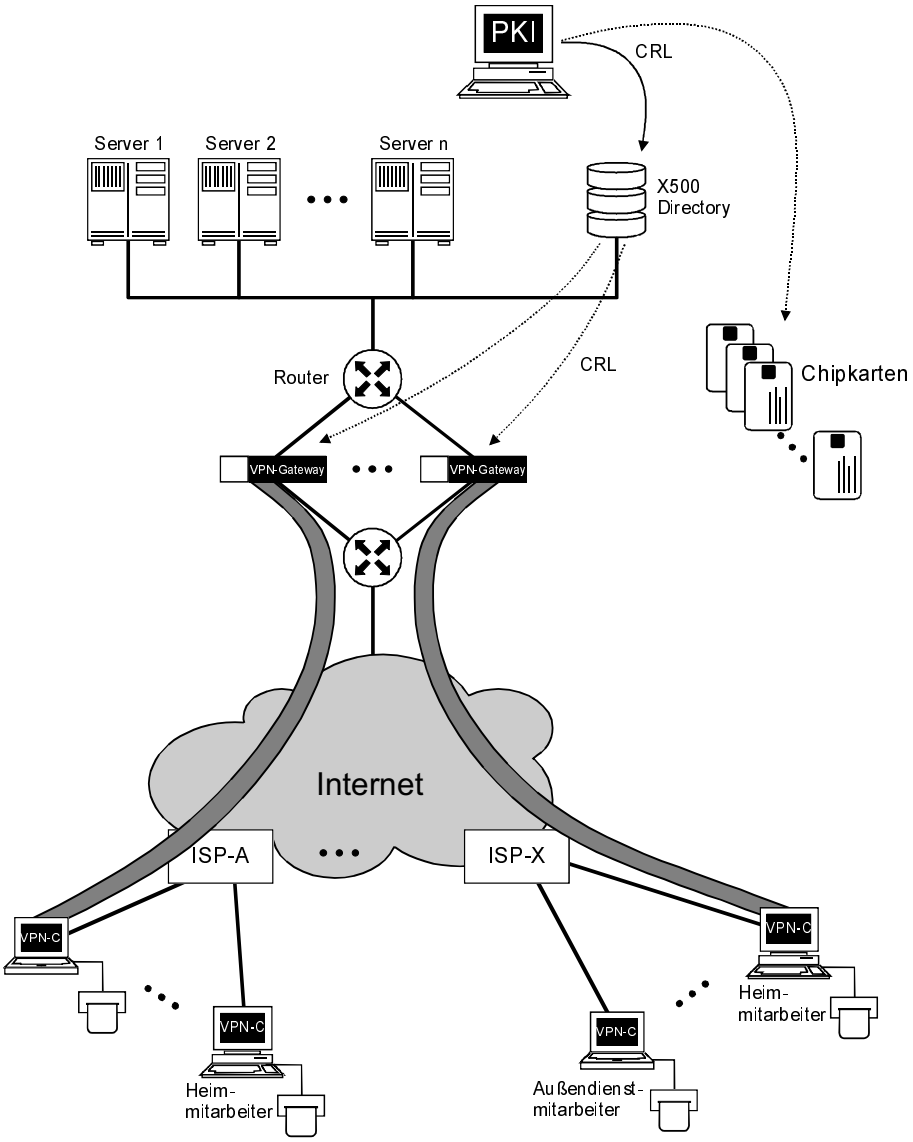


Abb. 7.1: VPN-Anwendung im Außendienst einer Versicherung

Das Hochverfügbarkeitskonzept sorgt dafür, dass beliebig viele VPN-Gateways parallel betrieben werden können, womit eine Performancesteigerung erreicht werden kann. Fallen einzelne VPN-Gateways aus, oder müssen zu Wartungszwecken abgeschaltet werden, werden ihre Verbindungen sofort an andere VPN-Gateways weitergegeben.

Ablauf

In der PKI – Certification Authority (CA) und Registration Authority (RA) – werden für die Außendienstmitarbeiter und für die VPN-Gateways Identitäten vergeben, Pubic-Key-Schlüsselpaare und passende Zertifikate generiert. Der geheime Schlüssel des Public-Key-Schlüsselpaares und das eigene Zertifikat wird auf den persönlichen Sicherheits-Token (Disketten oder Chipkarten) der Mitarbeiter gespeichert.

Das CA-Zertifikat steht entweder ebenfalls auf dem Sicherheits-Token oder befindet sich in einer Zertifizierungsdatenbank auf dem Client (zum Beispiel im Fall von PKCS#12).

In der PKI werden die aktuellen und ungültigen Zertifikate verwaltet. Mit Hilfe einer CRL werden die ungültigen Zertifikate dem X500-Directory-Service zur Verfügung gestellt.

Um den geheimen Schlüssel auf dem persönlichen Sicherheits-Token nutzen zu können, ist eine Personal Identification Number (PIN) notwendig. Die erste PIN wird dem Außendienstmitarbeiter per PIN-Brief auf eine sichere Art und Weise mitgeteilt. Das persönliche Sicherheits-Token sowie der PIN-Brief werden den Außendienstmitarbeiter separat übermittelt.

Auch in den VPN-Gateways wird der geheime Schlüssel eingeführt. Die VPN-Gateways können die Zertifikate von X.500-Directory Service abrufen. Die VPN Gateways haben, wie die Clients, ebenfalls Sicherheits-Token mit den entsprechenden Informationen.

Wenn alle Komponenten (VPN-Gateways und VPN-Clients mit Sicherheits-Token) personalisiert sind, kann die vertrauenswürdige Kommunikation über das VPN-System beginnen. Die Authentikation der Außendienstmitarbeiter wird zertifikatsbasiert durchgeführt, wobei das entsprechende Sicherheits-Token (Diskette oder Chipkarte) verwendet wird.

Falls ein Außendienstmitarbeiter nicht mehr über das VPN-System auf die Daten und Dienste des Versicherungsunternehmens zugreifen soll, wird das Zertifikat des entsprechenden Außendienstmitarbeiters in eine Revokationsliste (CRL) in der PKI eingetragen und ist damit gesperrt.

7.1.2 Vertrauenswürdige Kommunikation über ein internationales IP-Netzwerk

Anforderungen

Die Kommunikation zwischen den Botschaften und dem Auswärtigen Amt eines Landes soll in vertrauenswürdiger Art und Weise realisiert werden, weil hier Informationen von höchster Sicherheitsrelevanz ausgetauscht werden.

Ähnliche Anforderungen stellen alle zentral organisierten Unternehmen mit sternförmigen Netzwerken.

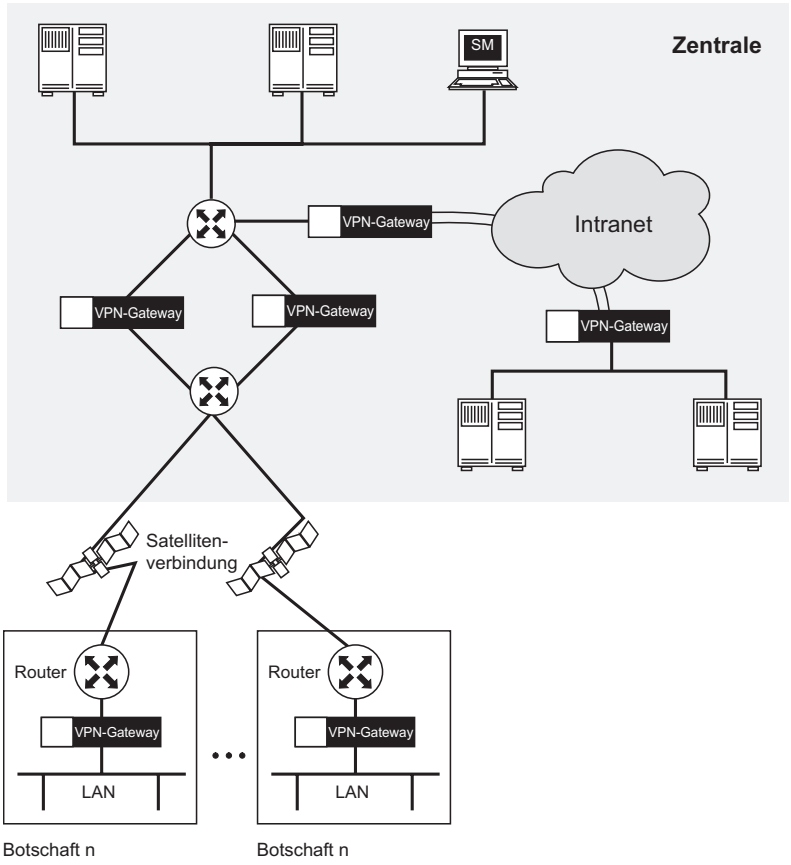


Abb. 7.2: VPN-Anwendung in zentral organisierten Unternehmen oder Behörden

Lösung

In den Botschaften der Länder wird jeweils ein VPN-Gateway vor den Anschluss an das internationale IP-Netzwerk geschaltet. Zentral im Auswärtigen Amt wird ein redundantes, hochverfügbares VPN-Gateway aufgebaut. Die VPN-Gateways sorgen dafür, dass alle Daten vertrauenswürdig über das internationale IP-Netzwerk übertragen werden.

Außerdem wird in der Zentrale ein VPN über das Intranet aufgebaut. Dadurch wird eine vertrauenswürdige Kommunikation zwischen den einzelnen Abteilungen des Auswärtigen Amts sowie zwischen den Abteilungen und den Botschaften gewährleistet.

Die Einrichtung separater VPNs im Intranet und im Extranet dient dazu, dass sowohl die Kommunikation der Abteilungen untereinander und mit den Botschaften als auch der Zugriff der Botschaften auf die Server des Auswärtigen Amts geschützt abläuft.

Ablauf

Die Architektur erlaubt die vertrauenswürdige Kommunikation zwischen der Zentrale und den Botschaften via Satellit. Auch die Kommunikation der Botschaften untereinander wird via Satellit über die Zentrale und somit über eine vertrauenswürdige Verbindung gelenkt.

Die Kommunikation im Intranet, also zwischen den Abteilungen, wird in diesem Modell ebenfalls vor unbefugten Zugriffen geschützt.

Die Verwaltung erfolgt über das Sicherheitsmanagement (SM) in der Zentrale der Organisation.

7.1.3 Angebot eines vertrauenswürdigen IP-Netzes durch einen Service Provider

Anforderung:

Ein Service Provider möchte nicht nur Kommunikationsmöglichkeiten über das IP-Netz, sondern auch die Möglichkeit *vertrauenswürdiger* Kommunikation anbieten. Dadurch brauchen seine Kunden nicht selbst in entsprechende Sicherheitsmaßnahmen zu investieren.

Lösung:

Der Service Provider rüstet die Unternehmen, die an ein vertrauenswürdiges IP-Netz angekoppelt werden wollen, nicht nur mit Routern, sondern zudem mit VPN-Gateways aus. Diese werden von einem zentralen Management-System beim Service Provider aus verwaltet. Für den Kunden ist diese Lösung völlig transparent; vertraglich ist geregelt, dass die Kommunikation vertrauenswürdig durchgeführt wird und der Service Provider die Verantwortung dafür trägt.

Ablauf:

Der Service Provider installiert die VPN-Gateways bei der Bereitstellung des Anschlusses und verwaltet sie zentral mit Hilfe eines Sicherheitsmanagements.

Er kann seinen Kunden nun vertrauenswürdige Netzwerkverbindungen zwischen deren Unternehmenseinheiten, aber auch zu den anderen am vertrauenswürdigen Netz beteiligten Unternehmen bereitstellen. Nach der Einstellung entsprechender Regeln kann damit eine vertrauenswürdige Kommunikation realisiert werden, die der Service Provider zu einem Mehrpreis anbietet.

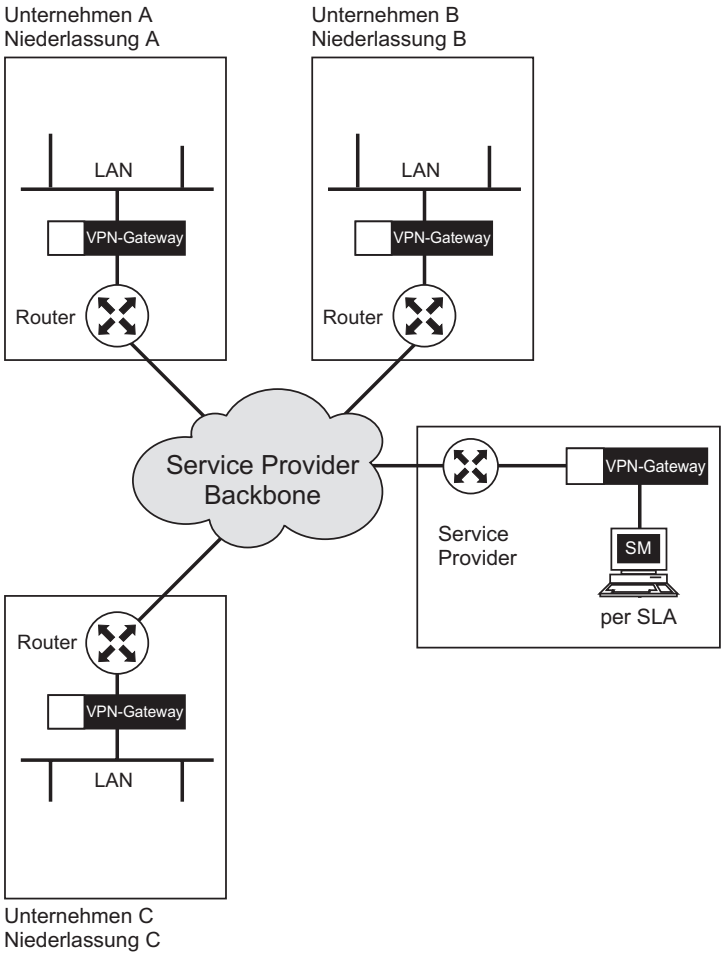


Abb. 7.3: VPN als Angebot eines Service Providers

Betrachtet man diese Lösung im Licht der aktuellen Diskussion um externe IT-Dienstleister, sogenannte Application Service Provider, die auch als Security Service Provider denkbar sind, kann man folgende Ergebnisse festhalten:

- Ein Modell, in dem unterschiedliche Organisationen den gleichen Sicherheits-Dienstleister nutzen, hat den Vorteil, dass durch die Verwendung eines öffentlichen Netzwerks und das Outsourcing der Netzwerkverwaltung und Sicherheitsverwaltung die Kosten deutlich reduziert werden.
- Die Qualität der Sicherheit hängt in diesem Fall von der Qualität und Vertrauenswürdigkeit des Service Providers ab.
- Inwieweit ein Service Provider im Schadensfall zur Rechenschaft gezogen werden kann, sollte vertraglich festgelegt werden.

7.1.4 Vertrauenswürdige Vernetzung von Polizeidienststellen

Anforderung:

Eine Polizeibehörde möchte über das Landesverwaltungsnetz 300 Polizeistationen miteinander vernetzen und hierbei eine vertrauenswürdige Kommunikation gewährleisten. Außerdem soll ein sicherer Zugang zum Internet oder zu anderen zentralen Diensten bereitgestellt werden.

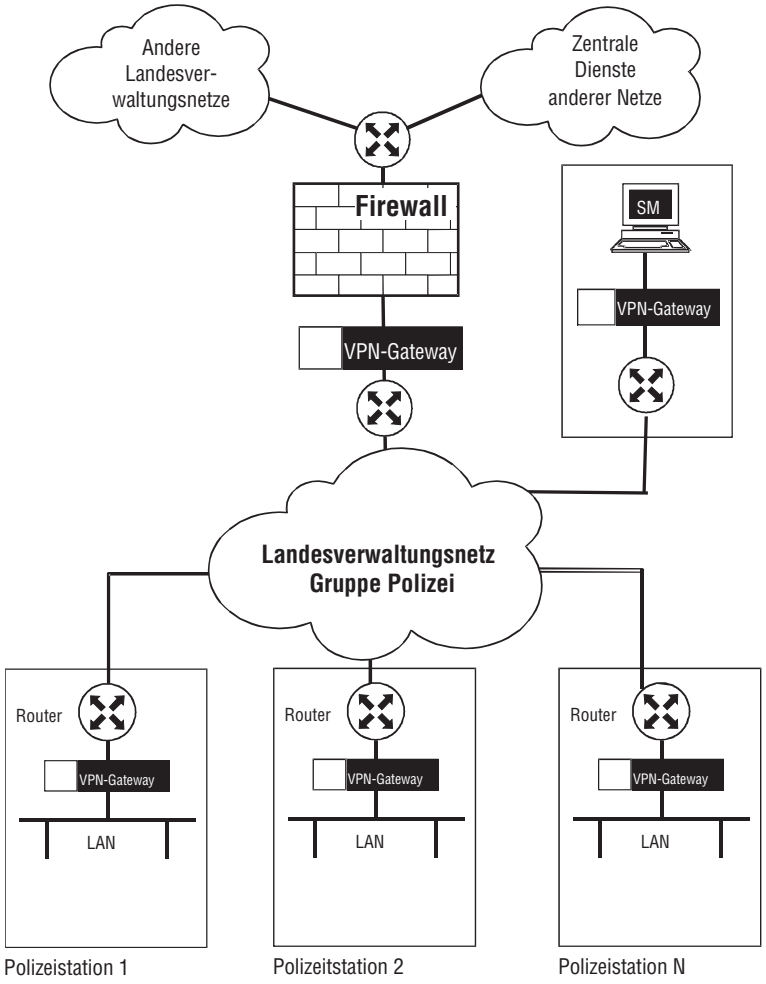


Abb. 7.4: VPN und Firewall-System in einem Landesverwaltungsnetz

Lösung:

Alle Polizeistationen werden mit einem VPN-Gateway ausgerüstet. Das Sicherheitsmanagement wird von einer zentralen Stelle aus durchgeführt. Der Zugang zu den anderen Netzen wird mit einem Firewall-System geschützt, das hinter den VPN-Gateways implementiert wird. Dadurch können die Benutzer in gesicherter Form auf andere Verwaltungsnetze und Netzdienste zugreifen.

Ablauf:

Die Polizeidienststellen sind somit in der Lage, miteinander vertrauenswürdig zu kommunizieren und den geforderten hohen Schutzbedarf zu erfüllen.

Außerdem wird es den Polizeibeamten ermöglicht, mit minimalem Risiko auf Ressourcen in anderen Netzen zuzugreifen. Angriffe aus diesen Netzen werden durch das Firewall-System abgeblockt, so dass Unbefugte keinen Zugriff auf das Netz der Polizei erhalten.

Durch das zentrale Sicherheitsmanagement ist eine einfache Verwaltung der vertrauenswürdigen Kommunikation möglich.

7.2 VPN-Implementierungen

Die praktische Umsetzung von VPN-Konzepten ist keine leichte Sache. Die Vielzahl an Algorithmen, deren unterschiedliche Implementierungen und die nur unzureichende Standardisierung machen die Konfiguration von VPNs oft zu einer mühsamen Angelegenheit. Besonders anspruchsvoll ist die Einrichtung einer VPN-Verbindung, deren Endpunkte von unterschiedlichen Herstellern stammen.

Um ein VPN ohne große »Reibungsverluste« einzuführen, empfiehlt sich deshalb die Beachtung einiger Randbedingungen:

- Die existierenden Standards sollten beachtet werden, d.h., man sollte nur IPSec mit IKE-Schlüsselaustausch benutzen. Wenn alle Stricke reißen, kann bei kleineren VPN-Lösungen ein Pre-Shared Key verwendet werden.
- Möglichst alle VPN-Gateways sollten von demselben Hersteller stammen und in derselben Soft- und Hardwareversion betrieben werden.
- Wenn Schwierigkeiten beim Zusammenspiel der VPN-Gateways auftreten, kann als letzte Möglichkeit eine manuelle IPSec-Konfiguration versucht werden. Dabei müssen alle Details wie eingesetzte Algorithmen oder die Security Association fest definiert werden.

Besonders der zweite Punkt ist in der Praxis kaum einzuhalten. Fusionen von Firmen oder die verschlüsselte Übertragung von Geschäftsdaten zwischen Kooperationspartnern führen zur Nutzung unterschiedlicher Hard- und Software. Hier muss in den meisten Fällen auf die (leider nicht sehr komfortable) Minimallösung »IPSec mit Pre-Shared Key« zurückgegriffen werden.

Nachfolgend werden zwei praktische Beispiele für die Einrichtung von VPNs gegeben. Zuerst wird ein VPN-Gateway auf Linux-Basis vorgestellt, als zweite Lösung kommt eine Firewall vom Typ »Checkpoint Firewall-1« in der Version 4.x mit integriertem VPN-Gateway zum Zuge.

7.2.1 FreeSWAN unter Linux

Zum Umfang einer normalen Linux-Distribution gehört das Freeware-Paket »FreeSWAN«, mit dem ein VPN mittels IPSec aufgebaut werden kann. Im Folgenden soll Schritt für Schritt gezeigt werden, wie ein VPN unter der »SuSE«-Distribution eingerichtet wird.

Installation

IPSec benötigt einen Kernel, der das Protokoll unterstützt. Da die neueren Versionen von Linux diese Option per Default aktiviert haben, erübrigt sich die Neukompilation des Kernels mit gesetzten IPSec-Optionen in den meisten Fällen. Mit dem YAST-Installationsprogramm wird zunächst auf allen beteiligten Rechnern die »FreeSWAN«-Software installiert. Anschließend muss (wieder mit dem YAST) die Startvariable START_IPSEC auf den Wert »yes« gesetzt werden. Damit wird das VPN bei jedem Neustart des Rechners ebenfalls gestartet.

Manuell kann IPSec jederzeit mit den folgenden Befehlen hoch- und heruntergefahren werden:

```
ipsec setup --start
ipsec setup --stop
```

Bei gestartetem IPSec ist ein neues Gerät *ipseco* hinzugefügt worden:

```
# ifconfig ipsec0
ipsec0Link encap:Point-to-Point Protocol
inet addr:149.209.1.241  Mask:255.255.255.255
UP RUNNING NOARP  MTU:16260  Metric:1
...
```

Der aktuelle Status von FreeSWAN kann mit dem Kommando

```
ipsec look
```

eingesehen werden.

Konfiguration

Im Verzeichnis */etc* befinden sich zwei Konfigurationsdateien, in denen alle Einstellungen des VPNs angegeben werden:

- Die allgemeine Konfiguration von FreeSWAN wird in der Datei */etc/ipsec.conf* vorgenommen.
- Die Datei */etc/ipsec.secrets* enthält Schlüsselinformationen.

Um unser Beispiel möglichst einfach zu halten, soll ein Pre-Shared Key zum Einsatz kommen.

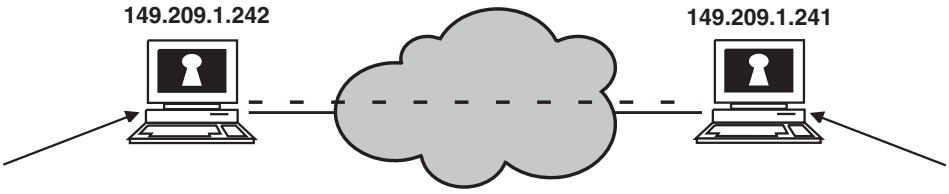


Abb. 7.5: Beispielkonfiguration

Die Konfiguration FreeSWAN geschieht sehr anschaulich über einen »linken« und »rechten« Rechner, wie in Abb. 7.5 angegeben. Bei beiden Rechnern soll die Netzwerkkarte eth0 für das VPN-Gateway genutzt werden.

Die Konfigurationsdateien */etc/ipsec.conf* auf beiden Seiten enthalten in unserem Beispiel die Einträge

```
# basic configuration
config setup
   interfaces="ipsec0=eth0"
   klipsdebug=none
   plutodebug=none
   plutoload="vpn1"
   plutostart="vpn1"
   uniqueids=yes
conn %default
   #authby=rsasig
   #leftrsasigkey=%dns
   #rightrsasigkey=%dns
conn vpn1
   left=149.209.1.242
   leftnexthop=
   right=149.209.1.241
   rightnexthop=
   auto=add
```

Die Schlüsseldatei */etc/ipsec.secrets* enthält auf beiden Seiten einen Pre-Shared Key (PSK).

```
149.209.1.242 149.209.1.241: PSK "1x9presharedkey9a5"
```

Wenn jetzt auf beiden Seiten das VPN gestartet wird (eventuelle Fehlermeldungen in */var/log/messages* beachten!), sollte ein »Ping« zwischen den Rechnern zu den IPSec-Paketen in Abbildung 7.6 führen – hier aufgenommen mit dem Netzwerksniffer »Ethereal«.

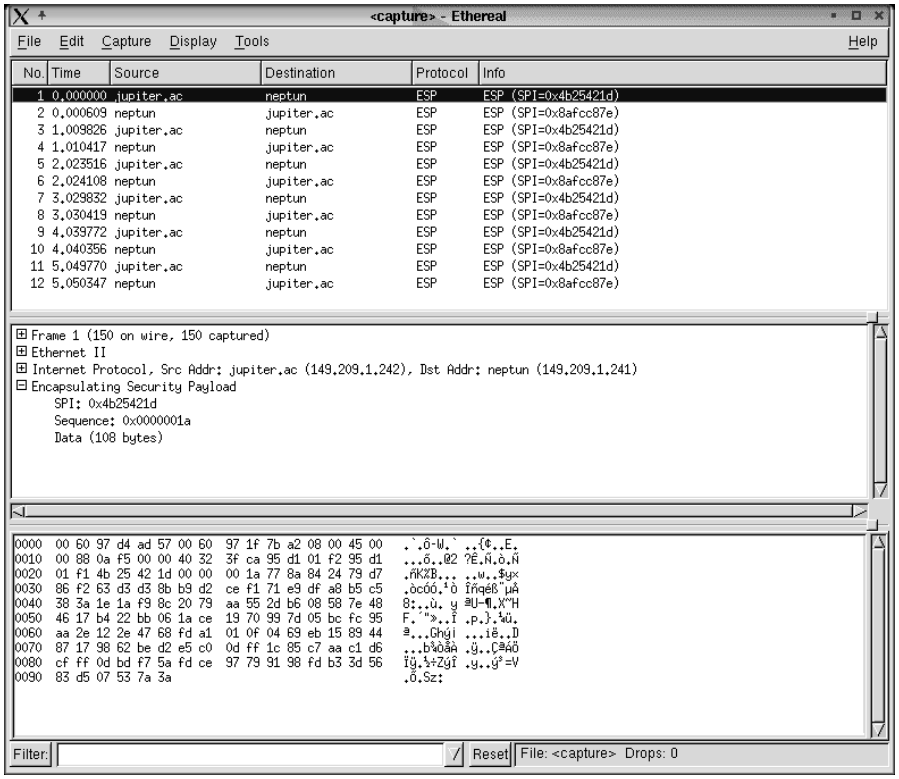


Abb. 7.6: Ping über IPSec

7.2.2 Checkpoint Firewall-1

Im zweiten Beispiel soll ein VPN über zwei NT-Rechner aufgebaut werden. In unserem Beispiel gehen wir von einer Default-Installation von CD aus. Benötigt wird dabei eine »Firewall-1/VPN-1«. Diese Software verfügt über eine ganze Reihe von Verfahren zur Verschlüsselung und zum Schlüsselaustausch, wir beschränken uns wieder auf IPSec mit IKE (siehe auch /LEU01/).

Da das VPN-Gateway in die Firewall integriert ist, muss zunächst die Konfiguration der Firewall durchgeführt werden. Das soll im Folgenden für den »rechten« Rechner in Abbildung 7.5 gezeigt werden, der andere Rechner wird anschließend analog konfiguriert.

Definition der beteiligten Firewalls

Als Erstes wird der eigene Rechner definiert. Wie in Abbildung 7.7 angegeben, muss dieser Rechner als internes Gateway und Management Station definiert werden.

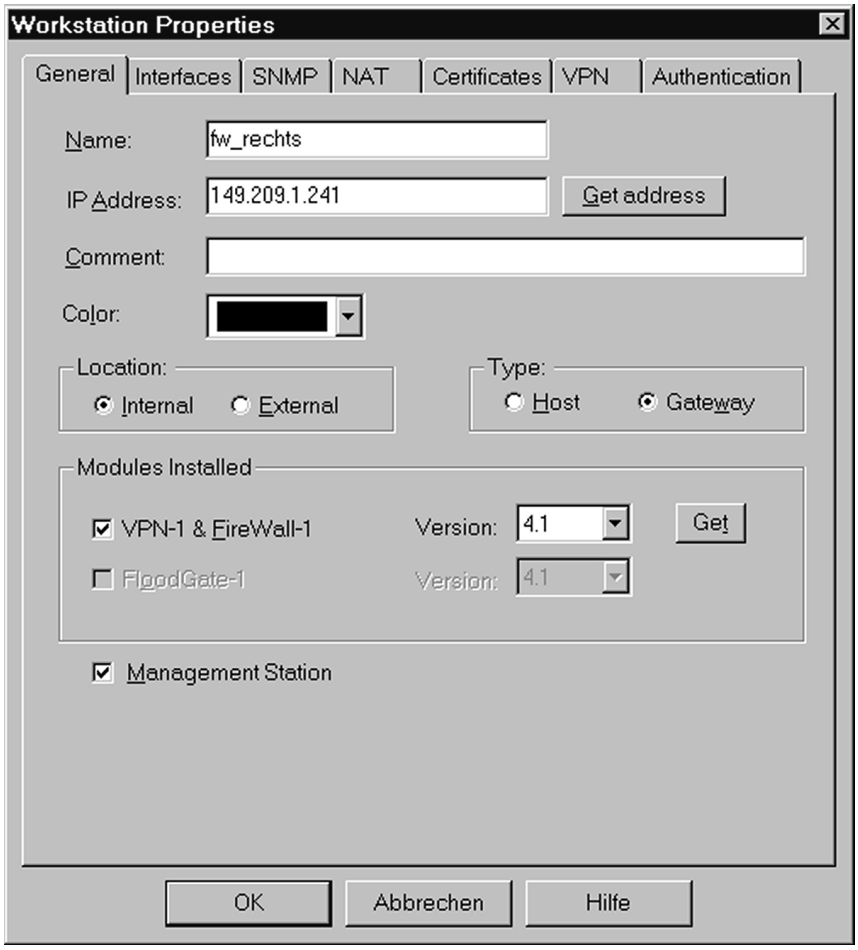


Abb. 7.7: Definition der rechten Firewall

Bei der Konfiguration der Netzwerkkarten (»Interfaces«) ist darauf zu achten, dass Maßnahmen gegen IP-Spoofing getroffen werden (Abb. 7.8). Diese Grundregel gilt natürlich für alle Firewall-Systeme.

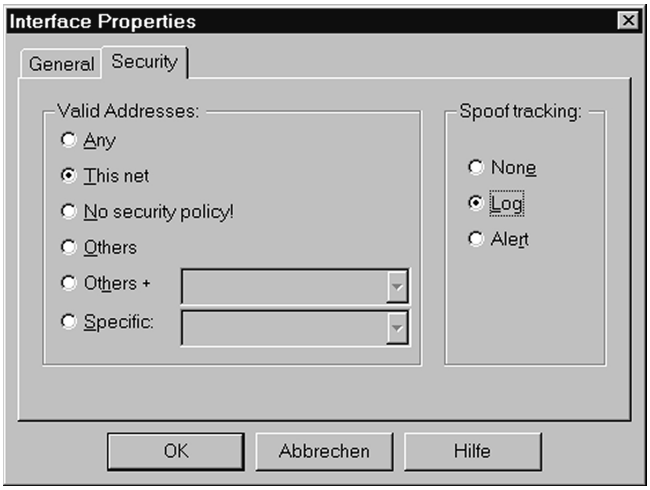


Abb. 7.8: Anti-Spoofing-Optionen

Die zweite Firewall wird als externes Gateway definiert (Abb. 7.9).

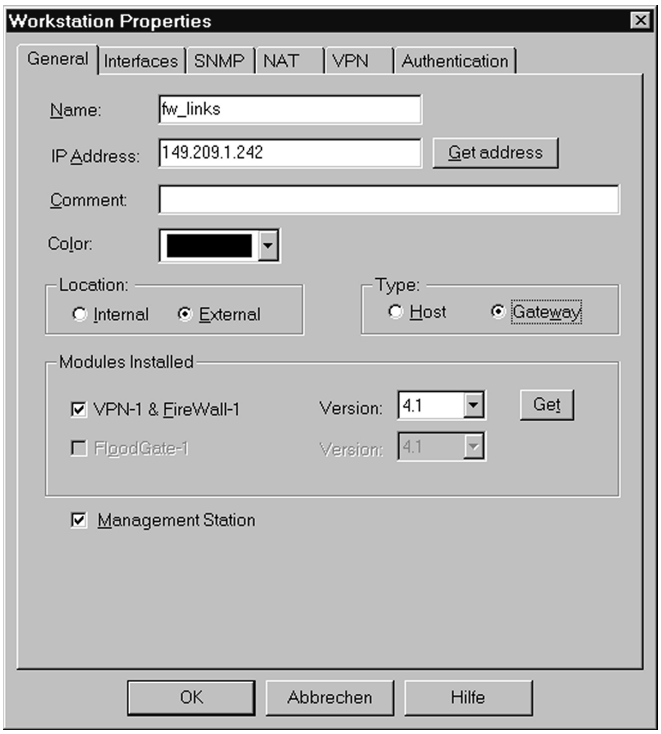


Abb. 7.9: Definition der linken Firewall

Definition der Netzwerke

Anschließend müssen die beteiligten lokalen Netzwerke definiert werden: das eigene Netz als »intern«, das gegenüberliegende Netz als »extern«.

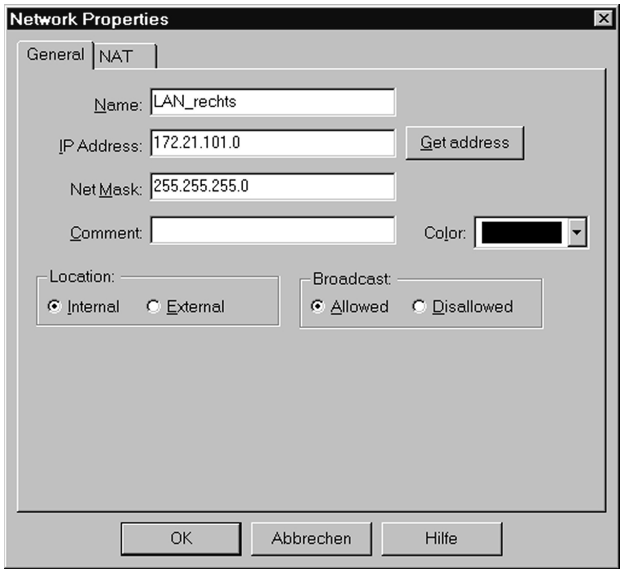


Abb. 7.10: Eigenes Netz

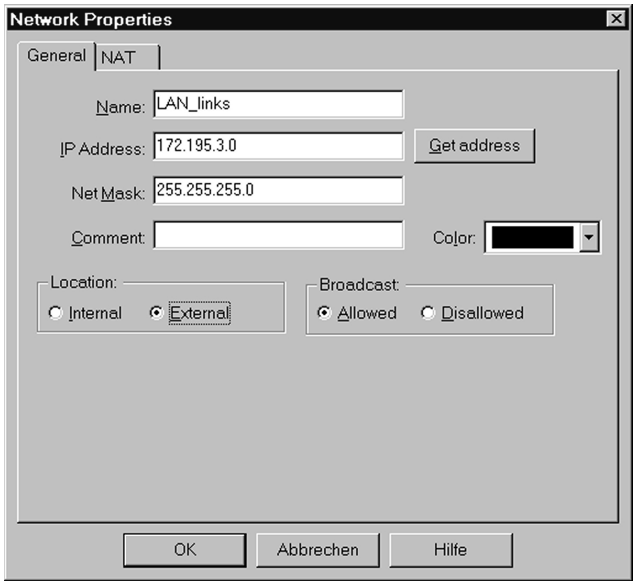


Abb. 7.11: Gegenüberliegendes Netz

Damit ist die Firewall-Konfiguration ohne VPN abgeschlossen. Hier empfiehlt sich ein Test mit der Firewall-Regel »Any Any Accept«. Ist dieser erfolgreich, kann die Konfiguration des VPN-Gateways durchgeführt werden.

Konfiguration von IPSec mit IKE

Nach der Definition der beteiligten Netzwerk-Komponenten kann nun das VPN-Gateway aktiviert werden. Das geschieht über die Konfigurationsmenüs der Firewalls. Dabei werden bei beiden Firewalls die Option IKE und die Verschlüsselungsdomäne des zu der Firewall gehörenden Netzwerks ausgewählt. Bei den Eigenschaften von IKE können dann Algorithmen und die Option »Pre-Shared Secret« (= Pre-Shared Key) ausgewählt werden. Beim Editieren der ersten Firewall kann der Key noch nicht angegeben werden, das ist erst im Menü der zweiten Firewall möglich.

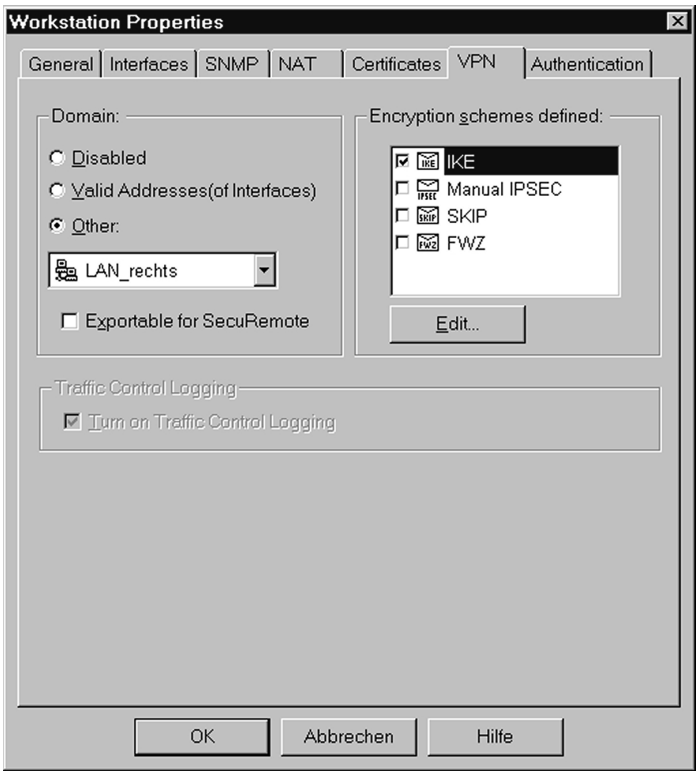


Abb. 7.12: Rechtes VPN-Gateway

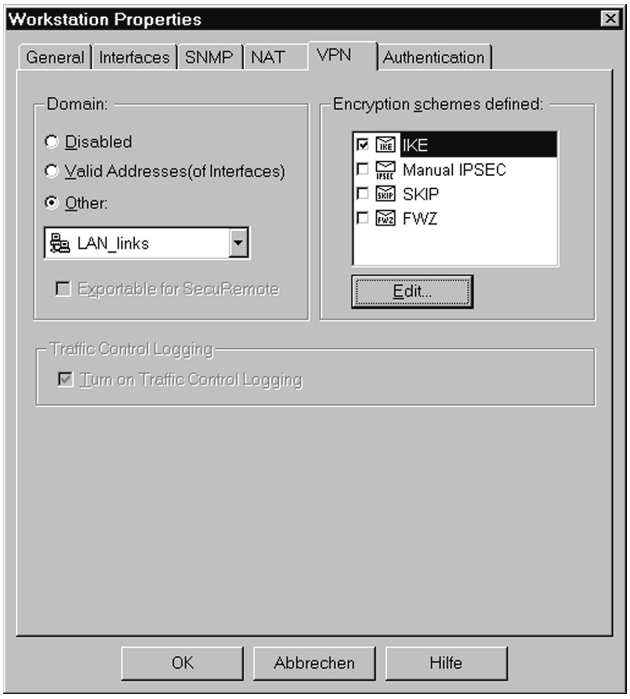


Abb. 7.13: Linkes VPN-Gateway

Abb. 7.14: Eigenschaften von IKE

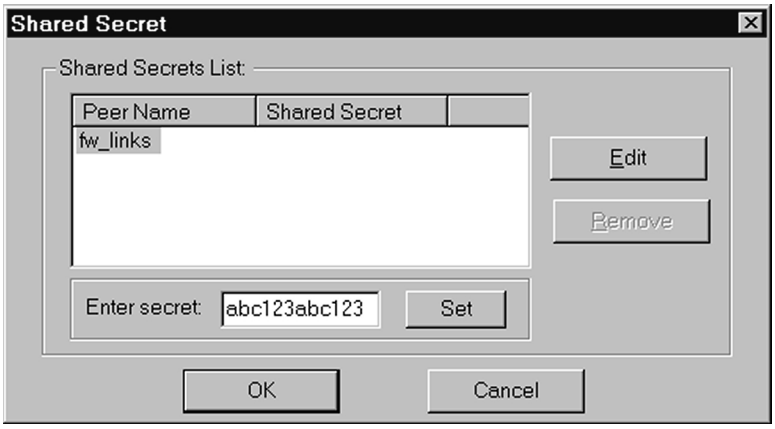


Abb. 7.15: Definition des Pre-Shared Keys

Damit ist die Konfiguration der Firewall-Objekte abgeschlossen.

Filterregeln für das VPN-Gateway

Auch die Definition der Filterregeln für das VPN-Gateway ist ein komplexer Vorgang. Insgesamt sind fünf Regeln zu definieren, die in Abbildung 7.16 angegeben sind:

- Regel 1 erlaubt als Kommunikation zwischen den beiden Firewalls ausschließlich die Dienste IKE, AH und ESP. Damit wird das IPSec-Protokoll zwischen den Endpunkten der VPN-Strecke zugelassen.
- Regel 2 verwirft alle anderen Pakete, die von außen auf das VPN-Gateway treffen.
- Die Regeln drei und vier beschreiben die Kommunikation zwischen den beiden hinter den Gateways liegenden lokalen Netzwerken. Hier muss »Encrypt« angegeben werden, um IPSec auch wirklich zu nutzen.
- Regel fünf ist ein »Any Any Drop«, allerdings im Gegensatz zu der impliziten letzten Regel »Any Any Drop« mit ausführlicher Protokollierung.

Zu guter Letzt müssen noch die Eigenschaften der beiden »Encrypt«-Einträge angepasst werden. Dabei sollte als »Allowed Peer Gateway« die gegenüberliegende Firewall angegeben werden (Abb. 7.17).

Dieselben Arbeiten müssen spiegelbildlich auf der anderen Firewall durchgeführt werden. Anschließend steht der verschlüsselten Kommunikation der beiden Netzwerke nichts mehr im Weg. Eine Beobachtung der Logbuch-Einträge der »Firewall-1« führt bei Fehlern meist schnell auf die richtige Spur.

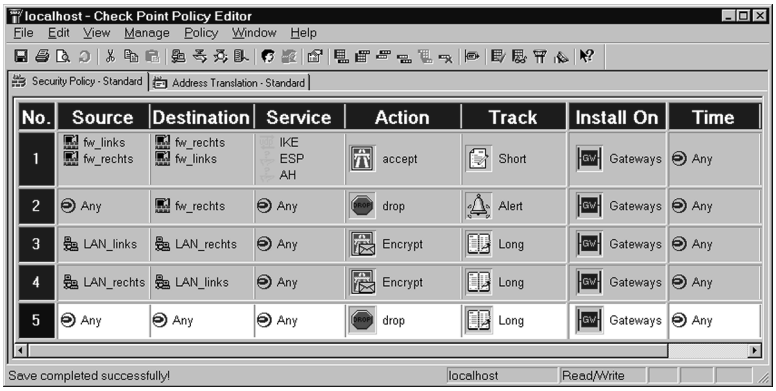


Abb. 7.16: Filterregeln für das rechte VPN-Gateway

Abb. 7.17: Weitere IKE-Eigenschaften

Kapitel 8

VPNs für E- und M-Business

Der große Vorteil von VPNs ist die Flexibilität in der Absicherung ganz unterschiedlicher Protokolle und Applikationen. Wegen der Sicherheitsfunktionen auf IP-Ebene brauchen sich Programmierer, Anbieter von Produkten und Dienstleistungen sowie Anwender keine Gedanken über die Sicherheit der Verbindung zu machen. Hacker haben beim Einsatz sicherer Verfahren mit genügend großen Schlüssellängen keine Chance.

8.1 Geschäftsabwicklung über Netzwerke

Öffentliche Netze, insbesondere das Internet, haben eine zentrale Bedeutung im Leben jedes Einzelnen gewonnen. Einkäufe, Reisebuchungen und andere finanzielle Transaktionen sind dabei im Zentrum des Interesses. Die Stichworte »E-Business« und »M-Business« stehen für die neue Flexibilität bei der Abwicklung von Geschäften. Der Begriff E-Business bezeichnet ganz allgemein die Abwicklung von geschäftlichen Transaktionen über öffentliche Netzwerke, M-Business bedeutet hingegen die Durchführung dieser Vorgänge über das Mobilfunknetz mittels Mobiltelefon oder Communicator (Abb. 8.1).

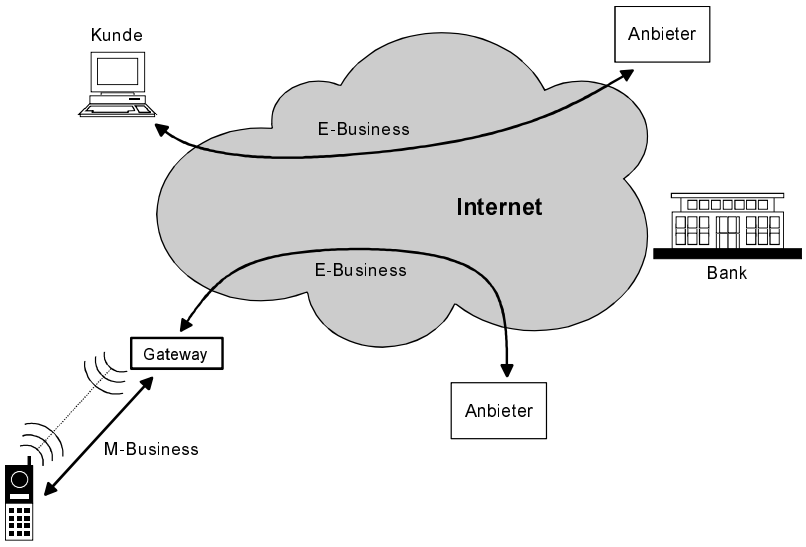


Abb. 8.1: E- und M-Business

Das Thema Sicherheit ist ein zentrales Element innerhalb der benötigten Infrastruktur. Authentikation, Verschlüsselung, digitale Signatur und die damit verbundene juristische Beweisbarkeit von Transaktionen sind Anforderungen, zu deren Erfüllung von technischer Seite her VPNs hervorragend geeignet sind.

- Im Bereich des E- und M-Commerce (elektronischer Handel) können VPNs die bei Angeboten, Bestellungen und finanziellen Transaktionen ausgetauschten Daten sichern.
- ASP (Application Service Provider) bieten komplette Rechenzentrums-Infrastrukturen inklusive der benötigten Software-Lizenzen an. Der Zugriff erfolgt über das Internet. Die zwischen Kunden und ASP ausgetauschten Daten können durch ein VPN gesichert werden.
- Der weitere Ausbau von B2B-Infrastrukturen (»Business to Business«), z. B. zwischen Zulieferern und Fertigungsbetrieben, verlagert sich auf öffentliche Netze mit Absicherung durch VPNs. Auch elektronische Marktplätze wie Auktionshäuser können durch temporäre VPNs abgesichert werden, die alle an der Geschäftsabwicklung beteiligten Gruppierungen verbinden.

Heutige Systeme zum E-Commerce arbeiten aus der Sicht des Endkunden nach einem recht starren Schema: Der Kunde verbindet sich über seinen Client mit einem Web-Server. Diese Verbindung wird über ein gesichertes Protokoll vor unberechtigten Zugriffen geschützt. Mit der Auswahl bestimmter Menüpunkte auf den Web-Seiten werden die Transaktionen initiiert. Praktisch die gesamte »Intelligenz« der Verarbeitung liegt auf der Server-Seite, eine VPN-Infrastruktur besteht nicht.

Mit der VPN-Technologie wäre im Internet eine Vereinheitlichung ungeahnten Ausmaßes möglich. Durch den großflächigen Einsatz von Protokollen wie IPSec auch bei Privatnutzern könnte eine Sicherheit bei der Kommunikation über das Internet erzielt werden, wie sie heute kaum vorstellbar erscheint.

Dabei wird auch mittelfristig die Abgrenzung von VPN-Strukturen und anderen Sicherheitsmechanismen durch das Verhältnis zwischen den Kommunikationspartnern definiert. Ein VPN kommt zum Einsatz, wenn mehrfache oder sogar permanente Kommunikation zwischen beiden den Aufbau und Betrieb einer VPN-Infrastruktur rechtfertigt. Bei gelegentlichen Zugriffen, die zudem mehr oder weniger anonym sind (z. B. Einkauf im Internet), lohnt sich der Aufwand für ein VPN hingegen nicht.

8.2 Risiken von E- und M-Business ohne VPN

8.2.1 Internet-Zugang über PC

Die meisten Benutzer wickeln ihre Online-Geschäfte mit einem herkömmlichen Web-Browser ab. Als Kommunikationsprotokoll dient dabei fast immer SSL. SSL unterstützt neben der Authentikation des Servers auch die des Clients. Das wird

aber nur in den seltensten Fällen (etwa durch SmartCards) realisiert, meist beweist nur der Server seine Identität. Damit sind Angriffe gegen SSL möglich, wenn der Angreifer sich in die Netzwerkverbindung des Kunden einklinken kann (»Man in the Middle«). Das soll am Beispiel eines lokalen Netzwerks beschrieben werden, von dem aus ein Benutzer Online-Banking durchführen möchte. Unter der Voraussetzung, dass sich der Angreifer im gleichen lokalen Netzwerk befindet, kann er folgendermaßen vorgehen:

- Falls sich ein Switch zwischen dem Hacker und dem Opfer befindet, wird der Rechner des Opfers mit einem gezielten Netzwerkpaket (»ARP-Spoofing«) dazu veranlasst, den Zugang ins Internet über den Rechner des Angreifers umzuleiten. Er sendet ab sofort alle Netzwerkpakete an den »Angreifer-PC«, dieser leitet sie ins Internet weiter.
- Um mit dem Browser auf den Server seiner Bank zugreifen, stellt der »Opfer-PC« eine DNS-Anfrage nach dessen IP-Adresse. Diese Anfrage passiert zunächst den Angreifer, der sie mit seiner eigenen IP-Adresse beantwortet (»DNS-Spoofing«). Ab jetzt werden Pakete an die Bank explizit an den Hacker gerichtet, der sie zunächst unverändert weiterleitet.
- Wird nun die SSL-Verbindung aufgebaut, präsentiert der Angreifer ein zuvor erzeugtes SSL-Serverzertifikat, das er selbst unterschrieben hat (»Root-Zertifikat«). Der Benutzer wird von seinem Browser aufgefordert, das Zertifikat zu akzeptieren. Tut er das, wird eine SSL-Verbindung zwischen dem Opfer und dem Hacker aufgebaut.
- Der Hacker baut dann eine zweite SSL-Verbindung mit der Bank auf. Ohne Client-Authentikation ist das ohne Schwierigkeiten möglich. Alle Daten der Verbindung können abgehört und nach Belieben manipuliert werden.

Ein zusätzliches Risiko sind die Schwächen des bei der SSL-Verschlüsselung hauptsächlich eingesetzten schwachen RC4-Algorithmus, der (zumindest in der Theorie) für Angreifer kein unüberwindbares Hindernis darstellt.

8.2.2 Kommunikation über Mobiltelefon

Mit der zunehmenden Mobilität in unserer Gesellschaft müssen auch immer mehr Geschäftsprozesse von unterwegs erledigt werden, z. B. über Mobiltelefone. Das Bezahlen von Waren über Tastenkombinationen auf dem Telefon ist längst keine Zukunftsmusik mehr. Allerdings sind in den heutigen Geräten meist keine ausreichend sicheren Algorithmen implementiert. Authentikation und Verschlüsselung sind zwar vorhanden, doch die proprietären Algorithmen A8 (Schlüsselaustausch), A5 (Verschlüsselung) und A3 (Authentikation) arbeiten mit dermaßen geringen Schlüssellängen, dass A5 »geknackt« ist und die anderen als stark gefährdet gelten (/Schmi02/). Erst UMTS bietet durch seine wesentlich größere Bandbreite und die Auswahl besserer Algorithmen eine passable Sicherheit.

Interessanterweise wird in der mobilen Telefonie einzig die Client-Authentikation über die SIM-Karte des Telefons genutzt, der Zugangspunkt braucht seine Identität nicht nachzuweisen. Angreifer können also eine eigene Sendestation in die Nähe des Opfers stellen, dessen Telefon sich dort einloggen lassen und die gesamte Kommunikation als »Man in the Middle« abhören und manipulieren.

Beim Versand von SMS-Nachrichten fehlt die Authentikation sogar ganz, so dass das Fälschen (»Spoofing«) von Nachrichten über allgemein zugängliche Seiten im Internet problemlos möglich ist. Das unbefugte Mitlesen von SMS-Nachrichten wird durch deren Zwischenspeicherung auf Servern des Netzwerkbetreibers erleichtert.

Sollen Mobiltelefone für sichere Kommunikation genutzt werden, muss deshalb auf proprietäre Lösungen ausgewichen werden. Einige Spezialhersteller bieten SIM-Karten an, bei denen auf Hardwareebene eine starke Verschlüsselung implementiert ist. Die Kommunikation zweier Mobiltelefone, die beide mit SIM-Karten desselben Anbieters bestückt sind, können dann eine End-to-End-Security aufbauen. Nur dann haben Angreifer bei Zugriffen auf die vertraulichen Nutzdaten keine Chance.

8.2.3 Internet-Zugang über Mobiltelefon

Eine mobile Alternative zum PC ist der Zugang ins Internet über das Mobiltelefon. Dabei ist nicht der Einsatz als Modem für einen Laptop gemeint, sondern der direkte Zugriff über das WAP-Protokoll. Wird das Telefon als Modem eingesetzt, gelten die Überlegungen für den Internet-Zugang für PCs.

Bei der in den meisten Mobiltelefonen implementierten WAP-Version 1.x wird zwischen dem Mobiltelefon und dem WAP-Gateway beim Mobilfunk-Betreiber die aus dem SSL-Standard abgeleitete Protokollschicht WTLS eingesetzt. Zur Kommunikation zwischen dem WAP-Gateway und dem eigentlichen WAP-Server mit der Applikation ist eine Konvertierung von WTLS in das IP-basierte SSL-Protokoll nötig. Hier entsteht eine temporäre Sicherheitslücke, da die Daten auf dem Gateway für einen gewissen Zeitraum unverschlüsselt vorliegen. Dazu kommen die bei WAP 1.x eingesetzten geringen Schlüssellängen von 40 Bit und weniger, die Angriffe wesentlich erleichtern.

Die Probleme der Konvertierung am Gateway und der geringen Schlüssellängen wurden in der WAP-Version 2.0 angegangen. Hier kommen bis zu 1 024 Bit zum Zuge, so dass die Sicherheit zumindest nicht geringer ist als bei der Arbeit mit dem PC.

8.2.4 Fazit

Im Gegensatz zur internen Kommunikation bei Firmen und Behörden werden im Verhältnis zwischen Endkunden und Anbietern die im Vergleich zu einem VPN weniger sicheren Client-Server-Protokolle WTLS und SSL eingesetzt. Es ist deshalb nötig, dass in der Zukunft mehr und mehr »Intelligenz« auf den Client des Endkunden verlagert wird, so dass auch hier die Mechanismen eines VPN zum Einsatz kommen können. Das setzt allerdings eine drastische Steigerung der Leistungsfähigkeit der Endgeräte voraus, kompakte Bauweise und lange Standby-Zeit sind dann nicht mehr die maßgeblichen Design-Kriterien. Im Mobilfunkbereich ist mit dem neuen Übertragungsstandard UMTS als Ersatz für GSM wegen der dann endlich passablen Bandbreite in einigen Jahren mit einem Boom im M-Commerce zu rechnen.

8.3 VPN-Systeme zum E-Commerce

An der Verarbeitung einer Transaktion sind im Normalfall mehrere Institutionen beteiligt. Der Anbieter einer kostenpflichtigen Leistung arbeitet mit einem Provider (beispielsweise einer Bank) zusammen, der in seinem Namen das Geld vom Kunden einzieht. Außerdem ist die Bank des Kunden am Geschäft beteiligt. Es ist sinnvoll, zwischen diesen Parteien ein oder mehrere Business-to-Business-VPNs (»B2B-VPNs«) einzurichten. Die Abbildungen 8.2 und 8.3 geben Implementierungs-Beispiele für einen SSL-Zugriff über das Internet und für einen WAP/WTLS-Zugriff mittels Mobiltelefon.

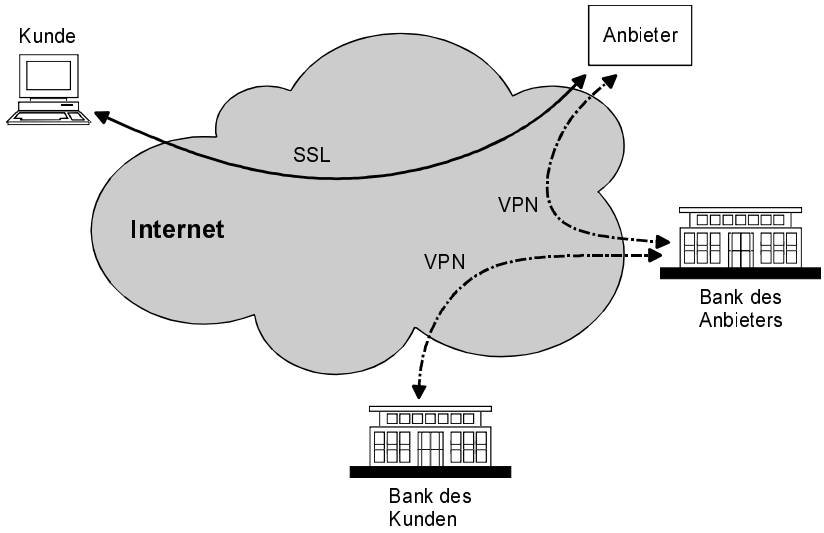


Abb. 8.2: SSL und VPN

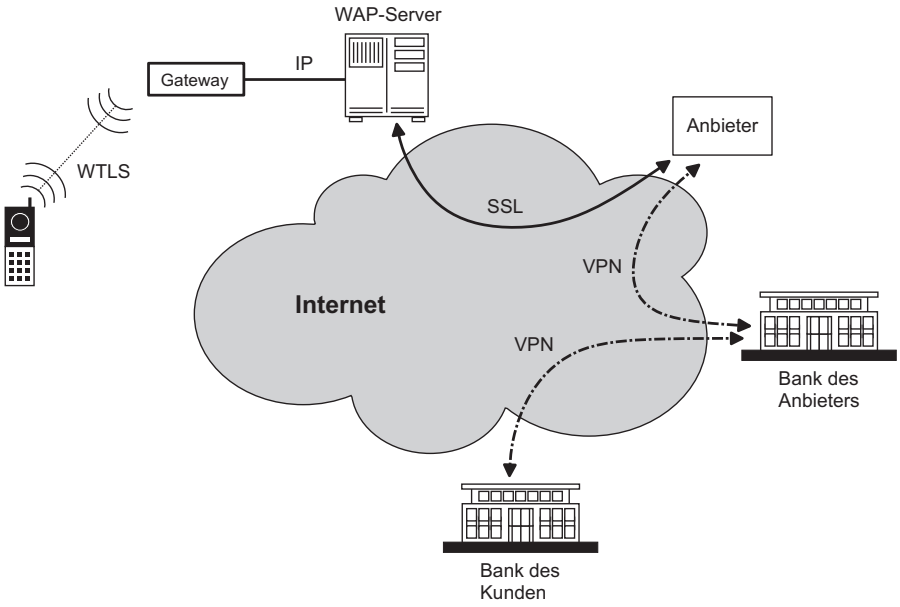


Abb. 8.3: WAP und VPN

8.4 Das »Jedermann-VPN«

Mit der zu erwartenden Verbreitung des E-Business auch für Endkunden muss immer mehr der beim Geschäftsvorgang benötigten »Intelligenz« auf den Client des Kunden verlagert werden. Angebote müssen beispielsweise automatisch recherchiert, mit den Wünschen des Interessenten verglichen und in einer Vorauswahl gegenübergestellt werden. Die dann benötigte Flexibilität im Umgang mit Zertifikaten, Internet-Protokollen und den dazugehörigen Anwendungen lässt eine Migration hin zu einem »echten« VPN erwarten, an dem der Endkunde über seinen Internet-Provider partizipiert. Die Kopplung der beteiligten Rechner zu einem VPN wäre dabei nur temporär und auf einen Geschäftsvorgang beschränkt. Auch Privatleute untereinander könnten für einen Datenaustausch auf die Online-Sicherungsmechanismen von VPNs setzen (Abb. 8.4).

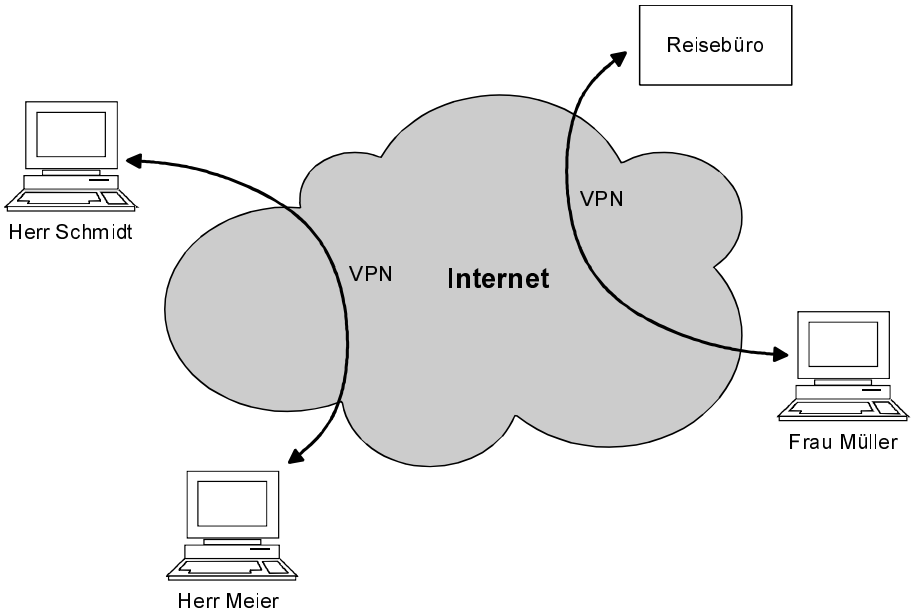


Abb. 8.4: Temporäre VPNs für den privaten Gebrauch

8.5 Protokolle im E- und M-Business

Da es noch auf absehbare Zeit eine Koexistenz zwischen WTLS, SSL und den allgemeineren VPNs geben wird, wird an dieser Stelle ein kurzer Überblick über die in diesem Buch bisher noch nicht behandelten Protokolle gegeben. Die Absicherung von öffentlichen Schlüsseln geschieht bei ihnen völlig identisch zu den bisher beschriebenen Mechanismen, so dass bei Bedarf dieselbe Infrastruktur aus CAs und RAs genutzt werden kann.

Ein immer wichtiger werdendes Protokoll im E-Business ist SET, mit dem ein bargeldloser Zahlungsverkehr über unsichere Netze implementiert werden kann. SET ist – im Gegensatz zu den innerhalb des Netzwerkstacks angesiedelten SSL und WTLS – innerhalb des Protokollstacks auf der Applikationsebene angesiedelt. Alle drei Protokolle liefern eine sichere Verbindung für ganz bestimmte Anwendungen. Sie kommen immer dann zum Einsatz, wenn ein »festes« VPN nicht erwünscht oder nicht praktikabel ist, wie zum Beispiel in einer losen Kunden-Händler-Relation. In einer Gesamtlösung, die auch den internen Netzwerkverkehr der Händler und der Banken mit seinem hohen Sicherheitsbedarf berücksichtigt, kommt es dann zu einer Koexistenz eines oder mehrerer VPNs mit den anderen Sicherheits-Protokollen.

8.5.1 Secure Socket Layer (SSL)

Das von Netscape entwickelte Protokoll SSL wird auch TLS (Transport Layer Security) bezeichnet. Es setzt auf der Transportschicht des Netzwerk-Stacks auf. Prinzipiell könnte es mit jedem Protokoll dieser Ebene kooperieren, doch in der Praxis sind nur Implementierungen für TCP bekannt.

SSL nimmt alle für Authentizität, Vertraulichkeit und Unversehrtheit der Daten benötigten Aufgaben wahr. Dazu verhandeln Client und Server über Algorithmen zur Datenkompression, Verschlüsselung und digitalen Signatur. Basis dieser »Vorverhandlungen« sind öffentliche Schlüssel des Servers und optional des Clients, die mithilfe von Zertifikaten von Zertifizierungsinstanzen (Certification Authorities, CAs) bestätigt werden. Wie bei VPNs werden langsame asymmetrische Private/Public-Key-Algorithmen mit symmetrischen Verfahren kombiniert.

Beschreibung des Verfahrens

SSL ist ein zustandsbehaftetes Protokoll. Mit ihm können zwischen zwei Rechnern ein oder mehrere Sitzungen aufgebaut werden, die ihrerseits jeweils eine oder mehrere Verbindungen enthalten können. Die Nutzdaten werden vor dem Senden fragmentiert, komprimiert, um eine digitale Signatur ergänzt und verschlüsselt. Der Empfänger kehrt die Reihenfolge der Operationen um und führt die Nutzdaten der nächsthöheren Ebene des Netzwerkstacks zu. Diese Aufgaben werden im SSL Record Layer wahrgenommen.

Zusätzlich zu diesem transparenten Teil setzen drei weitere Protokolle auf dem SSL Record Protocol auf, die aber nicht in höhere Schichten übermittelt werden (Abb. 8.5):

- Das *SSL Handshake Protocol* nimmt interne SSL-Kommunikations- und Verwaltungsaufgaben auf den beteiligten Rechnern wahr, wie etwa die (gegenseitige) Authentikation oder die Wahl des Verschlüsselungsverfahrens.
- Das *»change cipher spec«-Protokoll* teilt dem Partner den Wechsel in den zuvor ausgehandelten Verschlüsselungsalgorithmus mit. Vom Prinzip her hätte dieses Protokoll in die Familie des SSL Handshakes gehört, doch bestünde dann die Gefahr von Deadlocks.
- Das *Alert Protocol* schließlich wird im Fehlerfall aktiv.

Zum Austausch von Schlüsseln während des Handshakes stehen die Verfahren RSA, Diffie-Hellman und Fortezza zur Verfügung.

Die SSL-Kommunikation wird über reservierte TCP/IP-Ports abgewickelt:

- Port 443 lässt SSL-Verbindungen zu Webservern zu. Diese Art der Verbindung ist die einzige, die bisher in praktischen Implementierungen realisiert ist.
- Port 465 ist für SSL in Verbindung mit dem E-Mail-Protokoll SMTP reserviert.
- Port 563 schließlich ist für SSL in Verbindung mit Newsgroups reserviert.

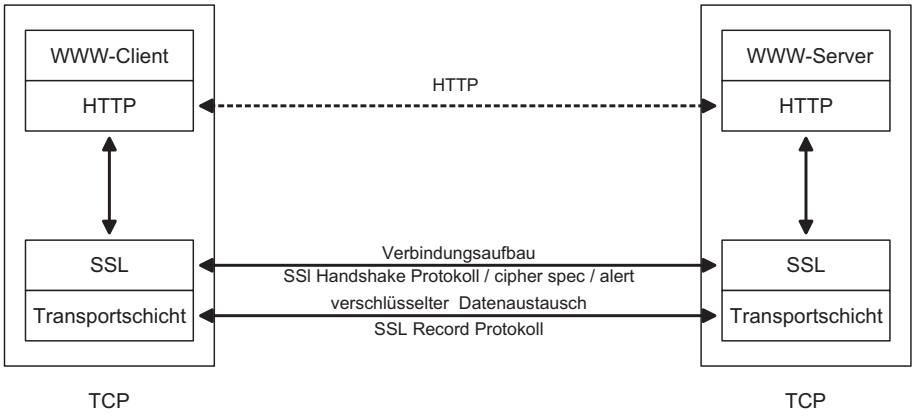


Abb. 8.5: Das Prinzip von SSL

Hier zeigt sich der Unterschied zwischen SSL und einer allgemeinen VPN-Definition: Ein VPN stellt eine für die verschiedenen Applikationen transparente Netzwerkverbindung zwischen beliebigen Netzwerkknoten her. Das sitzungsorientierte SSL ist hingegen nur für bestimmte Client-Server-Applikationen definiert, mit denen die wichtigsten Dienste im Internet abgedeckt werden.

Kryptographische Verfahren

In der aktuellen SSL-Version sind folgende Verfahren zur Verschlüsselung der Daten definiert:

- keine Verschlüsselung
- Stromverschlüsselung nach RC4 mit einer Schlüssellänge von 40 oder 128 Bit, mit allen Risiken und Nebenwirkungen
- Blockverschlüsselung mit CBC nach RC2 (40 oder 128 Bits), DES (40 oder 56 Bits), Triple-DES, IDEA und Fortezza

Für die digitale Signatur stehen folgende Optionen zur Verfügung:

- keine Signatur
- MD5
- SHA-1

Bewertung der Sicherheit

Wird nicht gerade RC4 genutzt, kann SSL als kryptographisch ausreichend abgesichert betrachtet werden. Die Kombination Triple-DES und SHA-1 entspricht dem Stand der Technik, AES wird in kommende Versionen einfließen. Leider handeln Client und Server die eingesetzten Protokolle ohne Einflussmöglichkeit durch den Benutzer aus, so dass RC4 in der Regel nicht vermieden werden kann. Vorsicht ist also geboten.

8.5.2 Wireless Application Protocol (WAP)

Der WAP-Standard wurde vom WAP-Forum für die langsamen Übertragungsraten von Mobiltelefonen definiert. Er stellt einen kompletten Netzwerk-Stack für diese Geräte zur Verfügung. Im Folgenden wird zunächst die heute übliche Version 1 beschrieben, die Neuerungen von WAP 2.0 folgen im Anschluss.

Beschreibung des Verfahrens

Auf der untersten Ebene wird die Verbindung durch den jeweiligen Träger – zum Beispiel GSM – gebildet. Darüber befindet sich die Transportschicht »Wireless Datagram Protocol« (WDP), die eine dem IP-Protokoll analoge Transportfunktion hat. Sie trennt die physikalische Übertragung von der darüber liegenden Sicherungsschicht »Wireless Transport Layer Security« (WTLS). WTLS weist eine große Ähnlichkeit mit SSL auf, im Unterschied zu SSL ist aber zusätzlich eine gesicherte Kommunikation zwischen zwei Clients möglich. Damit können beispielsweise zwei Mobiltelefone Visitenkarten austauschen.

Da das WAP-Protokoll primär für den Client-Server-Einsatz im Internet konzipiert wurde, haben sich die Entwickler für die Integration einer Transaktions-Ebene entschieden (»Wireless Transaction Protocol«, WTP). Damit wurde einer der Hauptnachteile von gewöhnlichen Internet-Verbindungen, das zustandslose HTTP-Protokoll und die damit nur schwer realisierbaren Transaktionen, von vornherein vermieden. Da nicht alle WAP-Zugriffe Transaktionen sind, bietet WTP drei unterschiedliche Dienste an:

- eine nicht abgesicherte Einweg-Anfrage (One Way Request)
- eine abgesicherte Einweg-Anfrage
- eine abgesicherte Zweiwege-Transaktion mit Request und Reply

Alle denkbaren WAP-Zugriffe müssen sich in Abfolgen dieser drei Transaktionen zerlegen lassen.

Der TCP- bzw. UDP-Ebene im IP-Stack entspricht das »Wireless Session Protocol« (WSP), bei dem zwei unterschiedliche Dienste definiert sind:

- Der verbindungsorientierte Dienst nutzt das Transaktions-Protokoll WTP und die darunter liegenden Schichten.
- Der verbindungslose Dienst hingegen greift direkt auf das Datagramm-Protokoll WDP zu.

Als Applikationsebene unter WAP wurde das »Wireless Application Environment« (WAE) definiert, das im Wesentlichen aus der an HTML angelehnten Sprache »Wireless Markup Language« (WML), einem JavaScript-Derivat namens »WMLScript« sowie Telefon-, Kalender- und anderen kleinen Anwendungen besteht.

Abbildung 8.6 verdeutlicht die WAP-Architektur grafisch. Abbildung 8.7 zeigt, wie deren Elemente in der Praxis unterschiedlich zu Netzwerk-Stacks kombiniert werden können. Die Grafik links zeigt, wie ein Benutzer über die Handy-Oberfläche Transaktionen ausführt. In den beiden anderen Grafiken kommunizieren Anwendungen direkt miteinander.

Abbildung 8.7 zeigt auch, dass die höheren Schichten von WAP alternativ über UDP/IP miteinander kommunizieren können. Hier könnte ein Ansatz zu einer Integration der beiden Stacks zu einer dann universell einsetzbaren VPN-Realisierung liegen.

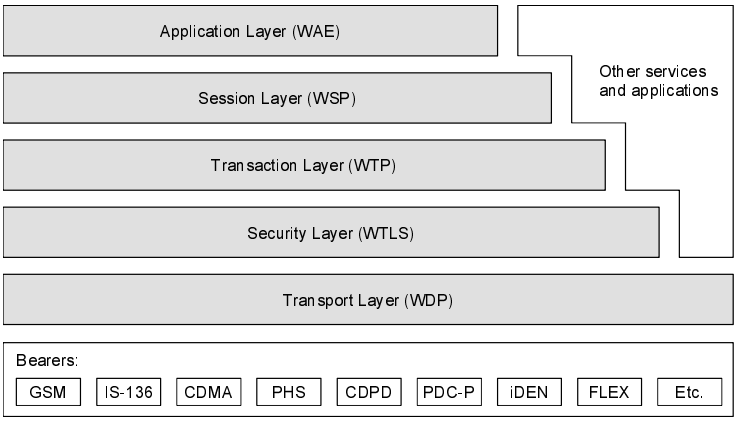


Abb. 8.6: WAP-Architektur

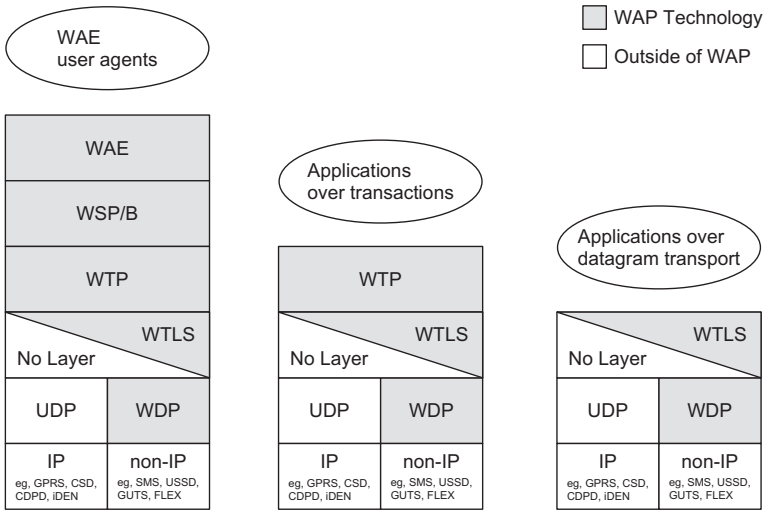


Abb. 8.7: WAP-Stacks

Kryptographische Verfahren

Die kryptographisch abgesicherte Ebene des WAP-Stacks (WTLS) wurde aus SSL abgeleitet. Die in diesem Kapitel beschriebenen Verfahren von SSL kommen im Wesentlichen auch unter WAP zum Einsatz, allerdings in extrem »abgespeckten« Versionen:

- Die Berechnung von Initialisierungs-Vektoren für die Verschlüsselung geschieht nach einem linearen Verfahren, so dass die Vektoren vorhersehbar sind.
- Die DES-Schlüssellänge von 35 Bit ist absolut unzureichend.
- Einer der für die Berechnung von MAC-Hashwerts vorgesehenen Algorithmen führt ein primitives 40 Bit-XOR durch.
- Gegen die gemäß dem Standard PKCS#1 implementierten RSA-Verfahren zur Verschlüsselung und digitalen Signatur hat Daniel Bleichenbacher einen Angriff entwickelt. Aus einer großen Zahl von gesendeten Nachrichten und der Reaktion des Opfers (PKCS#1-kombatibel oder nicht) kann eine Analyse begonnen werden, die deutlich schneller als Brute-Force zum gewünschten Ergebnis führt.
- Die beim Schlüsselaustausch über Diffie-Hellman benutzten Primzahlen haben nur eine Länge von 512 oder 768 Bit.

Bewertung der Sicherheit

WAP 1.x mit WTLS muss aus heutiger Sicht als völlig unzureichend für den Einsatz im M-Business angesehen werden. Wegen der Notwendigkeit der Konvertierung von WTLS in SSL am WAP-Gateway des Providers ist eine End-to-End-Verschlüsselung nicht möglich. Die geringen Schlüssellängen tun ihr Übriges.

Verbesserungen in WAP 2.0

Der Netzwerkstack von WAP 2.0 unterscheidet sich komplett von dem seiner Vorgänger-Versionen. WTLS als Sicherungsschicht wurde komplett gestrichen und durch das herkömmliche SSL (TLS) ersetzt, das seinerseits auf TCP/IP aufsetzt. Die WAP-Gateways wurden durch WAP-Proxies ersetzt, die ein Routing der Pakete unterhalb der SSL-Schicht vornehmen, ohne die verschlüsselten Nutzdaten anzutasten. Damit ist nun auch eine End-to-End-Sicherheit möglich.

Weniger spektakulär sind die eingesetzten Verfahren: RSA mit (nur) 1 024 Bit Schlüssellänge ist im Gespräch, ebenso wie Algorithmen auf Basis von Ellipsen (ECC). Käufer von Geräten sollten sich nicht mit RSA abspeisen lassen, sondern auf dem bisher als “starkes Verfahren” geltenden ECC bestehen.

8.5.3 Secure Electronic Transaction (SET)

Der SET-Standard (Secure Electronic Transaction) soll einen bargeldlosen Zahlungsverkehr über unsichere Netze ermöglichen. Das Verfahren wurde von IBM in Zusammenarbeit mit einigen Kreditkartenfirmen entwickelt. Die bei SET ausgetauschten Protokolle basieren, wie auch bei VPNs, auf der Kombination von symmetrischen und asymmetrischen Verschlüsselungsverfahren, wobei zur Absicherung der öffentlichen Schlüssel Gebrauch von X.509-Zertifikaten gemacht wird.

Bei SET sind fünf Partner involviert:

- Der Kunde, in der Regel der Besitzer einer Kreditkarte, kauft Waren oder Dienstleistungen über das Netz ein.
- Der Händler ist der Gegenpart des Kunden während der Abwicklung des Geschäfts.
- Das Geldinstitut des Kunden berechtigt den Kunden zum Zahlungsverkehr über SET und garantiert die Auszahlung von rechtmäßig angeforderten Beträgen.
- Das Geldinstitut des Händlers nimmt dessen Anforderungen nach Bezahlung an und zieht die entsprechenden Beträge vom Geldinstitut des Kunden ein.
- Das »Payment Gateway« ist ein von Geldinstitut des Händlers oder einer Drittfirma betriebener Rechner mit besonderen Funktionen.

Die Ziele von SET sind die Authentikation des Kunden, des Händlers und seines Geldinstituts sowie die Vertraulichkeit und Unversehrtheit der während des Zahlungsvorgangs ausgetauschten Daten.

Beschreibung des Verfahrens

SET definiert eine Reihe von Transaktionen, die jeweils aus einer ganzen Serie ausgetauschter Protokolle bestehen. Bei einer Transaktion gibt es immer nur zwei Partner, womit sich die Kommunikation der insgesamt fünf beteiligten Seiten in ihrer Komplexität stark reduziert. Folgende Transaktionen sind definiert (Abb. 8.8):

- Die **Registrierung des Kunden** umfasst seine Anmeldung bei einer CA, wobei ihm ein Zertifikat für seinen öffentlichen Schlüssel zur Verfügung gestellt wird.
- Die **Registrierung des Händlers** dient zu seiner Anmeldung bei einer CA, wobei ihm zwei Zertifikate zur Verfügung gestellt werden. Diese sichern seine beiden öffentlichen Schlüssel ab, die zum Schlüsselaustausch beziehungsweise zu seiner digitalen Unterschrift dienen. Neben dem Händler besitzen auch CA und Payment Gateway zwei Schlüsselpaare, der Kunde hingegen nur eins.
- Die **Kaufanforderung** dient zur Bestätigung der Kaufabsicht des Kunden an den Händler.
- Bei der anschließenden **Autorisierung der Zahlung** überprüft der Händler durch Anfrage an das Payment Gateway die Kreditwürdigkeit des Kunden. Bei positivem Bescheid kann er die Waren zum Kunden senden.

- Mit der **Anforderung zum Geldeinzug** setzt der Händler nach Auslieferung der Ware den Mechanismus der Geldüberweisung in Gang. Damit ist aus der Sicht von SET der Vorgang abgeschlossen.

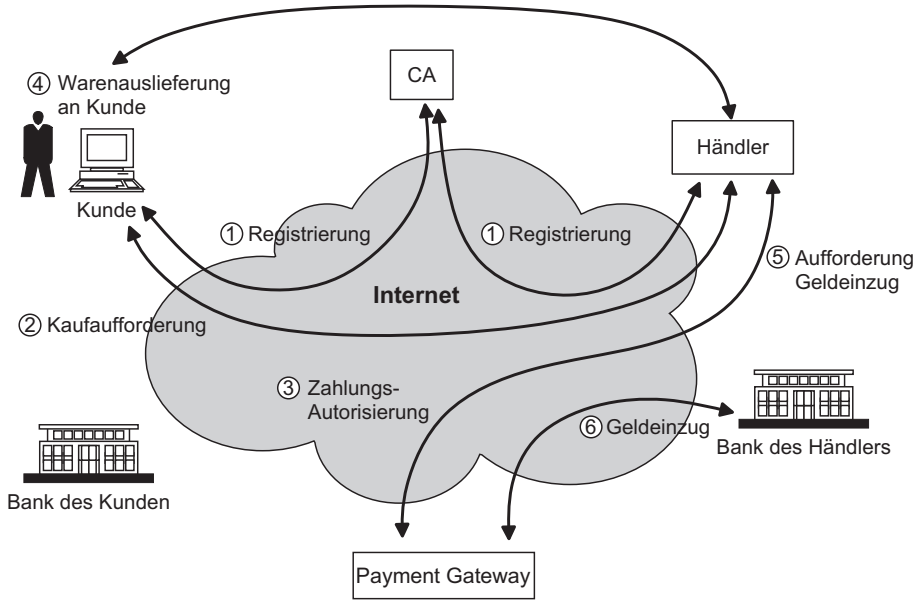


Abb. 8.8: Secure Electronic Transaction (SET)

Kryptographische Verfahren

SET lässt den Programmierern von Applikationen keine Freiheitsgrade in der Auswahl und Ausgestaltung der kryptographischen Algorithmen:

- Bei allen Operationen mit öffentlichen/privaten Schlüsseln wird RSA eingesetzt, meist mit einer Schlüssellänge von nur 1 024 Bit. Einzig bei den Root-CAs, der letzten Instanz in der Kette der Vertrauensverhältnisse der CAs untereinander, wird eine Schlüssellänge von 2 048 Bit eingesetzt.
- Die symmetrische Verschlüsselung wird mittels normalen DES (56 Bit Schlüssellänge) im CBC-Mode geleistet.
- Alle Hash-Werte werden mit SHA-1 gebildet.

Bewertung der Sicherheit

Die bis auf den SHA-1-Hash unzureichenden Schlüssellängen und Verfahren der Version 1 werden im Standard SET 2 optional erweitert. Triple-DES und AES (beide symmetrisch) sowie ECC im Bereich der asymmetrischen Verfahren schaffen dann eine akzeptable Sicherheit.

VPN-Sicherheitspolitik und weitere Sicherheitsmaßnahmen

Ein VPN ist kein Produkt, das »von der Stange« gekauft werden kann und dann automatisch Sicherheit gewährleistet. Unterschiedliche Aspekte müssen berücksichtigt werden, damit mit Hilfe eines VPN das gewünschte Sicherheitsmaß erreicht werden kann. Das VPN muss

- auf einer VPN-Sicherheitspolitik aufbauen,
- in das IT-Sicherheitskonzept der Organisation eingebettet sein,
- korrekt installiert und
- korrekt administriert werden.

In diesem Kapitel wird exemplarisch beschrieben, wie eine VPN-Sicherheitspolitik auszusehen hat und welche Sicherheitsmaßnahmen für den Betrieb eines VPN zusätzlich benötigt werden. Jedoch können Sicherheitsmaßnahmen für eine korrekte Installation oder Administration nicht berücksichtigt werden, weil sie vom jeweils eingesetzten Produkt abhängen. Auch die Einbettung der VPN-Sicherheitspolitik in ein IT-Sicherheitskonzept wird nicht dargestellt, da sie organisationsspezifisch ist /BSI99/.

9.1 VPN-Sicherheitspolitik

Eine VPN-Sicherheitspolitik ist die Voraussetzung für den sicheren Betrieb eines VPN. Ein VPN macht nicht automatisch sicher, sondern mit einem VPN kann die Kommunikation über unsichere Netze sicher gemacht werden. Die Installation eines VPN ohne vorausgehendes Sicherheitskonzept kann zu einem falschen Sicherheitsgefühl führen. Oft wird irrtümlicher weise davon ausgegangen, dass mit der Installation eines VPN alles gesichert sei. Dieser Irrtum wiegt noch schwerer, wenn keine genaue Kenntnis über die vorhandene Netzwerktopologie vorhanden ist. Denn bei Unkenntnis der Netzwerktopologie kann man nicht davon ausgehen, dass nicht doch mehr als eine Verbindung zum Internet oder zu anderen unsicheren Netzen existiert, über die dann die Daten ungesichert übertragen werden.

Die VPN-Sicherheitspolitik orientiert sich am Schutzbedarf der eingesetzten IT-Systeme und muss Teil einer vorhandenen organisationsweiten Sicherheitspolitik sein. Die Festlegung der VPN-Sicherheitspolitik kann auch bestehende Richtlinien und Vorschriften der allgemeinen Sicherheitspolitik betreffen, die dementsprechend mit berücksichtigt werden müssen.

Die VPN-Sicherheitspolitik definiert Sicherheitsziele, die durch den Einsatz eines VPN erfüllt werden sollen, und stellt die zu schützenden Ressourcen dar. Die Kommunikationsanforderungen werden darin festgelegt. Die VPN-Sicherheitspolitik ist wie eine organisationsweite Sicherheitspolitik auf die jeweilige Organisation und den Bereich abgestimmt, zum Beispiel Medizin, Banken, Versicherungen, Energieversorgungs-Unternehmen, Betriebs- oder Personalrat usw. /Pohl97a und Pohl97b/.

9.1.1 Sicherheitsziele

Im ersten Schritt müssen die Sicherheitsziele definiert werden, die mit dem Einsatz eines VPN erreicht werden sollen. Als Richtwerte können folgende Punkte betrachtet werden:

- Vertraulichkeit,
- Authentikation (implizit – über die Verschlüsselung – oder explizit),
- Zugangskontrolle (für Datenpakete oder Benutzer),
- Rechteverwaltung (für Kommunikationsprotokolle und -dienste),
- Beweissicherung und
- Protokollauswertung.

9.2 Zusätzliche Sicherheitsmaßnahmen

Das eigentliche VPN-Produkt besteht aus Soft- und Hardware. Neben dieser technischen Seite müssen weitere Aspekte beachtet werden, damit der sichere Betrieb des VPN garantiert werden kann. Die im folgenden Abschnitt aufgeführten Sicherheitsmaßnahmen gelten auch allgemein für den Einsatz von IT-Systemen und sind in den meisten Organisationen vorhanden. Andere Maßnahmen müssen speziell für den sicheren Betrieb eines VPN umgesetzt werden.

Die zusätzlichen Sicherheitsmaßnahmen gliedern sich in die folgenden Unterpunkte:

- Infrastruktur
- Organisation
- Personal
- Festlegungen für den Notfall

9.2.1 Infrastruktur

Die folgenden infrastrukturellen Sicherheitsmaßnahmen tragen dazu bei, die Sicherheit des VPN-Betriebs zu erhöhen:

Zugangsgesicherter Raum

Sämtliche Komponenten des VPN sollten in abgeschlossenen und zugangsgesicherten Räumen aufgestellt werden, um zu verhindern, dass unberechtigte Personen die technischen Sicherheitsmechanismen manipulieren oder ausschalten.

Unterbrechungsfreie Stromversorgung (USV)

Eine USV sollte installiert werden, um kurzzeitige Stromausfälle zu überbrücken oder die Stromversorgung wenigstens so lange aufrecht zu erhalten, dass ein geordnetes Herunterfahren angeschlossener Rechnersysteme möglich ist. Die Mehrzahl aller Stromausfälle ist innerhalb von 5 bis 10 Minuten behoben. Dauert ein Stromausfall länger, so bleibt bei einer Überbrückungszeit von ca. 10 bis 15 Minuten noch eine Reserve von etwa 5 Minuten, um das angeschlossene VPN geordnet herunterfahren zu können. Die meisten modernen USV-Geräte bieten Rechnerschnittstellen an, die ein automatisches Herunterfahren (Shut-down) nach einer vorher definierten Zeit einleiten können. Das Intervall wird dem Zeitbedarf zum Herunterfahren des VPN und der Kapazität der USV entsprechend festgelegt. Alternativ zu einer lokalen USV kann die Stromversorgung unterbrechungsfrei aus einer vorhandenen Quelle bezogen werden, beispielsweise durch den Anschluss an eine zentrale USV.

Geschützte Leitungsführung

Die Zuleitungen (zu schützendes und unsicheres Netz) sollen so eingerichtet werden, dass sie nicht außerhalb des zugangsgeschützten Raums überbrückt werden können.

Dokumentation

Durch eine gute Dokumentation und die eindeutige Kennzeichnung aller Leitungen des VPN kann einer fehlerhaften Verkabelung vorgebeugt werden, die zu einer Überbrückung des VPN führen könnte. Die Dokumentation ist ebenfalls für die Wartung sowie gegebenenfalls für eine erfolgreiche Fehlersuche und Instandsetzung erforderlich. Die Qualität dieser Dokumentation ist abhängig von ihrer Vollständigkeit, Aktualität und Lesbarkeit.

Zentrales Netzwerkmanagement-System

Durch Kopplung des VPN an ein vorhandenes Netzwerkmanagement-System können von diesem bestimmte Informationen über das VPN abgefragt werden oder werden vom VPN an das Netzwerkmanagement-System gemeldet. Dazu gehören Statusmeldungen und Alarme, die durch das Auftreten sicherheitskritscher Ereig-

nisse ausgelöst werden. Da Netzwerkmanagement-Systeme in der Regel lange Betriebszeiten erfüllen, häufig rund um die Uhr, erhöht die Kopplung des VPN an das Netzwerkmanagement-System die Verfügbarkeit des gesamten IT-Systems.

9.2.2 Organisation

Für den sicheren Betrieb eines VPN müssen auch einige organisatorische Sicherheitsmaßnahmen berücksichtigt werden. Diese Maßnahmen betreffen die allgemeine Organisation, die technische Realisierung, das Sicherheitsmanagement und die Benutzer.

Technische Realisierung

Externe Zugänge

Klare Richtlinien, die allen Benutzern bekannt sind, müssen genau festlegen, dass keine externen Zugänge unter Umgehung des VPN eingerichtet werden dürfen.

Sichere Anordnung weiterer Komponenten im Bereich des VPN:

Neben der Installation und dem Betrieb des VPN müssen auch weitere Komponenten, die der Kommunikation zwischen zu schützendem und unsicherem Netz dienen, sicher angeordnet werden. Dazu gehören zum Beispiel Firewall-Systeme.

Sicherheitsmanagement

Festlegung der Verantwortlichkeiten für das VPN

Die Verantwortlichkeiten für das VPN müssen klar geregelt und aufgeteilt sein. Für den VPN-Einsatz müssen die Fachverantwortung und die Betriebsverantwortung festgelegt werden. Der Fachverantwortliche ist zuständig für die Erarbeitung der fachlichen Vorgaben für das VPN. Die Fachverantwortung liegt in der Regel beim IT-Sicherheitsmanagement, das ein VPN-Sicherheitskonzept auf Grundlage der definierten VPN-Sicherheitspolitik erstellt. Die Betriebsverantwortung hingegen umfasst den sicheren Betrieb und die Überwachung des VPN. Diese Aufgabe wird vom Security Administrator ausgeführt, der unter anderem für die korrekte Einrichtung von weiteren Benutzerkonten für das Security Management verantwortlich ist.

Zugriffsrechte für das Security Management

Der Fachverantwortliche (IT-Sicherheitsmanagement) legt im VPN-Sicherheitskonzept die Zugriffsrechte von Benutzern für das Security Management fest. Die Zugriffsrechte regeln, in welcher Funktion ein Administrator das Security Management nutzen darf. Der Betriebsverantwortliche (Security Administrator) richtet die Funktionen ein, denen ein Administrator zugeordnet wird. Solche Funktionen sind zum Beispiel Operator, Auditor (Revisor), Editor (Datenerfasser) usw. Dabei sollten immer nur so viele Zugriffsrechte vergeben werden, wie für die Wahrneh-

mung der spezifischen Aufgaben notwendig ist (»Need-to-know-Prinzip«). Der jeweils Verantwortliche veranlasst und dokumentiert die Veränderung von Zugriffsrechten. Aus der Dokumentation muss hervorgehen,

- welche Funktion unter Beachtung der Funktionstrennung mit welchen Zugriffsrechten ausgestattet wird,
- welcher Administrator welche Funktion wahrnimmt,
- welche Zugriffsrechte ein Administrator erhält und
- welche Konflikte bei der Vergabe von Zugriffsrechten aufgetreten sind. Konflikte können beispielsweise daraus resultieren, dass ein Administrator unvereinbare Funktionen wahrnimmt oder daraus, dass abhängig vom VPN die Trennung bestimmter Zugriffsrechte nicht vorgenommen werden kann.

Der Security Administrator aktiviert sinnvoll einsetzbare Protokollfunktionen zur Beweissicherung, falls das Sicherheitsmanagement es zulässt. Dazu gehört die Protokollierung von erfolgreichen und erfolglosen An- und Abmeldevorgängen, unerlaubten Zugriffsversuchen und von Fehlermeldungen des Systems.

Im Vertretungsfall muss der Security Administrator kontrollieren, ob der Vertreter vom Fachverantwortlichen autorisiert ist, bevor er die erforderlichen Zugriffsrechte einrichtet.

Kontrolle der Protokolldaten

Die Protokollierung sicherheitsrelevanter Ereignisse ist als Sicherheitsmaßnahme nur wirksam, wenn die protokollierten Daten auch ausgewertet werden. Deshalb müssen die Protokolldaten in regelmäßigen Abständen durch einen Revisor ausgewertet werden. Wenn es technisch nicht möglich ist, die Rolle eines unabhängigen Revisors für Protokolldaten einzurichten, kann die Auswertung auch durch den Administrator erfolgen. In diesem Fall sind die Tätigkeiten des Administrators jedoch nur schwer zu kontrollieren. Das Ergebnis der Auswertung sollte dann dem IT-Sicherheitsbeauftragten, dem IT-Verantwortlichen oder einem anderen besonders zu bestimmenden Mitarbeiter vorgelegt werden.

Die regelmäßige Kontrolle und anschließende Löschung der Protokolldaten verhindert darüber hinaus ein übermäßiges Anwachsen der Protokolldaten. Da Protokolldaten in den meisten Fällen personenbezogene Daten beinhalten, ist sicherzustellen, dass diese Daten nur zum Zweck der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes verwendet werden (vgl. §§ 14 Abs. 4 und 31 BDSG).

Die nachfolgenden Auswertungskriterien dienen als Beispiele, die Hinweise auf eventuelle Sicherheitslücken, Manipulationsversuche und Unregelmäßigkeiten erkennen lassen:

- Liegen die Zeiten des An- und Abmeldens außerhalb der Arbeitszeit? (Hinweis auf Manipulationsversuche)

- Häufen sich fehlerhafte Anmeldeversuche? (Hinweis auf den Versuch, Passworte zu erraten)
- Häufen sich unzulässige Zugriffsversuche? (Hinweis auf Manipulationsversuche)
- Gibt es auffällig große Zeitintervalle, in denen keine Protokolldaten aufgezeichnet wurden? (Hinweis auf eventuell gelöschte Protokollsätze)
- Ist der Umfang der protokollierten Daten zu groß? (eine umfangreiche Protokolldatei erschwert das Auffinden von Unregelmäßigkeiten)
- Gibt es auffällig große Zeitintervalle, in denen anscheinend kein Login oder Logout stattgefunden hat? (Hinweis darauf, dass das konsequente Abmelden nach Arbeitsende nicht vollzogen wird)

Wenn regelmäßig umfangreiche Protokolldateien ausgewertet werden müssen, ist es sinnvoll, ein Werkzeug zur Auswertung zu benutzen. Dieses Werkzeug sollte wählbare Auswertungskriterien zulassen und besonders kritische Einträge (zum Beispiel mehrfache fehlerhafte Login-Versuche) hervorheben.

Informationsbeschaffung über Sicherheitslücken des VPN

Wenn durch Veröffentlichungen neue Sicherheitslücken bekannt werden, müssen die erforderlichen organisatorischen und administrativen Maßnahmen ergriffen oder zusätzliche Sicherheitshardware beziehungsweise -software eingesetzt werden, um diese Lücken zu schließen.

Deshalb ist es sehr wichtig, sich über neu bekannt gewordene Schwachstellen zu informieren. Informationsquellen sind:

- Hersteller bzw. Vertreiber von VPNs. Sie informieren registrierte Kunden über bekannt gewordene Sicherheitslücken ihrer Systeme und stellen korrigierte Versionen des VPN oder Patches zur Behebung der Sicherheitslücken zur Verfügung. Dieser Service kann zum Beispiel in einem Wartungsvertrag geregelt werden.
- Computer Emergency Response Teams (CERT)
- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- hersteller- und systemspezifische sowie sicherheitsspezifische Newsgroups im Internet
- IT-Fachzeitschriften

Reaktion auf Verletzungen der Sicherheitspolitik

Reaktionen auf Verletzungen der Sicherheitspolitik sollten vorab festgelegt werden, damit im Bedarfsfall schnell und wirksam gehandelt werden kann.

Art und Herkunft der Verletzung müssen untersucht und angemessene schadensbehebende oder -mindernde Maßnahmen ergriffen werden. Falls erforderlich, müssen zusätzlich schadensvorbeugende Konsequenzen gezogen werden. Welche

Aktionen durchgeführt werden müssen, hängt sowohl von der Art der Sicherheitsverletzung als auch von ihrem Verursacher ab.

Es muss vorab geklärt sein, wer dafür verantwortlich ist, Informationen über bekannte Sicherheitslücken einzuholen oder Informationen über aufgetretene Sicherheitslücken an andere Organisationen weiterzugeben. Auch muss dafür Sorge getragen werden, dass eventuell mitbetroffene Stellen schnellstens informiert werden.

Verpflichtung des Security Administrators zur Datensicherung

Da die Datensicherung eine wichtige Sicherheitsmaßnahme ist, sollte der zuständige Security Administrator zur Einhaltung des Datensicherungskonzepts beziehungsweise eines minimalen Datensicherungskonzepts für das VPN verpflichtet werden. Eine regelmäßige Erinnerung und Motivation zur Datensicherung sollte erfolgen.

Benutzer

Keine Weitergabe von Security Token und Passworten

Werden für die Authentisierung gegenüber dem *VPN* Security Token verwendet, so ist die Sicherheit der Zugangs- und Zugriffsrechteverwaltung entscheidend von der sicheren Benutzung der Security Token abhängig. Dazu gehört auch, dass die Passworte geheimgehalten und die Security Token nicht weitergegeben werden. Den Benutzern muss bewusst sein, dass sie für ihre Passworte und Security Token verantwortlich sind. Sie können auch dafür verantwortlich gemacht werden, wenn Fremde damit Schaden anrichten.

Betreuung und Beratung der Benutzer, die über das VPN kommunizieren

Der Einsatz eines VPN erfordert eine Schulung der Benutzer, die sie in die Lage versetzt, das eingesetzte VPN sachgerecht zu nutzen. Über die Schulung hinaus muss den Benutzern eine Betreuung und Beratung für im laufenden Betrieb eventuell auftretende Probleme zur Verfügung stehen. Probleme können aus unterschiedlichen Gründen entstehen, unter anderem wegen Unzulänglichkeiten der Benutzer, die eventuell eine andere Art und Weise der Nutzung von Diensten über das VPN erlernen müssen.

In größeren Organisationen kann es deshalb sinnvoll sein, eine zentrale Stelle mit der Betreuung der Benutzer, die über das VPN kommunizieren, zu beauftragen, und diese allen Benutzern bekannt zu geben.

Allgemeine Sicherheitsmaßnahmen

Regelung für Wartungs- und Reparaturarbeiten am VPN

Die ordnungsgemäße Durchführung von Wartungsarbeiten ist eine besonders wichtige vorbeugende Maßnahme, um das VPN vor Störungen zu bewahren. Die

Wartungsarbeiten sollten von vertrauenswürdigem Personal oder externen Firmen durchgeführt werden.

Wenn Wartungs- und Reparaturarbeiten durch externes Personal durchgeführt werden, sind Regelungen über deren Beaufsichtigung zu treffen: Während der Arbeiten sollte eine fachkundige Kraft die Arbeiten so weit beaufsichtigen, dass sie beurteilen kann, ob während der Arbeit nichtautorisierte Handlungen, beispielsweise die Einrichtung unerlaubter Zugriffsrechte aus dem unsicheren Netz, durchgeführt werden.

Vor und nach Wartungs- und Reparaturarbeiten sind folgende Maßnahmen einzuplanen:

- Die Arbeiten müssen den betroffenen Benutzern angekündigt werden.
- Wartungstechniker müssen sich auf Verlangen ausweisen.
- Die dem Wartungstechniker eingeräumten Zutritts-, Zugangs- und Zugriffsrechte sind auf das notwendige Minimum zu beschränken und nach den Arbeiten zu widerrufen beziehungsweise zu löschen.
- Nach der Durchführung von Wartungs- oder Reparaturarbeiten sind – je nach »Eindringtiefe« des Wartungspersonals – Passwortänderungen erforderlich.
- Die durchgeführten Wartungsarbeiten sind zu dokumentieren (Umfang, Ergebnisse, Zeitpunkt, eventuell Name des Wartungstechnikers).

Rechtzeitige Beteiligung des Personal- / Betriebsrats

Die Protokollierung ist eine Maßnahme, die geeignet ist, eine Verhaltens- oder Leistungsüberwachung von Benutzern zu ermöglichen, und bedarf somit der Mitbestimmung der Personalvertretung. Grundlage sind die Betriebsverfassungs- und Personalvertretungsgesetze von Bund und Ländern. Die rechtzeitige und umfassende Information des Betriebs- oder Personalrats kann eine Zeitverzögerung bei der Einführung eines VPN verhindern.

9.2.3 Personal

Personelle Sicherheitsmaßnahmen können das Sicherheitsmanagement und die Benutzer betreffen.

Sicherheitsmanagement

Profil des Security Administrators

Der Security Administrator muss grundlegende Kenntnisse im Bereich IT-Sicherheit und speziell über VPNs besitzen und diese Kenntnisse kontinuierlich aktualisieren und erweitern. Die Teilnahme an Schulungen über die Konfiguration und sichere Verwaltung des VPN, die vom jeweiligen Hersteller oder seinem Vertriebspartner angeboten werden, ist zu empfehlen. Der Security Administrator muss in der Lage sein, Fehlermeldungen und Alarme richtig einzuschätzen, um geeignete

Gegenmaßnahmen ergreifen zu können. Bei Eingriffen von externem Personal ins VPN muss der Administrator die durchgeführten Arbeiten nachvollziehen können.

Auswahl eines vertrauenswürdigen Administrators und Vertreters

Den Administratoren des VPN und ihren Vertretern muss großes Vertrauen entgegengebracht werden, da sie sehr weitgehende Befugnisse haben. Administrator und Vertreter sind in der Lage, auf alle gespeicherten Daten zuzugreifen, sie zu verändern und Berechtigungen zu vergeben, so dass durch einen Missbrauch der Befugnisse erheblicher Schaden entstehen könnte.

Das hierfür eingesetzte Personal muss sorgfältig ausgewählt und regelmäßig darüber belehrt werden, dass es seine Befugnisse nur für die erforderlichen Administrationsaufgaben verwenden darf.

Vertretungsregelungen

Vertretungsregelungen haben den Sinn, in vorhersehbaren (Urlaub, Dienstreise) und auch in unvorhersehbaren Fällen (Krankheit, Unfall, Kündigung) des Personalausfalls die Fortführung der Aufgabenwahrnehmung zu ermöglichen. Dazu muss *vor* Eintritt eines solchen Falls geregelt sein, wer wen in welchen Angelegenheiten mit welchen Kompetenzen vertritt. Dies ist beim VPN von besonderer Bedeutung, weil dafür meist Spezialwissen erforderlich ist und eine zeitgerechte Einarbeitung unkundiger Mitarbeiter im Vertretungsfall nicht möglich ist.

Für die Vertretungsregelungen sind folgende Randbedingungen einzuhalten:

- Der Verfahrens- oder Projektstand muss hinreichend dokumentiert sein.
- Der Vertreter muss geschult werden. Der Ausfall von Personen, die aufgrund ihres Spezialwissens nicht kurzfristig ersetzbar sind, bedeutet eine gravierende Gefährdung des Normalbetriebes. In diesem Fall ist die Schulung eines Vertreters von besonders großer Bedeutung.
- Es muss festgelegt sein, welcher Aufgabenumfang im Vertretungsfall von wem wahrgenommen werden soll.
- Der Vertreter darf die erforderlichen Zugangs- und Zutrittsberechtigungen nur im Vertretungsfall erhalten.
- Ist es in Ausnahmefällen nicht möglich, für eine Person einen kompetenten Vertreter zu benennen oder zu schulen, sollte frühzeitig überlegt werden, welche externen Kräfte im Vertretungsfall eingesetzt werden können.

Geregelte Verfahrensweise beim Ausscheiden von Benutzern

Scheidet ein Benutzer aus, so ist zu beachten, dass sämtliche für ihn eingerichteten Berechtigungen im VPN widerrufen beziehungsweise gelöscht werden müssen. Dies betrifft auch die externen Zugangsberechtigungen via Datenübertragungseinrichtungen.

Benutzer

Aufklärung der Benutzer über die Protokollierung von VPN-Daten

Die Benutzer müssen darüber aufgeklärt werden, dass ihre Verbindungen über das VPN protokolliert werden können. Gleichzeitig sollte der Grund der Protokollierung erklärt werden, damit er von den Benutzern verstanden und akzeptiert wird. Eine Aufklärung der Benutzer hat auch einen Warneffekt, der vor einem potentiellen Missbrauch schützen kann.

Sensibilisierung der Benutzer für mögliche Gefahren bei der Kommunikation über das Internet

Benutzer müssen darauf hingewiesen werden, welche Gefahren durch die Kommunikation über das Internet entstehen können. Durch Aufklärung und Sensibilisierung der Benutzer kann verhindert werden, dass das VPN, beispielsweise aus Bequemlichkeit, umgangen wird und dadurch eine ungeschützte Verbindung über das Internet mit all ihren Gefahren entsteht.

Schulung zum Thema Sicherheit

Die überwiegende Zahl von Schäden entsteht durch Nachlässigkeit. Um dem entgegenzuwirken, muss jeder einzelne Benutzer zum sorgfältigen Umgang mit der Informationstechnologie motiviert werden. Zusätzlich sind Verhaltensregeln zu vermitteln, die ein Verständnis für die Sicherheitsmaßnahmen wecken. Die Schulung zu Sicherheitsmaßnahmen soll insbesondere folgende Themen umfassen:

- *Sensibilisierung für IT-Sicherheit:* Jeder Benutzer ist auf die Notwendigkeit der IT-Sicherheit hinzuweisen. Das Aufzeigen der Abhängigkeit der Organisation und damit der Arbeitsplätze vom reibungslosen Funktionieren der IT-Systeme ist ein geeigneter Einstieg in die Sensibilisierung. Darüber hinaus ist der Wert von Informationen herauszuarbeiten, insbesondere unter den Gesichtspunkten der Vertraulichkeit, Integrität und Verfügbarkeit. Diese Sensibilisierungsmaßnahmen sind in regelmäßigen Zeitabständen zu wiederholen, eventuell auch durch praktische Hinweise in der Hauspost oder ähnliches.
- *Benutzerbezogene IT-Sicherheitsmaßnahmen:* Dieses Thema soll die Sicherheitsmaßnahmen vermitteln, die in einem VPN-Sicherheitskonzept erarbeitet wurden und von den einzelnen Benutzern umgesetzt werden müssen. Dieser Teil der Schulung ist von großer Bedeutung, da viele IT-Sicherheitsmaßnahmen erst nach entsprechender Schulung und Motivation effektiv umgesetzt werden können.
- *Vorbeugung gegen Social Engineering:* Die Benutzer sollen auf die Gefahren des Social Engineering hingewiesen werden. Die typischen Muster solcher Versuche, über gezieltes Aushorchen an vertrauliche Informationen zu gelangen, sollten ebenso bekannt gegeben werden wie die Methoden, sich dagegen zu schützen. Da Social Engineering oft mit der Vorspiegelung einer falschen Iden-

tität einhergeht, sollten Benutzer regelmäßig darauf hingewiesen werden, die Identität von Gesprächspartnern zu überprüfen und insbesondere am Telefon keine vertraulichen Informationen weiterzugeben.

9.2.4 Notfall

Festlegung von Verfügbarkeitsanforderungen

Verfügbarkeitsanforderungen an das VPN und die Dienste, die darüber zur Verfügung gestellt werden, müssen festgelegt werden. Bei Ausfall des VPN ermöglicht ein Übersichtsplan über die Verfügbarkeitsanforderungen eine schnelle Aussage, ab wann ein Notfall vorliegt. Dies bildet die Grundlage für eine Untersuchung und Einrichtung von Backup-Möglichkeiten.

Backup-Möglichkeiten

Sind die Verfügbarkeitsanforderungen an bestimmte Dienste besonders hoch, müssen Backup-Möglichkeiten geschaffen werden, die diesen Anforderungen genügen.

VPN: Eine Investition für die Zukunft

In diesem Kapitel werden die Kosten eines VPN-Systems aus unterschiedlichen Blickwinkeln betrachtet. Da ein VPN-System eine Investition für die Zukunft ist, sollten die Kosten-Nutzen-Aspekte schon bei der Planung besonders berücksichtigt werden.

10.1 Total Cost of Ownership

Im Folgenden soll beschrieben und abgeschätzt werden, wie groß der Aufwand ist, ein VPN anzuschaffen und zu betreiben.

Bei den Aufwendungen für ein VPN können drei Phasen unterschieden werden:

- Beschaffungsphase
- Installationsphase
- Aufrechterhaltung des Betriebs

Die Aufwendungen, die in diesem Abschnitt benannt werden, sind reale Aufwendungen, die unabhängig vom jeweiligen Zeitpunkt erbracht werden müssen. Aufwand wird auf Tage gerundet, wobei davon ausgegangen wird, dass sechs Stunden Aufwand einen Arbeitstag ausmachen.

Bei den angegebenen Aufwendungen wird davon ausgegangen, dass ein VPN 20 Organisationseinheiten und 300 Mobil- und Telearbeitsplätze miteinander verbindet.

Die Personalkosten werden mit EUR 750,- pro Tag veranschlagt. Falls die angegebenen Leistungen von Fachfirmen durchgeführt werden, muss sicherlich mit einem höheren Kostenbetrag gerechnet werden.

10.1.1 Beschaffungsphase eines VPN

In der Beschaffungsphase muss von der Organisation eine Sicherheitspolitik festgelegt werden, die als Grundlage für den Betrieb des VPN dient. Hier ist besonders wichtig, den Schutzbedarf des zu schützenden Netzes zu analysieren, damit eine richtige Sicherheitsanforderung festgelegt werden kann.

Sind die Randbedingungen der Sicherheitspolitik der Organisation definiert, dann kann die Produktauswahl eines VPN beginnen, zum Beispiel durch Einholen von Angeboten, Testinstallationen, Referenzbewertung etc. Dabei muss im Vorfeld festgelegt werden, nach welchen Kriterien ein Produkt bewertet werden soll.

Wichtig in dieser Phase ist, dass auch infrastrukturelle, personelle und organisatorische Sicherheitsmaßnahmen vorbereitet werden, damit die nächste Phase eingeleitet werden kann.

Aufwand für die Beschaffungsphase

Falls die Organisation noch keine generelle Sicherheitspolitik erarbeitet hat und diese im Rahmen der VPN-Beschaffung erstellt werden muss, ist der dafür erforderliche Aufwand in der Beschaffungsphase zu berücksichtigen. Die Erstellung einer Sicherheitspolitik kann je nach Größe der Organisation, je nach Anwendungsform und je nach Schutzbedarf zwischen zwei Wochen und zwei Monaten in Anspruch nehmen.

Für die Auswahl eines VPN-Produkts ist der Aufwand abhängig vom Auswahlverfahren sehr unterschiedlich, je nachdem, ob beispielsweise nur mit Hilfe von Prospekten ausgewählt wird oder Testinstallationen mehrerer VPNs mit Aufbau eines Testsystems stattfinden sollen. Der Aufwand liegt in der Regel zwischen zwei Wochen und drei Monaten.

Die Definition und Vorbereitung der infrastrukturellen, personellen und organisatorischen Sicherheitsmaßnahmen kann zwischen einer Woche und vier Wochen beanspruchen.

Die Anschaffungskosten für ein VPN-System (für 20 Organisationseinheiten und 300 Mobil- und Telearbeitsplätze) liegen zwischen 60 000 EUR und 150 000 EUR (20 VPN-Gateways und 300 VPN-Software-Clients), abhängig von seiner Leistungsfähigkeit und vom Maß an Sicherheit und Vertrauenswürdigkeit, das es erbringen kann.

Installationsphase eines VPN

In der Installationsphase gliedern sich die Aufwendungen für ein VPN in mehrere Teilbereiche.

- *Installation des VPN:* Diese Phase umfasst alle infrastrukturellen Sicherheitsmaßnahmen, die zum sicheren Betrieb eines VPN notwendig sind (siehe Kapitel 9 *Ein VPN ist mehr als ein Produkt*).
- *Inbetriebnahme des VPN:* In dieser Phase ist es sinnvoll, entsprechend den Vorgaben der Sicherheitspolitik Benutzerprofile für bestimmte Mitarbeitergruppen zu definieren, damit die Eingaben des Regelwerks später mit Hilfe dieser

Benutzerprofile schneller erfolgen können. Nach Formulierung der Profile werden die Benutzer, die über das VPN kommunizieren dürfen, mit ihren Rechten in das Sicherheitsmanagement eingetragen.

- *Sonstige Sicherheitsmaßnahmen:* In der Installationsphase ist es wichtig, dass weitere Sicherheitsmaßnahmen wie zum Beispiel die Schulung der Benutzer durchgeführt werden, damit diese den richtigen Umgang mit dem VPN lernen und dadurch unnötige Schwierigkeiten beim Betrieb vermieden werden. Hierzu gehört auch die Erarbeitung von Organisationsanweisungen usw. (siehe Kapitel 9 *Ein VPN ist mehr als ein Produkt*).

Die folgenden Tabellen sollen zeigen, welche zeitlichen und finanziellen Aufwendungen für die Beschaffungs- und Installationsphase einzuplanen sind.

Beschaffungsphase	Zeitaufwand	minimale Kosten	maximale Kosten
Sicherheitspolitik	zwei Wochen bis zwei Monate	EUR 7 500	EUR 30 000
Auswahl eines Produktes	zwei Wochen bis drei Monate	EUR 7 500	EUR 45 000
weitere Sicherheitsmaßnahmen	eine bis vier Wochen	EUR 3 800	EUR 15 000
Produktkosten		EUR 60 000	EUR 150 000

Tabelle 10.1: Aufwand und Kosten in der Beschaffungsphase

Installationsphase	Zeitaufwand	minimale Kosten	maximale Kosten
Installation des VPN	2 bis 5 Tage	EUR 1 500	EUR 3 800
Inbetriebnahme des VPN	3 bis 10 Tage	EUR 2 300	EUR 7 500
Sonstige Sicherheitsmaßnahmen	3 Wochen bis 3 Monate	EUR 11 300	EUR 45 000

Tabelle 10.2: Aufwand und Kosten in der Installationsphase

Anschaffungskosten	minimale Kosten	maximale Kosten
Summe	EUR 93 900	EUR 296 300

Tabelle 10.3: Gesamtkosten in der Beschaffungs- und Installationsphase

10.1.2 Aufrechterhaltung des Betriebs eines VPN

Die Aufwendungen für die Aufrechterhaltung des Betriebs eines VPN können unter verschiedenen Gesichtspunkten betrachtet werden.

Rechteverwaltung

Ein VPN ist prinzipiell so aufgebaut, dass es nach Eintrag sämtlicher Rechte vollkommen selbständig und ohne aktive Eingriffe eines Administrators betrieben werden kann.

Aus unterschiedlichen Gründen kann jedoch ein personeller Eingriff notwendig werden, unter anderem zur Einrichtung neuer Mitarbeiter oder Organisationseinheiten beziehungsweise zur Änderung der Rechte schon eingetragener Mitarbeiter oder Organisationseinheiten. Je nach Anzahl der definierten Benutzerprofile und der erforderlichen Änderungen ergibt sich ein sehr unterschiedlicher personeller Aufwand für diese Aufgaben.

Rechenbeispiel: Für die Eintragung eines neuen Mitarbeiters oder für die Änderung der Rechte eines schon eingetragenen Mitarbeiters benötigt der Administrator im Schnitt 10 Minuten. Die Veränderung der Mitarbeiterzahl in einer Organisation, die über das VPN kommunizieren darf, wird in unserem Beispiel mit 5 % im Monat veranschlagt.

Das bedeutet bei 300 (Mobil- und Tele-)Mitarbeitern, die potentiell über das VPN kommunizieren dürfen, dass 15 Veränderungen im Monat stattfinden. Für die Rechteverwaltung ist somit ein Zeitaufwand von 150 Minuten im Monat, also ca. 3 Stunden im Monat beziehungsweise 6 Tagen im Jahr notwendig.

Analyse der Logbuchdaten

Für die Analyse der Logbuchdaten, die vom VPN generiert werden, ist ein Aufwand für den Administrator einzukalkulieren. Auch hier kann der personelle Aufwand sehr unterschiedlich ausfallen. Bei VPNs, die eine automatische Vorauswertung durchführen, ist der Zeitaufwand weitaus geringer als bei VPNs, bei denen der Administrator die Logbuchdaten vollständig selbst auswerten muss.

Rechenbeispiel: Für die Analyse der Logbuchdaten wird 1 Stunde pro Woche veranschlagt. Dies bedeutet einen Aufwand von 1/2 Tag im Monat beziehungsweise 6 Tagen im Jahr.

Einrichtung von Updates

Da die TCP/IP-Technologie einer starken Dynamik und permanenten Veränderung unterworfen ist, muss davon ausgegangen werden, dass im Abstand von drei bis sechs Monaten ein Update des VPN durchgeführt werden muss, um den neuen

Anforderungen gerecht zu werden. Diese Updates erfordern ebenfalls einen bestimmten Zeitaufwand, da sie getestet werden müssen, um einen weiterhin sicheren Betrieb des VPN garantieren zu können.

Rechenbeispiel: Für diese Arbeit müssen pro Update 2 Tage vorgesehen werden, das bedeutet im Schnitt 6 Tage im Jahr.

Genereller administrativer Aufwand für das VPN

Für den sicheren Betrieb des VPN müssen Backups des aktuellen Regelwerks und der Logbuchdaten, regelmäßige Löschungen der Protokolldaten im Sicherheitsmanagement etc. durchgeführt werden.

Rechenbeispiel: Für diese generellen Arbeiten muss ein Aufwand von 1 Stunde pro Woche, das heißt von 1/2 Tag im Monat beziehungsweise 6 Tagen im Jahr, berücksichtigt werden.

Auswertung der Logbuchdaten im Sicherheitsmanagement

Da das Sicherheitsmanagement eines VPN sehr sicherheitskritisch ist, muss ein Revisor in regelmäßigen Abständen alle Aktionen der Administratoren des Management Systems mit Hilfe der Logbuchdaten des Sicherheitsmanagements überprüfen.

Rechenbeispiel: Für diese Arbeit sollen 3 Stunden im Monat berücksichtigt werden, das heißt 6 Tage im Jahr.

Sicherer Betrieb eines VPN

Damit mit Hilfe eines VPN ein effektiver Schutz für die Kommunikation durch das unsichere Netz gewährleistet werden kann, müssen die folgenden Bedingungen erfüllt sein:

- Das VPN-Konzept muss in das IT-Sicherheitskonzept der Organisation eingebunden werden.
- Der Betrieb des VPN muss auf eine umfassende Sicherheitspolitik aufbauen.
- Das VPN muss korrekt installiert sein.
- Das VPN muss korrekt administriert werden.

Aus diesem Grund ist eine regelmäßige Überprüfung der umgesetzten Sicherheitsmaßnahmen notwendig. Hierbei soll festgestellt werden, ob die unterschiedlichen Maßnahmen ordnungsgemäß eingehalten werden.

Diese Überprüfung muss alle Sicherheitsmaßnahmen einschließen, die zum sicheren Betrieb des VPN beitragen.

- Technische Sicherheitsmaßnahmen:
  - Durch regelmäßige Tests sollte überprüft werden, ob die in der Sicherheitspolitik festgelegten Regeln korrekt umgesetzt worden sind.
  - Mit einem Penetrationstest sollte überprüft werden, ob das VPN-System sicher konfiguriert ist.
- Infrastrukturelle Sicherheitsmaßnahmen:
  - In regelmäßigen Abständen sollte überprüft werden, ob die infrastrukturellen Sicherheitsmaßnahmen (zugangsgesicherter Raum, geschützte Leitungsführung, Dokumentation und Kennzeichnung der Verkabelung des VPN usw.) eingehalten werden.
- Organisatorische Sicherheitsmaßnahmen:
  - In zyklischen Abständen muss überprüft werden, ob neue ungesicherte Verbindungen nach außen geschaffen wurden.
  - Die Logbuchdaten müssen regelmäßig überprüft werden, ob beispielsweise Angriffsversuche stattgefunden haben.
- Personelle Sicherheitsmaßnahmen:
  - In regelmäßigen Abständen sollten Aktionen eingeleitet werden, die das Sicherheitsbewusstsein erhöhen, zum Beispiel Rundschreiben, Schulungen, Informationsveranstaltungen

Durchzuführende Maßnahmen	Aufwand
Technische Sicherheitsmaßnahmen	2 Tage pro Jahr
Infrastrukturelle Sicherheitsmaßnahmen	2 Tage pro Jahr
Organisatorische Sicherheitsmaßnahmen	2 Tage pro Jahr
Personelle Sicherheitsmaßnahmen	6 Tage pro Jahr
Summe	12 Tage pro Jahr

Tabelle 10.4: Aufwendungen für den sicheren Betrieb eines VPN

Durchzuführende Maßnahmen	Aufwand
Rechteverwaltung	6 Tage pro Jahr
Analyse der Logbuchdaten	6 Tage pro Jahr
Einrichtung neuer Dienste	6 Tage pro Jahr
Genereller administrativer Aufwand	6 Tage pro Jahr
Auswertung der Logbuchdaten im Sicherheitsmanagement	6 Tage pro Jahr
Weitere Maßnahmen für den sicheren Betrieb eines VPN	12 Tage im Jahr
Summe	42 Tage pro Jahr

Tabelle 10.5: Aufwendungen für die Aufrechterhaltung des Betriebs eines VPN

Für die Aufrechterhaltung des Betriebs eines VPN, über das 300 Mobil- und Telearbeiter sowie 20 Organisationseinheiten unter den beschriebenen Annahmen kommunizieren dürfen, ergibt sich ein Kostenaufwand von ca. EUR 31 500 im Jahr.

10.1.3 Zusammenfassung aller Kosten im Sinne der Total Cost of Ownership

Aufwendungen für ein VPN sind zum einen die Anschaffungskosten, die zwischen EUR 93 900 und EUR 296 300 liegen können, und zum anderen die Kosten für die Aufrechterhaltung des Betriebs, die in unserem Rechenbeispiel mit EUR 31 500 im Jahr veranschlagt werden.

Diese Zahlen hängen sehr stark von der Struktur und der Größe der Organisation ab. Außerdem müssen die folgenden Aspekte berücksichtigt werden:

- Typ des verwendeten VPN
- Qualität des VPN-Konzepts
- Möglichkeit eines automatischen Updates von zentraler Stelle
- funktionierendes Redundanz-Konzept
- Anzahl der Benutzer, die über das VPN kommunizieren dürfen
- Veränderung der Kommunikationsprofile
- Qualifikation der Administratoren des Sicherheitsmanagements
- Betriebszeiten
- Veränderungen der Benutzer
- Veränderung der Netzstruktur
- Tiefe der Auswertung der Logbuchdaten
- verwendetes Authentikationsverfahren

Bei der Auswahl eines VPN-Systems ist neben der gewünschten Sicherheit auch die Möglichkeit des einfachen und kostengünstigen Managements der einzelnen VPN-Komponenten ein wichtiges Kriterium, damit das System im Sinne der Total Cost of Ownership wirtschaftlich betrieben werden kann.

10.2 Kosten-Nutzen-Betrachtung im Hinblick auf die Sicherheit

Am Beispiel einer Bank mit 100 Filialen soll eine Kosten-Nutzen-Betrachtung eines VPN-Systems durchgeführt werden. Dabei wird angenommen, dass ohne den Einsatz eines VPN-Systems die Wahrscheinlichkeit eines erfolgreichen Angriffs sehr hoch ist.

Profit der Bank im letzten Jahr

- Profit: EUR 25 000 000

Kosten eines VPN-Systems

- Anschaffungskosten: EUR 250 000 (1 % des Profits)
- Betriebskosten: EUR 35 000/Jahr

Beschreibung eines möglichen Angriffs

Die Bank wird von einem professionellen Kriminellen über das Internet angegriffen. Dieser liest während einer Übertragung zwischen der Zentrale und einer Filiale der Bank die Namen und Kontostände der 500 wichtigsten Kunden mit. Diese Daten werden dann via Internet veröffentlicht, Fernsehen und Presse berichten und die Bank erleidet dadurch einen enormen Imageverlust.

Möglicher Schaden durch diesen Angriff

Durch den enormen Imageverlust wechseln sehr viele Kunden zu einer anderen vertrauenswürdigeren Bank. Der dadurch entstehende Schaden für die angegriffene Bank wird folgendermaßen angenommen:

- sofort: EUR 12.500.000 (50 % des Gewinns)
- mittelfristig: EUR 2.500.000/Jahr

Zusammenfassung

Unter der Voraussetzung, dass der Schaden mit Hilfe eines VPN-Systems vollständig verhindert worden wäre, hätte sich die Investition in ein VPN-System gelohnt. Mit der Investition von 1 % des Gewinns kann der Bank ein Schaden erspart werden, der sich auf ein Vielfaches der Investition beläuft (in diesem Beispiel das 50fache).

Mit Bekanntwerden des Angriffs werden auch »Trittbrettfahrer« animiert, den Angriff nachzuahmen. Dadurch steigt das Risiko, erneut Opfer zu werden, und zu den Aufwendungen zur Behebung des Schadens kommen die Aufwendungen für die Anschaffung eines geeigneten VPN-Systems, um weiteren Angriffen vorzubeugen.

10.3 Wahrscheinlichkeit eines bestimmten Profits

Die folgende Abbildung stellt dar, wie die Höhe des Investments in Sicherheitsmechanismen vom eigenen Schutzbedarf und der Wahrscheinlichkeit, einen bestimmten Profit erreichen zu können, abhängig ist.

Die Abbildung zeigt, dass in Bereichen mit hohem Schutzbedarf (zum Beispiel in Finanzinstituten) höhere Investitionen in Sicherheitsmaßnahmen notwendig sind, um die gleiche Chance auf einen bestimmten Gewinn zu bewahren.

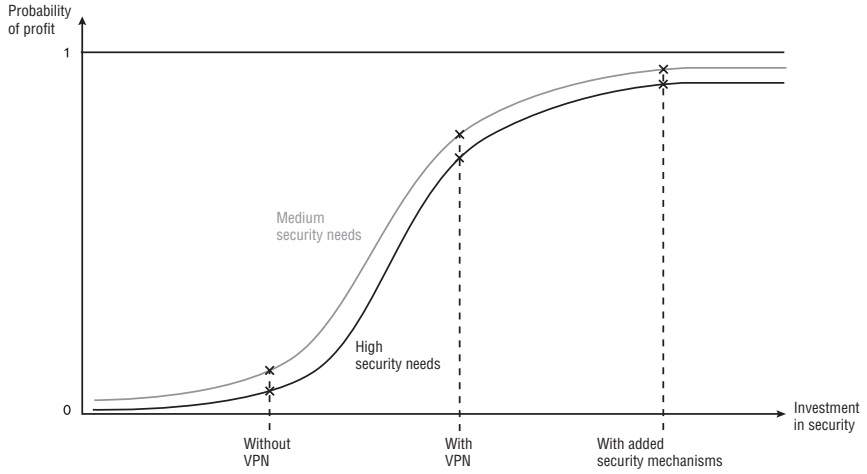


Abb. 10.1: Investment in Sicherheitsmechanismen und Wahrscheinlichkeit eines bestimmten Profits

Mit den Investitionen in Sicherheitsmechanismen steigt auch die Wahrscheinlichkeit, einen bestimmten Profit zu erreichen. Das heißt, die Anschaffung von Sicherheitssystemen wie VPN, Firewall-System, Intrusion Detection und Viren-Scanner ist ein Investment in die Absicherung des Gewinns. Die Wahrscheinlichkeit auf einen bestimmten Gewinn wird um so höher, je höher die Ausgaben für Sicherheitsmechanismen sind. Der Gewinn kann durch diese Maßnahmen allein aber nie hundertprozentig sicher sein, da immer ein Restrisiko bestehen bleibt.

Die Wahrscheinlichkeit der Gewinnerzielung hängt auch vom Schutzbedarf und damit von der Eintrittswahrscheinlichkeit eines Angriffs ab. Bei höherer Eintrittswahrscheinlichkeit steigt auch der Schutzbedarf vor einem Angriff.

Ist der Schutzbedarf sehr hoch, ist die Wahrscheinlichkeit auf einen Profit geringer als bei niedrigem Schutzbedarf. Bei Verzicht auf Sicherheitsmechanismen ist dieser Unterschied viel größer als bei hohem Einsatz von Sicherheitsmechanismen, da die Eintrittswahrscheinlichkeit eines Angriffs bei niedrigem Schutzbedarf kleiner ist.

Letztlich ist die Unternehmensleitung für die Sicherheit in einem Unternehmen verantwortlich und muss über das richtige Kosten-Nutzen Verhältnis entscheiden. Die Unternehmensleitung ist gut beraten, wenn sie einen gewissen Prozentsatz des Gewinns als Gewinnversicherung für die IT-Sicherheit ausgibt. Dieser Prozentsatz wird bei Unternehmen, deren Image als vertrauenswürdiges Unternehmen die Basis ihres Erfolgs darstellt (beispielsweise bei Banken und Versicherungen), höher liegen als bei Unternehmen wie Speditionen und Brauereien, bei denen die IT-Sicherheit in bezug auf das Image eine untergeordnete Rolle spielt.

10.4 Kosten-Nutzen-Betrachtung im Hinblick auf die Kommunikation

Mit der Hilfe von Virtual Private Networks können Kosten im IT-Bereich massiv gesenkt werden.

Im Folgenden werden zwei mögliche Lösungen zum Aufbau einer vertrauenswürdigen Kommunikationsinfrastruktur zwischen mehreren Niederlassungen und der Zentrale eines Unternehmens verglichen.

Bedingungen

- Die Zentrale des Unternehmens ist in Frankfurt. Niederlassungen befinden sich in Aachen, Berlin, Hamburg und München.
- Die Übertragungsrate zwischen der Zentrale und den Niederlassung soll 2 Mbit/s betragen.
- Beim Datenvolumen wird davon ausgegangen, dass im Schnitt nicht mehr als 30 Gigabyte im Monat übertragen werden. Das macht bei einer Auslastung von 100 % mehr als 5 Stunden Übertragungszeit pro Tag aus.

Lösung 1

Zwischen der Zentrale und den Niederlassungen werden »Leased Links« mit 2 Mbit/s genutzt, um eine IP-Kommunikation zu realisieren. Die notwendigen Router hat das Unternehmen bereits gekauft.

Eine zusätzliche Sicherheit wird nicht eingesetzt, da die Wahrscheinlichkeit eines Schadens bei Leased Links als gering anzusetzen ist.

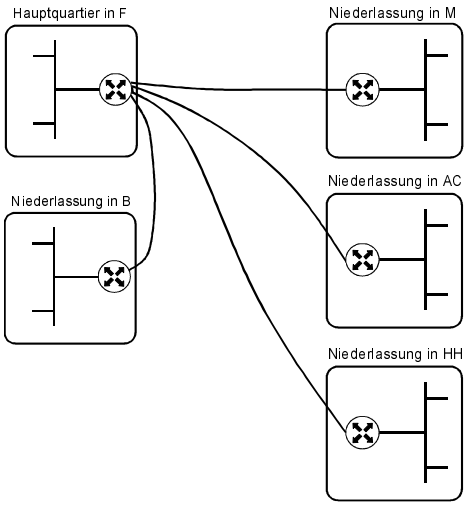


Abb. 10.2: Kommunikation eines Unternehmens über »Leased Links«

Kosten dieser Lösung (in EUR)

	Miete/Monat	Kosten/Monat für Datenvolumen	Einmalige Kosten für Installation	Einmalige Investitionskosten umgerechnet in Kosten/Monat über 5 Jahre
Frankfurt/ Aachen	ca. 2 750,–	0	ca. 2 100,–	ca. 35,–
Frankfurt/ Hamburg	ca. 3 400,–	0	ca. 2 100,–	ca. 35,–
Frankfurt/ Berlin	ca. 3 500,–	0	ca. 2 100,–	ca. 35,–
Frankfurt/ München	ca. 3 150,–	0	ca. 2 100,–	ca. 35,–
Summe	ca. 12 800,–	0		ca. 140,–

Die Kosten pro Monat betragen in diesem Beispiel 12 940,– EUR.

Lösung 2

Die Zentrale und die Niederlassungen werden mit Hilfe von »T-InterConnect«-Anschlüssen mit 1,92 Mbit/s an das Internet angeschlossen. Die notwendigen Router hat das Unternehmen bereits gekauft.

Zusätzlich wird in jede Niederlassung ein VPN-Gateway installiert, damit eine vertrauenswürdige Kommunikation gewährleistet werden kann.

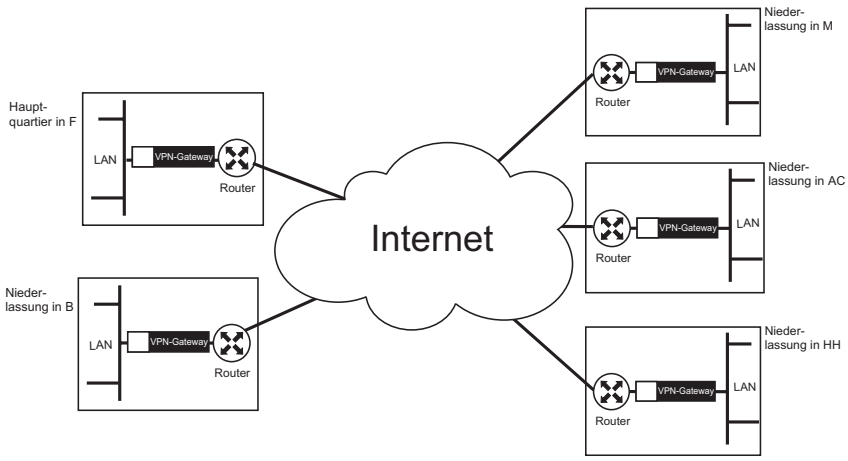


Abb. 10.3: VPN-gesicherte Kommunikation eines Unternehmens über das Internet

Kosten dieser Lösung (in EUR)

	Miete/ Monat	Kosten/ Monat für Datenvolumen	Einmalige Kosten für VPN-Gateways	Einmalige Kosten für Installation der VPN-Gateways	Einmalige Kosten für Installation der Anschlüsse	Einmalige Investitionskosten umgerechnet in Kosten/Monat über 5 Jahre
Frankfurt	ca. 900,-	ca. 850,-	ca. 1 000,-	ca. 4 450,-	ca. 2 400,-	ca. 130,-
Aachen	ca. 900,-	ca. 850,-	ca. 1 000,-	ca. 4 450,-	ca. 2 400,-	ca. 130,-
Hamburg	ca. 900,-	ca. 850,-	ca. 1 000,-	ca. 4 450,-	ca. 2 400,-	ca. 130,-
Berlin	ca. 900,-	ca. 850,-	ca. 1 000,-	ca. 4 450,-	ca. 2 400,-	ca. 130,-
München	ca. 900,-	ca. 850,-	ca. 1 000,-	ca. 4 450,-	ca. 2 400,-	ca. 130,-
Summe	ca. 4 500,-	ca. 4 250,-				ca. 650,-

Die Kosten pro Monat betragen in diesem Beispiel ca. 9 400,- EUR

Vergleich der beiden Lösungen

- Die erste Lösung kostet im Monat ca. 3 500,- EUR mehr und bietet einen höheren garantierten Datendurchsatz.
- Die zweite Lösung ist flexibler in ihrer Verwendung, da sie auf einer weltweit verbreiteten Infrastruktur basiert und bietet eine höhere Sicherheit.
- Soll mit Niederlassungen im Ausland kommuniziert werden, vergrößert sich die Kostendifferenz zwischen den beiden Lösungen wesentlich.
- Die Sicherheit der ersten Lösung beruht lediglich auf der Annahme, dass die Leased Links nicht abgehört werden.
- Die Sicherheit der zweiten Lösung wird vom Unternehmen eigenverantwortlich und seinem Schutzbedarf entsprechend realisiert.

10.5 Kosten-Nutzen-Betrachtung im Hinblick auf die Nicht-Realisierung von Kommunikation

Verzichtet ein Anwender aufgrund von Sicherheitsbedenken darauf, das Internet als geschäftliches Kommunikationsmittel zu nutzen, so kann er das darin liegende – oftmals erhebliche – Rationalisierungspotenzial nicht ausschöpfen. Auf längere Sicht droht dadurch ein Verlust geschäftlicher Handlungsmöglichkeiten.

Aus diesem Grund kann die Investition in IT-Sicherheitskomponenten, sofern sie geringer ist als die dadurch mögliche Wertschöpfung, zu einer Steigerung der Effizienz beitragen, die letztlich auch die Wachstumschancen des Unternehmens verbessern kann.

Kapitel 11

Evaluierung und Zertifizierung von VPNs

Vor der Anschaffung eines VPN stellt sich Kunden und Benutzern die Frage, welche Sicherheitskriterien es wirklich erfüllt.

Mit dem Mittel der Evaluation kann überprüft werden, ob angegebene Sicherheitsfunktionalitäten tatsächlich vorhanden sind und ihre Funktion korrekt erfüllen. Ziel der Evaluierung ist, dem Anwender des Sicherheitssystems das Vertrauen zu geben, dass das VPN-System ordnungsgemäß und wunschgemäß arbeitet.

Ein Kunde oder Benutzer kann die Evaluation eines VPN selbst durchführen oder von einem Spezialisten durchführen lassen. Eine Evaluation selbst durchzuführen, scheitert oft an der fehlenden Fachkenntnis oder dem damit verbundenen enormen Aufwand.

Die Alternative besteht darin, die Evaluation durch eine kompetente und unabhängige Stelle durchführen zu lassen. Ein von Experten aufgrund einer durchgeführten Evaluation vergebenes Zertifikat bietet Kunden und Benutzern einen Maßstab bei der Bewertung unterschiedlicher VPNs. Die Evaluation erfolgt dabei nach definierten Kriterien.

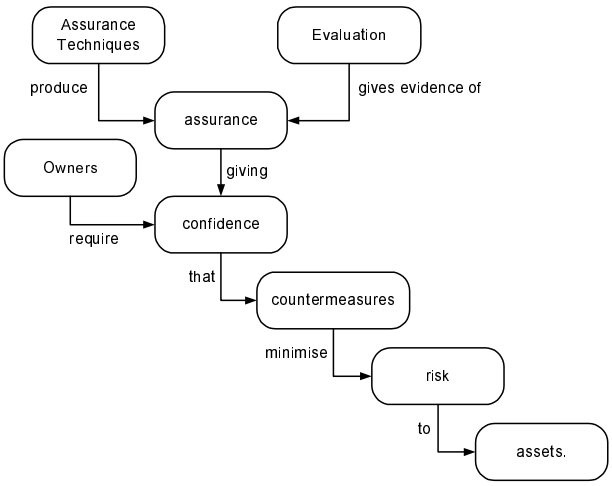


Abb. 11.1: Evaluierung und Zertifizierung

Zur Durchführung der Evaluierung und Zertifizierung von VPNs gibt es verschiedene Möglichkeiten. In den folgenden Abschnitten wird exemplarisch das bekannteste Zertifizierungsverfahren dargestellt, die Zertifizierung nach ITSEC. Zugleich wird die in der Praxis erreichbare »Tiefe« der Bewertung der beiden Verfahren beschrieben.

11.1 ITSEC-Zertifizierung

Die ITSEC (Information Technologie Security Evaluation Criteria) wurden von Frankreich, der Bundesrepublik Deutschland, den Niederlanden und Großbritannien auf der Grundlage von existierenden nationalen IT-Sicherheitskriterien [CESG3, DTIEC, SCSSI, ZSIEC, TCSEC] erarbeitet. Für eine Harmonisierung der unterschiedlichen Kriterien sprach die Forderung der Industrie, die in den verschiedenen Ländern verschiedene Sicherheitskriterien vorfand, und zum anderen der Vorteil, den sich die Beteiligten davon versprachen, die in den unterschiedlichen Ländern gesammelten Erfahrungen gemeinsam gewinnbringend zu nutzen.

Die erarbeiteten Kriterien stellen die Grundlage für eine Zertifizierung durch die nationalen Zertifizierungsstellen dar, die nach diesen Kriterien erstellte Zertifikate gegenseitig anerkennen.

Eine Zertifizierung kann sowohl vom Hersteller als auch vom Vertreiber eines VPN beantragt und durchgeführt werden. Der Vorteil einer vom Hersteller beantragten Zertifizierung liegt darin, dass die notwendigen Unterlagen bereits vorhanden sind und nicht erst erstellt werden müssen. Der mit dem Zertifizierungsprozess verbundene Aufwand ist allerdings sehr hoch. Die Zertifizierung durch einen Vertreiber lohnt nur bei einer niedrigen Evaluationsstufe, da dem Vertreiber die entsprechenden Sourcen (zum Beispiel für die Software) nicht zur Verfügung stehen.

Im folgenden wird exemplarisch dargestellt, welche Unterlagen vom Hersteller beziehungsweise Entwickler bereitzustellen sind und welche Tests durchgeführt werden müssen, um eine Zertifizierung nach Stufe E3 zu erreichen.

Neben dem Hersteller beziehungsweise Entwickler und der Zertifizierungsstelle ist eine akkreditierte Prüfstelle an der Evaluierung beteiligt. Die Prüfstelle (Prüflabor) führt die erforderlichen technischen Prüfungen im Auftrag des Herstellers unter Aufsicht der Zertifizierungsstelle durch und erstellt die jeweiligen Prüfberichte. Abschließend wird von der Zertifizierungsstelle ein Zertifizierungsreport mit allen Ergebnissen erstellt und veröffentlicht. Ergebnisse im Zertifizierungsreport sind beispielsweise die Beschreibung der Bedrohungen, denen das VPN entgegenwirkt, die Liste der implementierten Sicherheitsmechanismen, Angaben zur genauen technischen und organisatorischen Einsatzumgebung des VPN und Restrisiken unter bestimmten Voraussetzungen.

Die Evaluation erfolgt unter den Aspekten Korrektheit und Wirksamkeit. Bei der Bewertung der Korrektheit wird untersucht, ob die sicherheitsspezifischen Funktionen und Mechanismen korrekt implementiert wurden. Bei der Bewertung der Wirksamkeit wird beurteilt, ob die sicherheitsspezifischen Funktionen und Sicherheitsmechanismen des VPN die vorgegebenen Ziele tatsächlich erreichen. Zusätzlich wird die Fähigkeit der Sicherheitsmechanismen bewertet, Widerstand gegen einen direkten Angriff zu leisten (Stärke der Sicherheitsmechanismen).

Die für die Bewertung der Korrektheit erforderlichen Unterlagen, die der Hersteller beziehungsweise Vertreiber zur Verfügung stellen muss, sind:

- die informelle Beschreibung der Architektur des VPN
- die informelle Beschreibung des Feinentwurfs des VPN
- die Testdokumentation
- die Bibliothek der Testprogramme und -werkzeuge, die für den Test des VPN benutzt wurden
- Der Quellcode beziehungsweise die Hardware-Konstruktionszeichnungen für alle sicherheitspezifischen und sicherheitsrelevanten Komponenten
- die informelle Zuordnungsbeschreibung, die den Bezug zwischen Quellcode beziehungsweise Hardware-Konstruktionszeichnungen und Feinentwurf darstellt
- die Konfigurationsliste, die eindeutig die Version des VPN identifiziert
- die Informationen über das Konfigurationskontrollsystem
- die Informationen über das Abnahmeverfahren
- die Informationen über die Sicherheit der Entwicklungsumgebung
- die Beschreibung aller benutzten Implementierungssprachen
- die Benutzerdokumentation
- die Systemverwalter-Dokumentation
- die Auslieferungs- und Konfigurationsdokumentation
- die Anlauf- und Betriebsdokumentation

Folgende Unterlagen des VPN müssen unter dem Aspekt der Wirksamkeit zur Verfügung gestellt werden:

- die Analyse der Eignung der Sicherheitsmechanismen
- die Analyse des Zusammenwirkens der Sicherheitsmechanismen
- die Analyse der Stärke der Sicherheitsmechanismen des VPN
- die Liste der bekannten Schwachstellen in der Konstruktion
- die Analyse der Benutzerfreundlichkeit
- die Liste der bekannten Schwachstellen bei der operationellen Nutzung des VPN

Sicherheitsvorgaben

In den Sicherheitsvorgaben werden die Sicherheitseigenschaften des VPN beschrieben. Dabei handelt es sich um Kriterien, die die Sicherheitsmaßnahmen auf drei Ebenen betrachten:

- Sicherheitsziele: Weshalb wird die Funktionalität gebraucht?
- sicherheitsspezifische Funktionen: Welche Funktionalität wird zum Erreichen der Sicherheitsziele zur Verfügung gestellt?
- Sicherheitsmechanismen: Wie wird die Funktionalität zur Verfügung gestellt?

Die Sicherheitsvorgaben müssen die folgenden Punkte enthalten:

- eine Produktbeschreibung (welche Dienste sind implementiert, was für ein Security Management steht zur Verfügung usw.)
- die Art des Produkteinsatzes
- die vorgesehene Einsatzumgebung (technisch und administrativ)
- die Definition der Sicherheitsziele
- die angenommenen Bedrohungen, denen das VPN entgegenwirkt
- die zur Verfügung gestellten sicherheitsspezifischen Funktionen
- die Sicherheitsmechanismen
- eine Beschreibung der Zweckmäßigkeit der Sicherheitsmechanismen

Das Prüflabor prüft, ob für jede mögliche Bedrohung mindestens eine sicherheitsspezifische Funktion existiert, die ihr entgegenwirkt. Die Sicherheitsmechanismen, die die entsprechenden Funktionen zur Verfügung stellen, werden auf ihre Zweckmäßigkeit überprüft.

Architekturentwurf

Im Architekturentwurf wird die grundsätzliche Struktur des VPNs mit allen seinen externen Schnittstellen beschrieben. Hier findet eine Aufteilung des VPN-Systems in sicherheitsspezifische und nicht-sicherheitsspezifische Komponenten statt. Sicherheitsspezifische Komponenten sind Komponenten, die direkt sicherheitsspezifische Funktionen ausführen oder daran beteiligt sind. Die Trennung von sicherheitsspezifischen und nicht-sicherheitsspezifischen Komponenten wird beschrieben und die Wirksamkeit dieser Trennung wird überprüft.

Feinentwurf

Der Feinentwurf des VPN enthält die Spezifikation aller Komponenten und ihrer Schnittstellen. Alle sicherheitsspezifischen Funktionen müssen beschrieben und auf die Komponenten abgebildet werden. Alle Sicherheitsmechanismen müssen definiert und spezifiziert werden. Im Feinentwurf muss nachgewiesen werden, dass die angegebenen Sicherheitsmechanismen nicht in irgendeiner Form umgangen werden können.

Tests

Alle Sicherheitsmechanismen müssen dem Quellcode zugeordnet werden, das heißt, es muss beschrieben werden, welcher Sicherheitsmechanismus wo und wie implementiert ist. Jeder einzelne Sicherheitsmechanismus muss durch Tests nachgewiesen werden. Dazu muss der Hersteller neben dem Quellcode des VPN die Testpläne, Testziele, Testverfahren, Testergebnisse und die Bibliotheken aller verwendeten Testprogramme und -werkzeuge in einer Testdokumentation festhalten.

Das Prüflabor überprüft anhand des Quellcodes und der Testdokumentation, ob alle sicherheitsspezifischen Funktionen betrachtet und alle Sicherheitsmechanismen getestet wurden. Dazu wird der Quellcode auf eventuell vorhandene Möglichkeiten zur Umgehung von Sicherheitsmechanismen analysiert und die Tests werden wiederholt. Zusätzlich werden Penetrationstests und Tests zur Fehlersuche durchgeführt.

Entwicklungsumgebung

Die Entwicklungsumgebung umfasst das Konfigurationskontrollsystem, das Abnahmeverfahren, die Konfigurationsliste, die Beschreibung aller benutzten Implementierungssprachen und die Sicherheit der Entwicklungsumgebung.

Mit dem Konfigurationskontrollsystem, dem Abnahmeverfahren und der Konfigurationsliste stellt der Hersteller sicher, dass das VPN mit der zur Verfügung gestellten Dokumentation übereinstimmt, dass nur autorisierte Änderungen daran möglich sind sowie dass das VPN vollständig und die angegebene Version eindeutig ist.

Das Prüflabor prüft den Einsatz des Konfigurationskontrollsystems und das Abnahmeverfahren beim Hersteller.

Die Programmiersprachen, die für die Implementierung benutzt werden, müssen mit allen verwendeten Optionen eindeutig angegeben werden. Dies dient zu einer eventuell notwendigen Rekonstruktion der VPN-Software.

Der Hersteller muss mit Informationen über die Sicherheit seiner Entwicklungsumgebung beschreiben, wie die Schutzmaßnahmen bezüglich der Integrität des VPN und die Vertraulichkeit der zugehörigen Dokumente realisiert werden. Alle dazu notwendigen Sicherheitsmaßnahmen müssen beschrieben werden. Die Maßnahmen werden eingeteilt in

- materielle Sicherheitsmaßnahmen, wie zugangsgeschützte Räume für die Entwicklungsrechner des VPN, USV und ähnliches,
- organisatorische Sicherheitsmaßnahmen, beispielsweise restriktive Rechteverwaltung für die Entwicklungsrechner des VPN und Regelungen für den Modemgebrauch, und
- personelle Sicherheitsmaßnahmen, wie zum Beispiel Sicherheitsüberprüfungen der VPN-Entwickler und Mitarbeiter.

Das Prüflabor prüft die Anwendung und Einhaltung der angegebenen Verfahren beziehungsweise Vorschriften. Zusätzlich wird nach eventuell vorhandenen Fehlern in den angewendeten Verfahren gesucht.

Betriebsdokumentation

Die Betriebsdokumentation des VPN unterteilt sich in Benutzerdokumentation und Systemverwalterdokumentation.

Die Benutzerdokumentation muss strukturiert aufgebaut und in sich konsistent sein. Sie muss Richtlinien für ihre sichere Anwendung enthalten und beschreiben, wie der Benutzer das VPN auf sichere Art und Weise bedient.

Die Systemverwalterdokumentation muss ebenfalls strukturiert aufgebaut und in sich konsistent sein. Sie muss beschreiben, wie das Produkt installiert, konfiguriert und sicher verwaltet wird. Die Beschreibung der Sicherheitsparameter, der möglichen sicherheitsrelevanten Ereignisse, der Verfahren für die Sicherheitsadministration, der Sicherheitseigenschaften und deren Zusammenwirken müssen in der Systemverwalterdokumentation enthalten sein.

Betriebsumgebung

Die Betriebsumgebung kann unter zwei Aspekten betrachtet werden:

- Auslieferung und Konfiguration
- Anlauf und Betrieb

Die Informationen zum angewendeten Verfahren der Auslieferung und Konfiguration müssen beschreiben, wie der Hersteller die Sicherheit des VPN aufrechterhält, beispielsweise durch Prüfsummen der Software, Siegel usw. Sind unterschiedliche Konfigurationen möglich, muss die Auswirkung der einzelnen Konfigurationen auf die Sicherheit beschrieben werden.

Das Prüflabor hat die korrekte Anwendung des Auslieferungsverfahrens für das VPN zu überprüfen und nach Fehlern zu suchen.

Der Hersteller muss beschreiben, wie die Prozeduren für den Anlauf und Betrieb realisiert sind und auf welche Weise sie die Sicherheit aufrecht erhalten. Dazu müssen die sicherheitsspezifischen Funktionen beschrieben werden, die eventuell während des Anlaufs, des Betriebs oder der Wartung ausgeschaltet oder modifiziert werden können. Beispiele von Protokollaufzeichnungen beziehungsweise Ergebnisse von Diagnoseprozeduren, die während des Anlaufs und des Betriebs erstellt werden, müssen vorgelegt werden. Das Prüflabor prüft die Protokollaufzeichnungen beziehungsweise die Ergebnisse von Diagnoseprozeduren und sucht nach Fehlern in den Prozeduren.

Wirksamkeit

Die Untersuchung der Wirksamkeit basiert auf einer Schwachstellenanalyse des VPN. Bei dieser Analyse werden alle Wege gesucht, die es einem Angreifer erlauben würden, die sicherheitsspezifischen Funktionen und Sicherheitsmechanismen zu deaktivieren, zu umgehen, zu verändern, auszuschalten, direkt anzugreifen oder anderweitig außer Kraft zu setzen. Dabei werden alle zur Verfügung stehenden Informationen, das heißt auch der Quellcode, verwendet.

Analyse der Eignung der Funktionalität

Bei der Analyse der Eignung der Funktionalität wird geprüft, ob es Bedrohungen gibt, denen nicht eine oder mehrere sicherheitsspezifische Funktionen des VPN angemessen entgegenwirken.

Analyse des Zusammenwirkens der Funktionalität

Mit der Analyse des Zusammenwirkens wird gezeigt, dass die sicherheitsspezifischen Funktionen und Sicherheitsmechanismen des VPN so zusammenwirken, dass sie sich gegenseitig unterstützen und ein wirksames Ganzes bilden. Des Weiteren wird gezeigt, dass keine sicherheitsspezifische Funktion und kein sicherheitsspezifischer Sicherheitsmechanismus existiert, die oder der in Konflikt mit anderen sicherheitsspezifischen Funktionen oder Sicherheitsmechanismen geraten oder ihnen entgegenwirken kann.

Analyse der Stärke der Sicherheitsmechanismen

Diese Analyse bewertet die Fähigkeit der Sicherheitsmechanismen, direkten Angriffen zu widerstehen, die auf Mängel in den ihnen zugrunde liegenden Algorithmen, Prinzipien oder Eigenschaften zurückzuführen sind. Dabei wird auch der Aufwand an Betriebsmitteln betrachtet, den ein Angreifer benötigen würde, um einen erfolgreichen direkten Angriff durchzuführen. Analysen über die Algorithmen, Prinzipien und Eigenschaften, die diesen Sicherheitsmechanismen zugrunde liegen, müssen erstellt oder es muss auf solche Analysen verwiesen werden. Die Analyse erfolgt hinsichtlich der Einstufung der Mindeststärke und unter Verwendung aller zur Verfügung stehenden Informationen, einschließlich des Quellcodes des VPN.

Das Prüflabor überprüft unter Verwendung aller zur Verfügung stehenden Informationen einschließlich des Quellcodes, ob die Sicherheitsmechanismen die beanspruchte Mindeststärke gewährleisten. Zusätzlich werden aktive und aggressive Penetrationstests zur Bestätigung der Mindeststärke durchgeführt.

Analyse der Benutzerfreundlichkeit

Ob sicherheitsspezifische Funktionen oder Mechanismen durch menschliche oder andere Fehler ausgeschaltet oder unbrauchbar gemacht wurden, muss einfach festzustellen und zu erkennen sein, damit Endbenutzer oder Administratoren

nicht von einem sicheren Zustand ausgehen, obwohl das VPN möglicherweise in einer Weise konfiguriert oder benutzt wird, die unsicher ist. Die Analyse der Benutzerfreundlichkeit muss mögliche Betriebsarten des VPN – einschließlich des Betriebs nach Bedien- und Betriebsfehlern – und ihre Konsequenzen für die Aufrechterhaltung eines sicheren Betriebs beschreiben.

Das Prüflabor hat Analysen der Benutzerfreundlichkeit unter Verwendung aller zur Verfügung stehenden Informationen einschließlich des Quellcodes nach undokumentierten oder unvernünftigen Annahmen über die vorgesehene Betriebsumgebung zu überprüfen. Es muss jede Konfigurations- und Installationsprozedur nachvollziehen, um zu überprüfen, ob das VPN sicher konfiguriert und benutzt werden kann.

11.2 Wirksamkeit von VPN-Sicherheitsmechanismen

Im Folgenden werden die Wirksamkeitsaspekte von VPN-Sicherheitsmechanismen untersucht.

Die Untersuchung der Wirksamkeit basiert auf einer Schwachstellenanalyse des VPN-Systems. Bei dieser Analyse werden alle Wege gesucht, die es einem Angreifer erlauben würden, die sicherheitsspezifischen Funktionen und Sicherheitsmechanismen zu deaktivieren, zu umgehen, zu verändern, auszuschalten, direkt anzugreifen oder anderweitig außer Kraft zu setzen. Dabei werden alle zur Verfügung stehenden Informationen, auch der Quellcode, verwendet.

Stärke der Sicherheitsmechanismen, die im VPN-System realisiert sind:

Selbst wenn ein Sicherheitsmechanismus nicht umgangen, außer Kraft gesetzt oder in andere Weise korrumpiert werden kann, kann es dennoch möglich sein, ihn aufgrund von Mängeln in den zugrunde liegenden Algorithmen, Prinzipien oder Eigenschaften durch einen direkten Angriff zu überwinden. Für diesen Aspekt der Wirksamkeit muss die Fähigkeit der Sicherheitsmechanismen bewertet werden, solchen direkten Angriffen zu widerstehen. Der Aspekt der Wirksamkeit unterscheidet sich von anderen Aspekten dahingehend, dass er den Aufwand an Betriebsmitteln betrachtet, die ein Angreifer benötigen würde, um einen erfolgreichen direkten Angriff durchzuführen.

Wirksamkeit von Sicherheitssystemen:

Für die Beurteilung von Sicherheitssystemen ist es ein wichtiges Kriterium, ob die Sicherheitssysteme, die zum Beispiel ein VPN-System bietet, auch tatsächlich geeignet sind, den realen Angriffen entgegenzuwirken.

Im Folgenden wird dargestellt, wie die Wirksamkeit von Sicherheitssystemen generell beurteilt werden kann /ITSEM94/.

In der ersten Grafik werden die Werte einer Organisation, die es vor einem Angriff zu schützen gilt, durch einen Geldsack dargestellt. Die Angriffe, denen ein System ausgesetzt ist, werden durch Nägel repräsentiert, deren Länge proportional zur Größe der Fachkenntnisse, der Gelegenheiten und Ressourcen ist, über die der Angreifer verfügt.

Die Sicherheitsmechanismen, die eingesetzt werden, sind durch eine Wand dargestellt. Die Dicke dieser Wand ist proportional zur Stärke des Sicherheitsmechanismus. Je länger also der Nagel ist, desto schwerwiegender ist die Bedrohung. Je dicker die Wand, desto größer die Fähigkeit der Sicherheitsmechanismen, diese Bedrohung der Werte einer Organisation abzuwehren.

Sicherheitsmechanismen sind dann sicher, wenn die Werte vollständig von einer Wand umgeben sind und die Dicke der Wand auch an ihrer schwächsten Stelle mindestens gleich der Länge des größten Nagels ist.

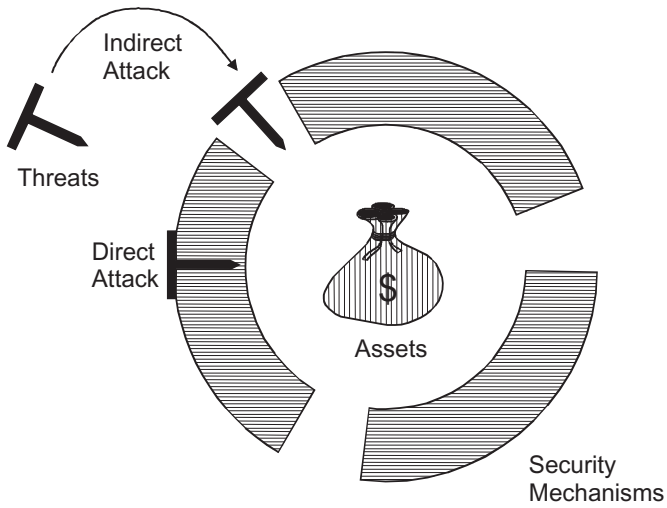


Abb. 11.2: Wirksamkeit

Es kann aber auch der Fall auftreten, dass die gewählten Sicherheitsdienste zur Abwehr der Bedrohung nicht ausreichen, obwohl ihre Sicherheitsmechanismen eigentlich stark genug sind.

Beispiel für »Indirect Attack«:

Ein Angreifer hat die Möglichkeit, zum Beispiel über das eingesetzte Betriebssystem die Rechteverwaltung des VPN-Systems zu verändern.

Grundsätzlich kann die Stärke der Sicherheitsmechanismen von Sicherheitssystemen unterschiedlich bewertet werden. Hierbei wird die Bewertung niedrig, mittel und hoch verwendet.

Eine wichtige Größe für die Bewertung von Sicherheitsmechanismen ist die Mindeststärke des Sicherheitsmechanismus (SoMmin), die notwendig ist, um allen Angriffen erfolgreich entgegenzuwirken.

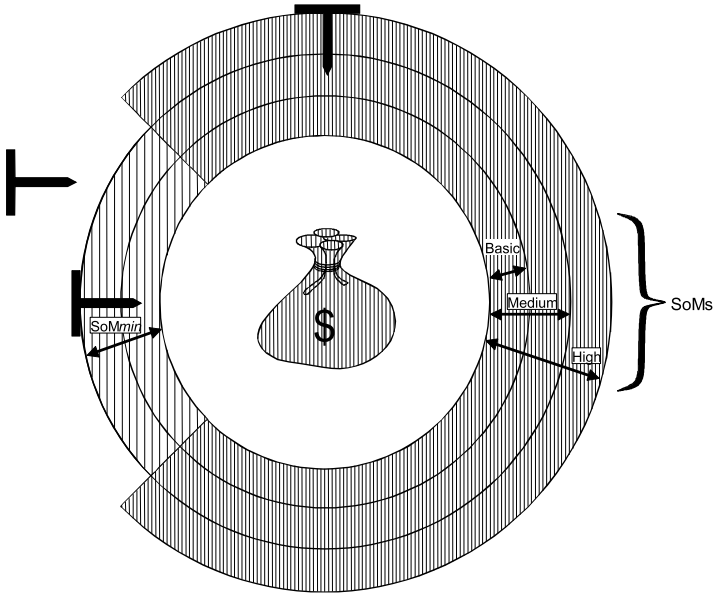


Abb. 11.3: Mindeststärke

Die nun folgenden Bilder sollen verdeutlichen, wie Schwachstellen im VPN-System einzuschätzen sind, wie sie eingeordnet und schließlich wie sie behoben werden können.

Bild (a) zeigt eine erfolgreiche Überwindung der Sicherheitsmechanismen. Die Breite der Wall entspricht nicht der erforderlichen Mindeststärke des Sicherheitsmechanismus und kann daher vom Angreifer überwunden werden.

In Abbildung (b) ist ersichtlich, dass durch die eingesetzten Mechanismen, also Algorithmen, Prinzipien und Eigenschaften, die erforderliche Mindeststärke der Sicherheitsmechanismen gewährleistet ist und der Angriff daher erfolgreich abgewehrt werden kann.

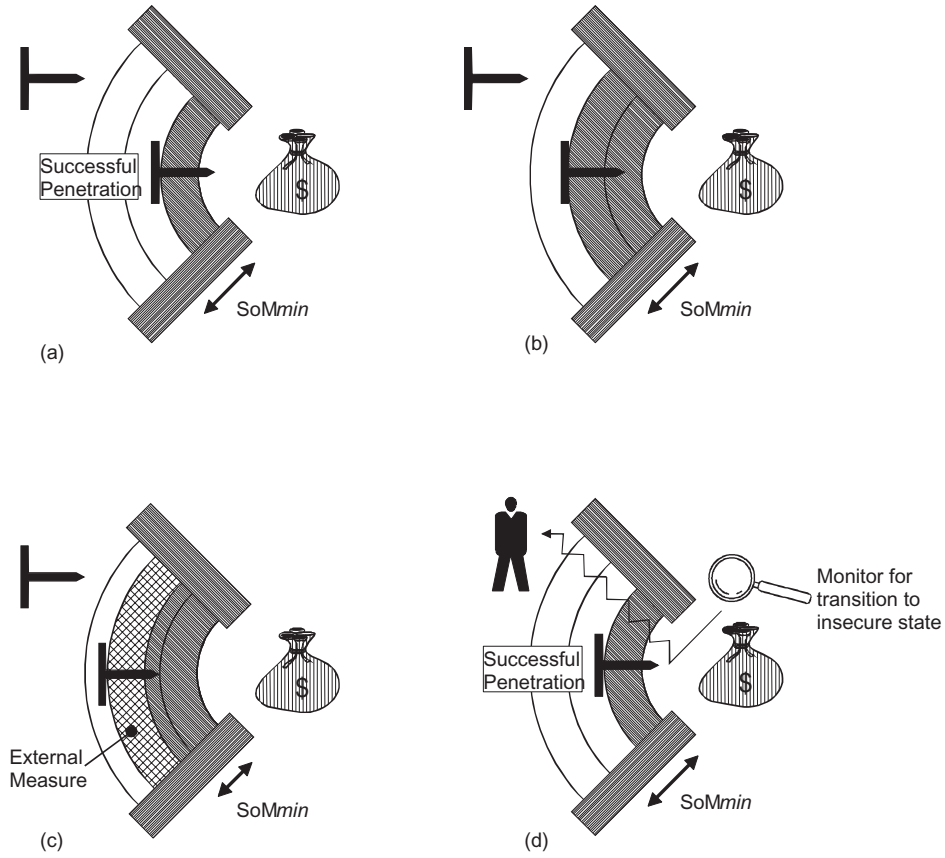


Abb. 11.4: Schwachstellen

Bild (c) stellt dar, wie durch externe Maßnahmen die Wirksamkeit des Sicherheitsmechanismus noch erhöht werden kann, mit dem Ziel, den Angriff abzuwehren.

Im Bild (d) ist dargestellt, dass zwar ein erfolgreicher Angriff nicht verhindert werden konnte, es jedoch möglich ist, den Angriff zu verfolgen, und dass so Maßnahmen eingeleitet werden können, um den Schaden – die Verwundbarkeit – zu reduzieren.

Mechanismenstärke und Evaluationsstufen

Dieser Abschnitt gibt die Mechanismenstärke und die Evaluationsstufen wieder, wie sie in den ITSEC-Kriterien definiert sind.

Mechanismenstärke	Beschreibung
niedrig	Es muss erkennbar sein, dass der Mechanismus Schutz gegen zufälliges Eindringen bietet, während er durch sachkundige Angreifer überwunden werden kann.
mittel	Es muss erkennbar sein, dass der Mechanismus Schutz gegen Angreifer mit beschränkten Gelegenheiten oder Betriebsmitteln bietet.
hoch	Es muss erkennbar sein, dass der Mechanismus nur von Angreifern überwunden werden kann, die über sehr gute Fachkenntnisse, Gelegenheiten und Betriebsmittel verfügen, wobei ein solcher erfolgreicher Angriff als normalerweise nicht durchführbar beurteilt wird.

Tabelle 11.1: Unterscheidung der Mechanismenstärke in den Stufen niedrig, mittel und hoch.

Evaluationsstufe	Beschreibung
E0	Diese Stufe repräsentiert unzureichende Vertrauenswürdigkeit.
E1	Auf dieser Stufe müssen für den EVG die Sicherheitsvorgaben und eine informelle Beschreibung des Architekturentwurfs vorliegen. Durch funktionale Tests muss nachgewiesen werden, dass der EVG die Anforderungen der Sicherheitsvorgaben erfüllt.
E2	Zusätzlich zu den Anforderungen für die Stufe E1 muss hier eine informelle Beschreibung des Feinentwurfs vorliegen. Die Aussagekraft der funktionalen Tests muss bewertet werden. Ein Konfigurationskontrollsystem und ein genehmigtes Distributionsverfahren müssen vorhanden sein.
E3	Zusätzlich zu den Anforderungen für die Stufe E2 müssen der Quellcode beziehungsweise die Hardware-Konstruktionszeichnungen, die den Sicherheitsmechanismen entsprechen, bewertet werden. Die Aussagekraft der Tests dieser Mechanismen muss bewertet werden.
E4	Zusätzlich zu den Anforderungen für die Stufe E3 muss ein formales Sicherheitsmodell Teil der Sicherheitsvorgaben sein. Die sicherheitsspezifischen Funktionen, der Architekturentwurf und der Feinentwurf müssen in semiformaler Notation vorliegen.
E5	Zusätzlich zu den Anforderungen für die Stufe E4 muss ein enger Zusammenhang zwischen dem Feinentwurf und dem Quellcode beziehungsweise den Hardware-Konstruktionszeichnungen bestehen.
E6	Zusätzlich zu den Anforderungen für die Stufe E5 müssen die sicherheitsspezifischen Funktionen und der Architekturentwurf in einer formalen Notation vorliegen, die konsistent mit dem zugrunde liegenden formalen Sicherheitsmodell ist.

Tabelle 11.2: Unterscheidung der Evaluationsstufen

Kapitel 12

VPN-Systeme versus Firewall-Systeme

Der Sicherheitsmechanismus Verschlüsselung bei VPN-Systemen wirkt nur gegen die unerlaubte Einsicht der Informationen während der Kommunikation per Internet. Zusätzlich muss noch – mit Hilfe von Firewall-Systemen – das zweite Hauptrisiko beim Anschluss an das Internet, der unerlaubte Zugriff auf die eigenen Rechnersysteme, verhindert werden.

12.1 Die Idee von Firewall-Systemen

Firewall-Systeme werden als Schranke zwischen ein zu schützendes Netz (zum Beispiel ein internes Unternehmensnetzwerk) und ein unsicheres Netz (zum Beispiel das Internet) geschaltet, so dass der gesamte Datenverkehr zwischen den beiden Netzen nur über das Firewall-System möglich ist. Ein Angreifer darf nicht in der Lage sein, ein Firewall-System zu überwinden.

Ein Firewall-System ist somit das elektronische Äquivalent zu einem Pförtner: Es überprüft, wer aus dem unsicheren Netz auf das zu schützende Netz der Organisation zugreifen darf, und kontrolliert, über welche Protokolle und Dienste zugegriffen und mit welchen Rechnersystemen kommuniziert wird.

Auf dem Firewall-System werden Sicherheitsmechanismen implementiert, die diesen Übergang sicher und beherrschbar machen. Dazu analysiert das Firewall-System die Kommunikationsdaten, kontrolliert die Kommunikationsbeziehungen und Kommunikationspartner, reglementiert die Kommunikation gemäß der Sicherheitspolitik des Unternehmens, protokolliert sicherheitsrelevante Ereignisse und alarmiert bei starken Verstößen den Security Administrator.

Allgemeine Ziele eines Firewall-Systems sind:

- Zugangskontrolle auf der Netzwerkebene
  Es wird überprüft, welche Rechnersysteme (IP-Adressen) über das Firewall-System miteinander kommunizieren dürfen.
- Zugangskontrolle auf der Benutzerebene
  Das Firewall-System überprüft, welche Benutzer über das Firewall-System eine Kommunikationsverbindung aufbauen dürfen. Dazu wird die Echtheit (Authentizität) des Benutzers verifiziert.

- Rechteverwaltung
  Im Rahmen der Rechteverwaltung wird festgelegt, mit welchen Protokollen und Diensten und zu welchen Zeiten eine Kommunikation über das Firewall-System stattfinden darf.
- Kontrolle auf der Anwendungsebene
  Es wird überprüft, ob Kommandos genutzt oder Dateiinhalte übertragen werden, die nicht zu der durch die Anwendung definierten Aufgabenstellung gehören.
- Entkopplung von Diensten
  Dienste werden entkoppelt, damit Implementierungsfehler, Schwachstellen und Konzeptionsfehler der Dienste keine Möglichkeit für Angriffe bieten.
- Beweissicherung und Protokollauswertung
  Verbindungsdaten und sicherheitsrelevante Ereignisse werden protokolliert und können für die Beweissicherung von Handlungen der Benutzer und für die Erkennung von Sicherheitsverletzungen ausgewertet werden.
- Alarmierung
  Besonders sicherheitsrelevante Ereignisse werden an ein Sicherheitsmanagement gesendet, damit bei Sicherheitsverletzungen schnell reagiert werden kann.
- Verbergen der internen Netzstruktur
  Die Kenntnis der Kommunikationswege erleichtert Hackern die Arbeit. Daher ist es wichtig, die Struktur des zu schützenden Netzes gegenüber dem unsicheren Netz geheim zu halten. Das Firewall-System schirmt die Struktur des zu schützenden Netzes nach außen hin ab. Es soll vom unsicheren Netz aus nicht sichtbar sein, ob im zu schützenden Netz 10, 100, 1.000 oder 10.000 Rechnersysteme vorhanden sind.

Ein Firewall-System stellt den »Common Point of Trust« für den Übergang zwischen unterschiedlichen Netzen dar, das heißt der einzige Weg zwischen den Netzen führt kontrolliert über das Firewall-System.

Firewall-Systeme werden eingesetzt, um sich an unsichere Netze wie zum Beispiel das Internet sicher ankoppeln zu können. Sie werden aber auch eingesetzt, um das eigene Netz zu strukturieren und hier Sicherheitsdomänen mit unterschiedlichem Schutzbedarf zu schaffen.

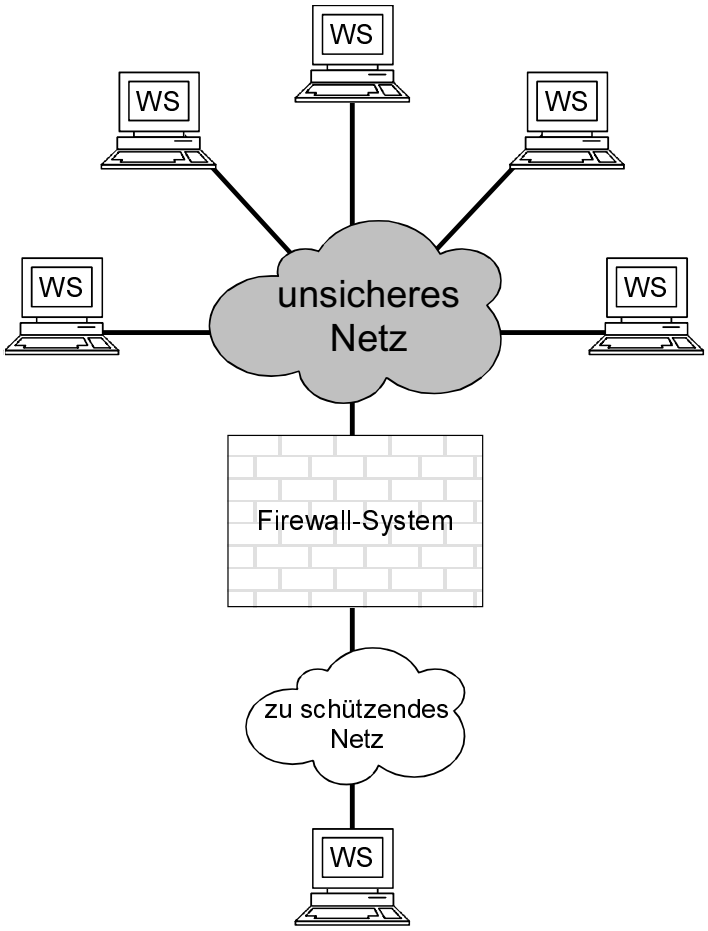


Abb. 12.1: Firewall-System

12.2 Grundsätzliche Unterschiede von VPN- und Firewall-Systemen

In diesem Abschnitt werden die grundsätzlichen Unterschiede von VPN- und Firewall-Systemen dargestellt.

- Geltungsbereich
  - *Firewall-Systeme* schützen eine Organisationseinheit.
  - *VPN-Systeme* schützen die Kommunikation mehrerer Einheiten (Kommunikationspartner) untereinander.

  Typischerweise werden Firewall-Systeme hinter die VPN-Gateways geschaltet.

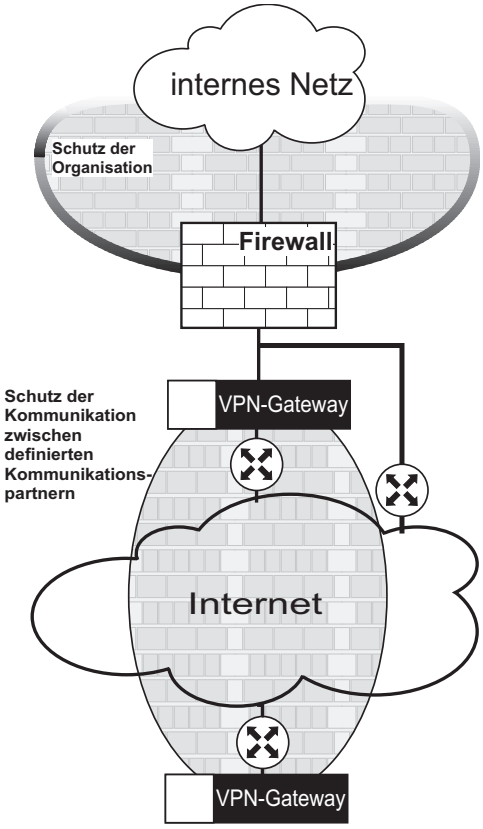


Abb. 12.2: Geltungsbereiche von VPNs und Firewall-Systemen

- Ziele
  - *Firewall-Systeme* schützen vor unerlaubtem Zugriff auf Rechnersysteme und deren Dienste und Daten. Hacker, Cracker, Spione und sonstige Angreifer werden aktiv abgehalten und erlaubte Kommunikationsverbindungen werden auf das für die Aufgabenstellung notwendige Maß reduziert.
  - *VPN-Systeme* schützen vor unerlaubten Zugriff auf die Daten während der Übertragung zwischen definierten Kommunikationspartnern.
- Unabhängigkeit
  - Ein besonderer Aspekt bei *Firewall-Systemen* ist, dass sie lokal verwaltet werden können, das heißt, bezogen auf die Kommunikationsmöglichkeiten und die Protokollierung kann die eigene lokale Sicherheitspolitik unabhängig von anderen realisiert werden.

– Bei *VPN-Systemen* muss die Sicherheitspolitik in Übereinstimmung mit den Kommunikationspartnern realisiert werden, damit eine einheitliche Sicherheit gewährleistet werden kann.

Einige Hersteller bieten in ihren VPN-Lösungen auch Firewall-Funktionalitäten. Diese müssen dann aber auch den Kriterien vom sicheren Aufbau von Firewall-Systemen genügen /Pohl2001a/.

12.3 Kombinationen von VPN- und Firewall-Systemen

Es gibt verschiedene Möglichkeiten, VPN- und Firewall-Systeme miteinander zu kombinieren. In diesem Abschnitt werden die Vor- und Nachteile der unterschiedlichen Kombinationen diskutiert.

Bei der Beschreibung der verschiedenen Anordnungen wird die Sichtweise »von außen«, d.h. aus dem Internet, zugrunde gelegt.

12.3.1 VPN-System vor einem Firewall-System

Bei dieser Kombination steht das Firewall-System hinter den VPN-Gateways. Die Kommunikation, die nicht verschlüsselt werden soll, z.B. der Zugriff auf frei zugängliche Web-Server, wird an den VPN-Gateways vorbeigeführt.

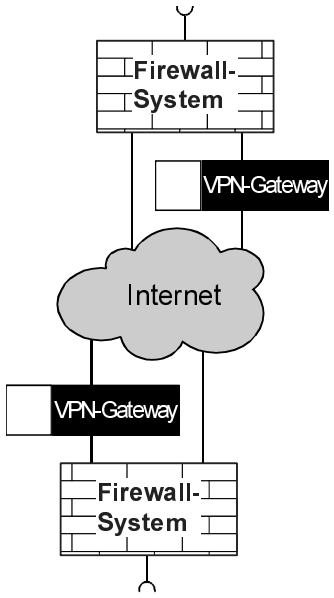


Abb. 12.3: VPN-System vor einem Firewall-System

- **Vorteile:**
  - Der gesamte Datenstrom kann vom Firewall-System analysiert und kontrolliert werden, da er im Klartext vorliegt.
  - Die Verwaltung von Firewall- und VPN-System kann getrennt durchgeführt werden.
- **Nachteile:**
  - Die Daten liegen im Firewall-System im Klartext vor. Dies ist ein Problem, wenn die Verwaltung des Firewall-Systems in der Verantwortung einer Organisation steht, die die Daten nicht lesen soll oder darf. Dieser Fall tritt jedoch in der Praxis selten auf.
  - Da Application Gateways nicht jedes Protokoll (z. B. NetBIOS) unterstützen und dies auch nicht sollen, können evtl. nicht alle Kommunikationsverbindungen durch das Firewall-System geführt werden.

12.3.2 VPN-System vor einem Firewall-System, dahinter ein weiteres VPN-System

Bei dieser Kombination wird ein weiteres VPN-System im Intranet installiert.

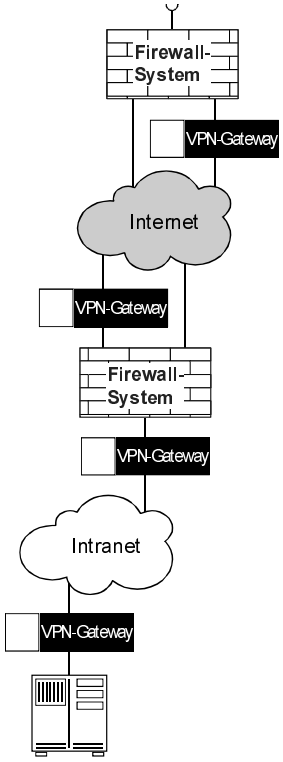


Abb. 12.4: VPN-System vor einem Firewall-System, dahinter ein weiteres VPN-System

- **Vorteile**
  - Es bestehen die gleichen Vorteile wie bei der in Kapitel 12.3.1 *VPN-System vor einem Firewall-System* beschriebenen Anordnung.
  - Die Sicherheitsumgebung ist modular aufgebaut und es können granuläre Regeln verwendet werden.
  - Bei dieser Anordnung kann eine höhere Tiefe der End-to-End-Verschlüsselung erzielt werden.
  - Verschlüsselte Kommunikation kann nur mit Server-Systemen durchgeführt werden, die in den Verbindungsregeln der VPN-Gateways eingetragen sind.

Nähere Informationen hierzu finden Sie in dem Buch »Firewall-Systeme. Sicherheit für Internet und Intranet« von Norbert Pohlmann, MITP-Verlag, 5. Auflage 2002, Kap. 10.2 *Internet Server.*

- **Nachteile**
  - Es bestehen die gleichen Nachteile wie bei der in Kapitel 12.3.1 *VPN-System vor einem Firewall-System* beschriebenen Anordnung.
  - Aufgrund der zusätzlichen Geräte sind die Kosten für Anschaffung und Betrieb hoch.

12.3.3 VPN-System hinter einem Firewall-System

Bei dieser Kombination steht das VPN-Gateway hinter dem Firewall-System. Die Kommunikation, die nicht verschlüsselt werden soll, z. B. der Zugriff auf frei zugängliche Web-Server hinter dem Firewall-System oder in der DMZ, wird an den VPN-Gateways vorbeigeführt.

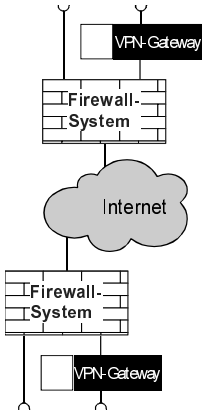


Abb. 12.5: VPN-System hinter einem Firewall-System

- **Vorteile**
  - Hierbei wird eine höhere Tiefe der End-to-End-Verschlüsselung erreicht.
  - Die VPN-Gateways können auch außerhalb des Intranets positioniert werden, z. B. vor dem Ziel-System.
  - Das VPN-System ist optimal vor Angriffen und Manipulationsversuchen aus dem Internet geschützt. Über das Firewall-System können nur die verschlüsselten Dienste (ESP, AH, IKE) auf das VPN-Gateway zugreifen.
- **Nachteile**
  - Das Firewall-System ist nicht in der Lage, den verschlüsselten Datenstrom zu analysieren und zu kontrollieren, da die Daten auf der IP-Ebene (IPSec-Tunnel) verschlüsselt sind. Dies ist dann ein Problem, wenn über die verschlüsselte Kommunikation ein Angriff durchgeführt wird.
  - Da ein Firewall-System typischerweise eine Adressumwandlung (Network Address Translation, NAT) durchführt, können viele VPN-Gateways nicht verwendet werden, da IPSec die NAT-Funktionalität nicht unterstützt. Stattdessen gibt es verschiedene proprietäre NAT-Lösungen (L2TP, NAT traversal u. Ä.).

12.3.4 VPN- und Firewall-System zusammen realisiert

Bei dieser Kombination sind die Firewall- und VPN-Lösung in einem System zusammengefasst.

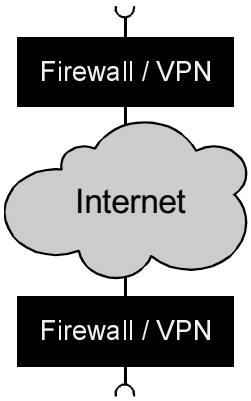


Abb. 12.6: VPN- und Firewall-System zusammen realisiert

- **Vorteile**
  - Typischerweise sind die Kosten geringer.
  - Aufgrund der einheitlichen Verwaltung der Firewall- und VPN-Lösung können transparentere Regeln verwendet werden.

- **Nachteile**
  - Falls eine organisationsübergreifende Verschlüsselung notwendig ist, muss eine VPN-Kommunikation auch mit anderen Lösungen realisiert werden.
  - Da der Geltungsbereich und die Ziele von VPN- und Firewall-Systemen unterschiedlich sind (siehe Kapitel 12.2 *Grundsätzliche Unterschiede von VPN- und Firewall-Systemen*), können Konflikte auftreten.

12.3.5 VPN- und Firewall-System parallel

Bei dieser Kombination arbeiten Firewall- und VPN-System parallel und voneinander unabhängig.

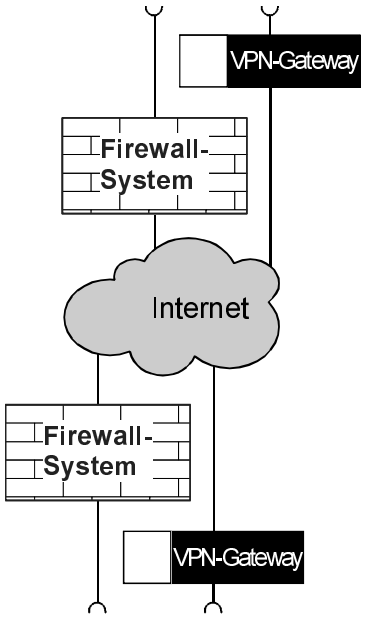


Abb. 12.7: VPN- und Firewall-System parallel

- **Vorteile**
  - VPN- und Firewall-System sind völlig unabhängig voneinander.
- **Nachteile**
  - Die verschlüsselte Kommunikation wird in dieser Kombination nicht analysiert und kontrolliert, da in diesen Kommunikationsweg kein Firewall-System eingebunden ist.
  - Die Sicherheit gegen Angriffe aus dem Internet hängt von der Sicherheit des VPN-Gateways ab.

12.4 Grundelemente von Firewall-Systemen

In diesem Abschnitt wird beschrieben, aus welchen Grundelementen ein Firewall-System aufgebaut werden kann. Es soll aufgezeigt werden, wie technische Sicherheitsmechanismen für Firewall-Elemente realisiert werden können, welche konkreten Möglichkeiten bestehen, um Sicherheit zu gewährleisten, wie sie wirken und wo ihre Grenzen liegen.

Ein Firewall-System kann aus den folgenden Grundelementen bestehen:

- Packet Filter
- Stateful Inspection
- Application Gateway
- Proxies
- Adaptive Proxies

Um die konzeptionellen Unterschiede zu verdeutlichen und so das Verständnis zu erleichtern, werden die einzelnen Firewall-Elemente im Folgendenmit Hilfe von Analogien erläutert.

Eine plastische, leicht fassbare Analogie zu einen Firewall-System ist ein Pförtner. Alle Zugänge zu einem Gebäude sollen vom Pförtner überwacht werden. Hier gilt: Je weniger Zugänge es gibt, desto besser kann der Pförtner den Zugang kontrollieren (Common Point of Trust).

12.4.1 Packet Filter

Das aktive Firewall-Element »Packet Filter« analysiert und kontrolliert die ein- und ausgehenden Pakete auf der Netzzugangs-, der Netzwerk- und der Transportebene. Dazu werden die Pakete (zum Beispiel Ethernet oder Token Ring), die durch das physikalische Kabel übertragen werden, aufgenommen und analysiert. Durch den Packet Filter werden die Netze physikalisch entkoppelt. Ein Packet Filter verhält sich im Normalfall wie eine einfache Bridge. Packet Filter sind nicht nur auf TCP/IP-Protokolle beschränkt.

Ein Packet Filter interpretiert den Inhalt der Pakete und verifiziert, ob die Daten in den entsprechenden Headers der Kommunikationsebenen den definierten Regeln entsprechen. Die Regeln werden so definiert, dass nur die notwendige Kommunikation erlaubt ist und bekannte sicherheitskritische Einstellungen, zum Beispiel die IP-Fragmentierung, vermieden werden. Die Packet Filter werden transparent (als Black Box) in die Leitung eingefügt.

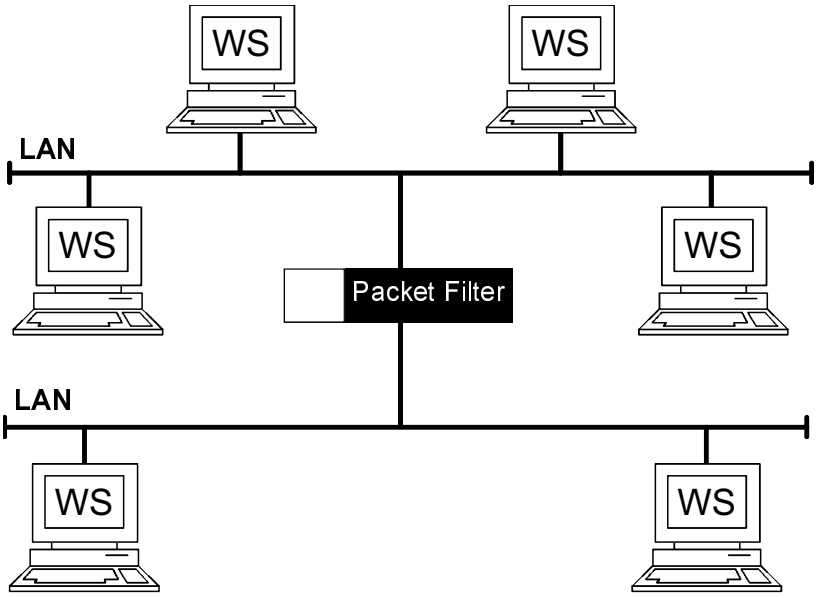


Abb. 12.8: Firewall-Element: Packet Filter

Analogie zum Pförtner:

Wenn der LKW eines Lieferanten am Werktor mit einer Lieferung vorfährt, schaut der »Packet-Filter-Pförtner« auf das Logo an der Seite des LKW, um zu überprüfen, ob es ihm bekannt ist, und lässt den LKW gegebenenfalls unmittelbar durch das Tor, ohne den Lieferschein zu kontrollieren.

Allgemeine Arbeitsweise von Packet Filtern

In der folgenden Abbildung ist die allgemeine Arbeitsweise von Packet Filtern dargestellt. Hier ist zu erkennen, welche Informationen aus den Paketen zur Analyse verwendet werden.

Hier können auf den verschiedenen Kommunikationsebenen unterschiedliche Überprüfungen durchgeführt werden:

- Es wird überprüft, von welcher Seite das Paket empfangen wird (Information aus dem Einbindungsmodul).
- Auf der Netzzugangsebene werden die Quell- und Ziel-Adresse und der verwendete Protokolltyp kontrolliert.

- Auf Netzwerkebene wird je nach Protokoll überprüft:
  - IP-Protokoll: zum Beispiel die Ziel- und die Quell-Adresse und das verwendete Schicht-4-Protokoll, aber auch Optionsfeld und Flags
  - ICMP: die ICMP-Kommandos
  - IPX-Protokoll: zum Beispiel Network/Node
  - OSI-Protokoll: die OSI-Netzwerkadresse
- Auf Transportebene findet
  - bei UDP/TCP zum Beispiel eine Überprüfung der Portnummern (Quell- und Ziel-Port) statt. (Hierüber werden die Dienste wie FTP, Telnet, HTTP definiert.)
  - bei TCP beispielsweise zusätzlich eine Überprüfung der Richtung des Verbindungsaufbaus statt.
- Zusätzlich kann überprüft werden, ob der Zugriff über den Packet Filter in einem definierten Zeitraum durchgeführt wird (zum Beispiel montags bis freitags von 7 Uhr bis 19 Uhr, samstags von 7 bis 13 Uhr, sonntags nicht).

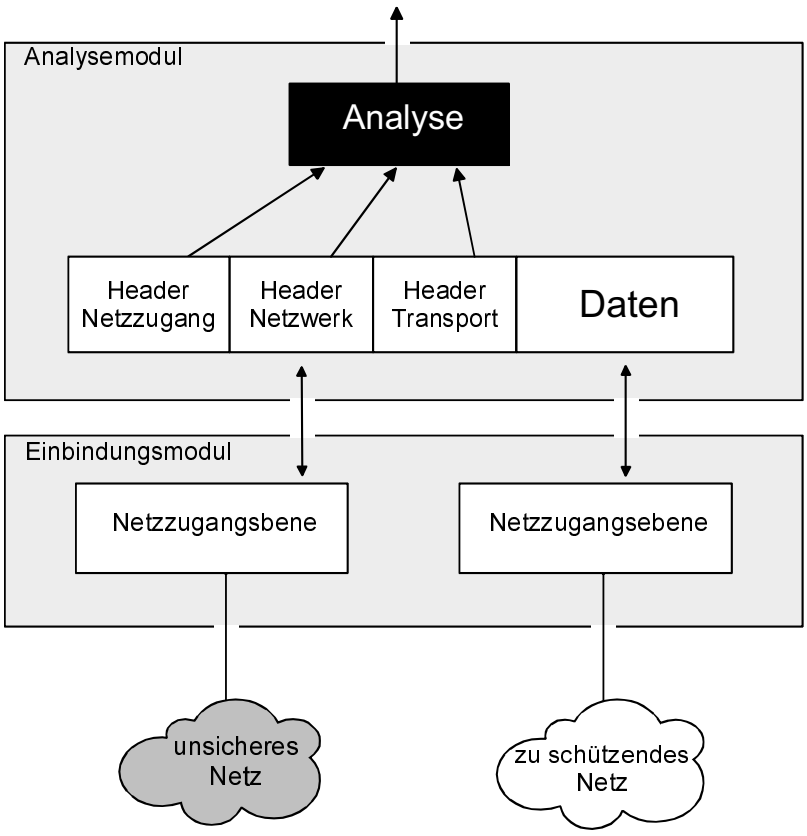


Abb. 12.9: Allgemeine Arbeitsweise eines Packet Filter

Die entsprechenden Prüfinformationen werden dem Regelwerk (Accessliste, Rechteliste) entnommen und mit den Analyse-Ergebnissen verglichen.

Bei Verstoß gegen die Regeln wird dies als sicherheitsrelevantes Ereignis entsprechend protokolliert. Falls diese Option eingerichtet ist, wird eine Spontane Meldung mit den Protokolldaten des sicherheitsrelevanten Ereignisses an das Sicherheitsmanagement gesendet, um eine schnelle adäquate Reaktion zu ermöglichen.

Im Folgenden wird dargestellt, welche Überprüfungen auf den verschiedenen Kommunikationsebenen durchgeführt werden können. Dabei ist zu berücksichtigen, dass die Überprüfung auf der Netzzugangsebene in der Regel bei Intranets im lokalen Bereich zur Anwendung kommt und die Überprüfungen der Netzwerk- und Transportebene bei der Kontrolle der Kommunikation über Internet und Intranets Anwendung finden.

Überprüfungen auf der Netzzugangsebene

Auf der Netzzugangsebene sind unterschiedliche Standards zu unterstützen. Im folgenden werden die Möglichkeiten beim Ethernet aufgezeigt /IEEE1/.

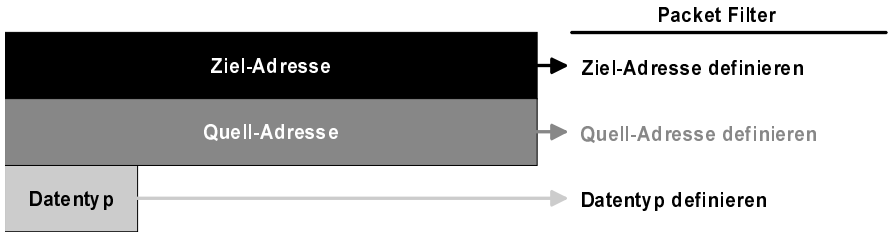


Abb. 12.10: Aufbau des Ethernet MAC-Frame (DIX2)

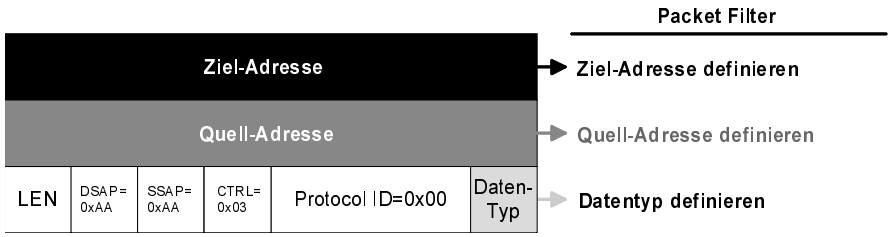


Abb. 12.11: Aufbau des Ethernet MAC Frame (802.3 + 802.2 SNAP)

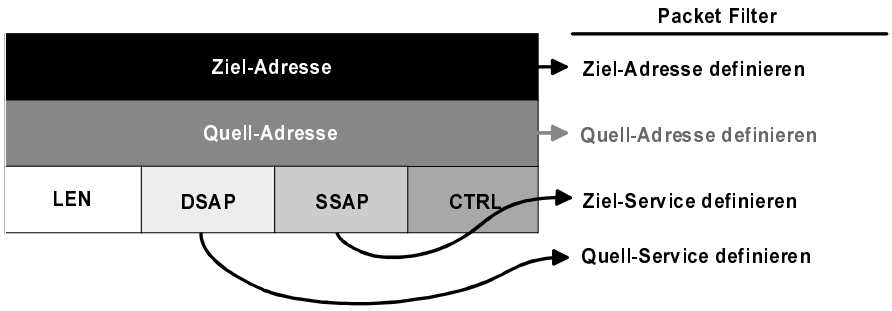


Abb. 12.12: Aufbau des Ethernet MAC Frame (802.3 + 802.2)

Bei Ethernet-Paketen kann der Packet Filter die Ziel- und Quell-Adresse analysieren und im entsprechenden Regelwerk nachsehen, ob die Rechnersysteme, Server und Router, zu denen die Adressen (MAC-Adressen) gehören, eine Kommunikation über den Packet Filter durchführen dürfen oder nicht. Bei Firewall-Systemen kann hier der unmittelbare Kommunikationspartner auf unterster Kommunikationsebene (zum Beispiel Application Gateway, Mail- oder DNS-Server) definiert werden.

Im »Datentyp«-Feld oder DSAP/SSAP-Feld kann festgestellt werden, über welches Kommunikationsprotokoll die Kommunikation auf der nächsthöheren Schicht stattfindet, zum Beispiel IPX, IP, DECNET-Protokolle usw. Die Definitionen für das »Datentyp«-Feld sind in /RFC1700/ festgelegt.

Außerdem wird zum Beispiel bei einer IP-Kommunikation unterbunden, dass mehrere IP-Pakete in einem MAC-Frame enthalten sind. Dabei wird eine Verbindung zwischen der Analyse der Netzzugangs- und Netzwerkebene realisiert. Hier sind in der Vergangenheit Angriffe durchgeführt worden.

Überprüfungen auf der Netzwerkebene

Auf der Netzwerkebene werden im Fall eines IP-Protokolls die Ziel- und Quell-Adresse und das Transport-Protokoll überprüft. Im Fall eines IPX-Protokolls werden Network und Node überprüft.

In Abbildung 12.13 ist dargestellt, welche Möglichkeiten bei IP-Frames (/RFC791/) bestehen, eine Analyse durchzuführen, um die Kommunikation über den Packet Filter zu kontrollieren.

Bei einem IP-Frame werden Ziel- und Quell-Adresse überprüft und festgestellt, ob hier eine Kommunikationsverbindung über den Packet Filter erlaubt ist. Außerdem kann dem »Protokoll«-Feld entnommen werden, welches Transport-Kommunikationsprotokoll verwendet wird. Auch hier kann gegenüber der Rechteliste überprüft werden, ob das entsprechende Transport-Kommunikationsprotokoll (wie TCP oder UDP) verwendet werden darf oder nicht.

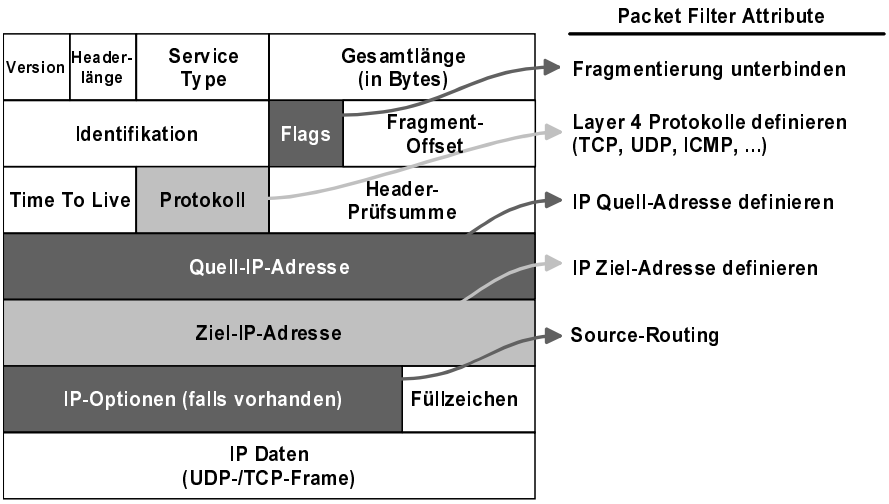


Abb. 12.13: Aufbau des IP-Frame

Dem »Flags«-Feld kann entnommen werden, ob eine Fragmentierung der IP-Pakete durchgeführt wird. Da über Fragmentierungen Angriffe durchgeführt werden können, kann die Fragmentierung über die Festlegung der Rechte unterbunden werden.

Mit Hilfe des »IP-Optionen«-Felds kann festgelegt werden, welche Optionen (Source-Routing etc.) über den Packet Filter verwendet werden dürfen. Hier kann und sollte das Source-Routing unterbunden werden, da über diese Funktion Angriffe durchgeführt werden können.

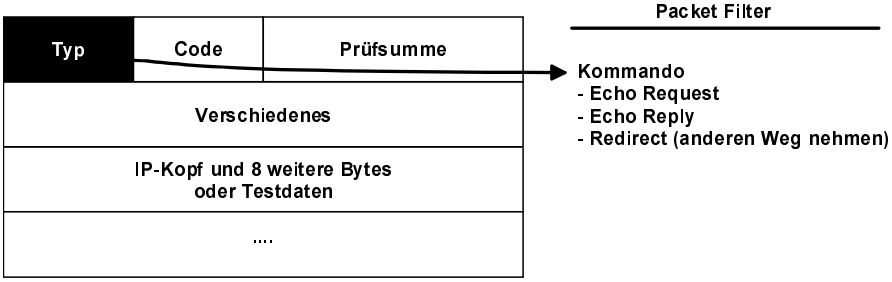


Abb. 12.14: Aufbau des ICMP-Frame

Bei ICMP /RFC792/ kann das »Type«-Feld analysiert werden, in dem die Kommandos definiert sind. Hier können Kommandos wie `EchoRequest`, `EchoReply`, `Redirect`, `Destination Unreachable` etc. erlaubt oder verboten werden. Zum Bei-

spiel werden `EchoRequest` und `EchoReply`, die für den »Ping«-Befehl verwendet werden, erlaubt, aber der Befehl `Redirect`, der für Angriffe benutzt werden kann, verboten. Die Kommandos sind durch RFCs definiert.

Überprüfungen auf der Transportebene

Auf der Transportebene findet im Fall von UDP/TCP (und damit auch indirekt für die TCP/IP-Anwendungen HTTP, FTP, Telnet usw.) eine Überprüfung der Portnummern statt. Im Fall von TCP wird zusätzlich die Richtung des Verbindungsaufbaus überprüft.

- Transportprotokoll – UDP:
  UDP ist ein verbindungsloses Kommunikationsprotokoll, das heißt, die UDP-Pakete werden unabhängig voneinander übertragen. Bei UDP gibt es keine Garantie oder Kontrolle über die korrekte Auslieferung der Pakete. Zwischen dem Aufbau einer neuen UDP-Verbindung oder den Paketen innerhalb einer bestehenden UDP-Verbindung wird nicht unterschieden.

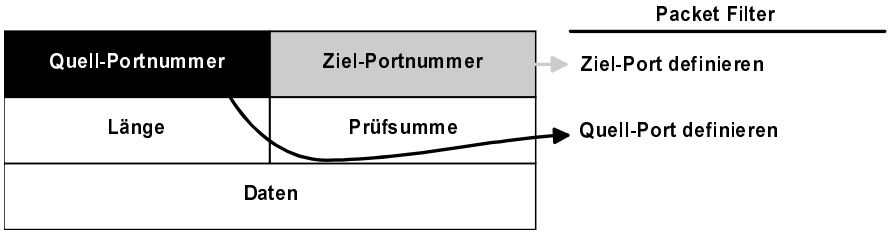


Abb. 12.15: Aufbau des UDP-Frame

Beim UDP-Frame /RFC768/ können durch den Packet Filter Quell- und Ziel-Port analysiert werden. Anhand einer Rechteliste kann bestimmt werden, welche Dienste über UDP gefahren werden können, zum Beispiel SNMP, TFTP usw.

In der Regel sollen UDP-Pakete möglichst nicht zugelassen werden, weil sonst mehr Angriffe realisiert werden können.

- Transportprotokoll – TCP:
  In Abbildung 12.16 ist zu sehen, welche Informationen bei einem TCP-Frame analysiert und kontrolliert werden können.

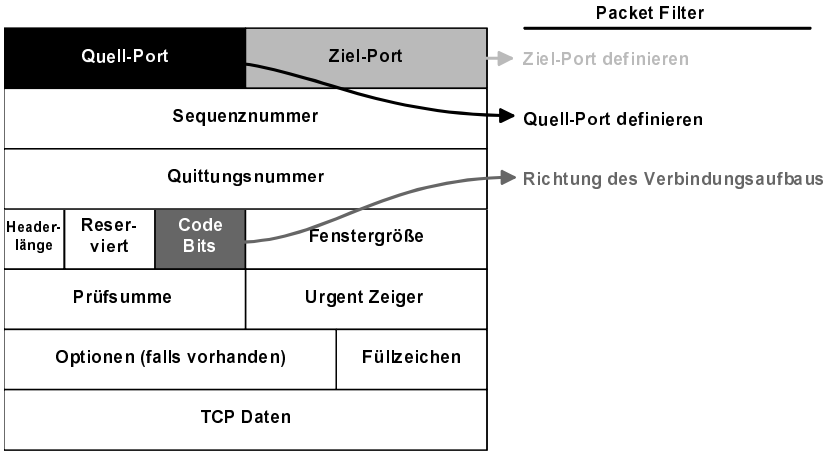


Abb. 12.16: Aufbau des TCP-Frame

Beim TCP-Frame /RFC793/ können durch den Packet Filter wiederum Quell- und Ziel-Port analysiert werden. In einer Rechteliste wird festgelegt, welche Dienste zu welcher Zeit über den Packet Filter erlaubt sind. Außerdem kann dem »Code Bits«-Feld durch die Interpretation des ACK-Bits (acknowledge) entnommen werden, in welche Richtung der Verbindungsaufbau durchgeführt wird. So besteht die Möglichkeit, aus Sicherheitsgründen für den Verbindungsaufbau nur eine bestimmte Richtung zu erlauben (siehe unten das Beispiel für den Einsatz von Packet Filtern).

Überprüfung des Verbindungsaufbaus

TCP ist ein verbindungsorientiertes Kommunikationsprotokoll. Beim Verbindungsaufbau arbeitet TCP immer ohne das ACK-Bit im »Code Bits«-Feld, das heißt ACK=0. Alle weiteren Pakete einer TCP-Verbindung haben dann das ACK-Bit gesetzt, das heißt ACK=1 /ChZw96/. Dadurch sind TCP-basierte Anwendungen besser durch einen Packet Filter zu kontrollieren (siehe Abb. 12.17).

Filterung bei FTP-Verbindungen

Die FTP-Anwendungen /RFC959/ arbeiten mit zwei logischen TCP-Verbindungen: eine für den Austausch der Kommandos, die andere für den Austausch der Daten. Für den Aufbau dieser logischen TCP-Verbindungen gibt es zwei Methoden, die aktive und die passive Methode aus der Sicht des FTP-Clients /ChZw96/.

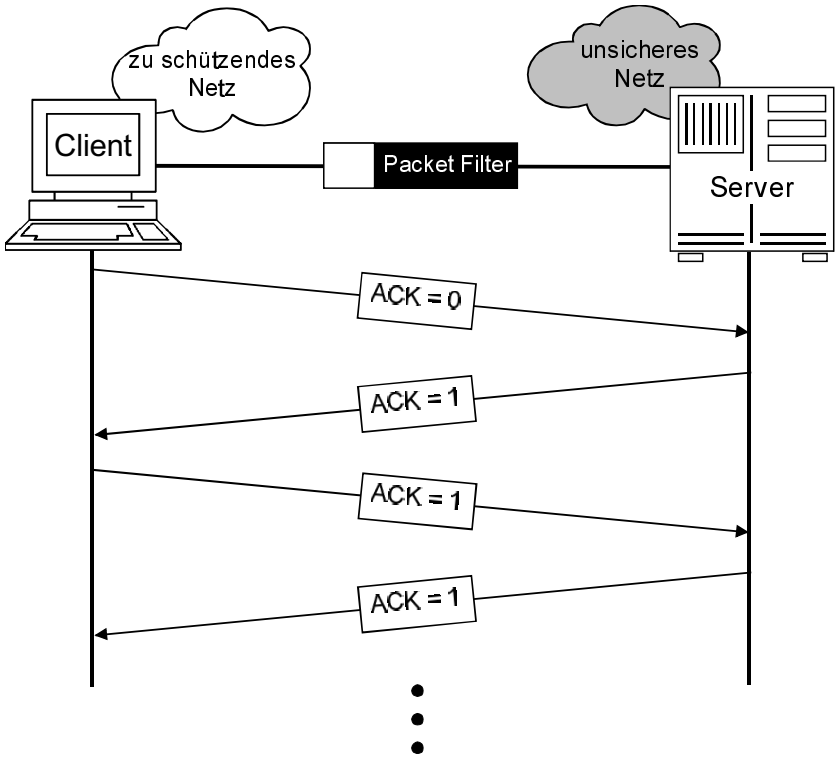


Abb. 12.17: Überprüfung des Verbindungsaufbaus

FTP-Verbindungsaufbau

Bei einem FTP-Verbindungsaufbau nutzt der Client zwei Portnummern oberhalb 1024 (zum Beispiel 4320 und 4321). Über den ersten Port (zum Beispiel 4320) baut er die TCP-Verbindung für die Kommandos auf. Der Server empfängt die Kommandos über den definierten Port 21.

Im folgenden werden die beiden Methoden beschrieben, wie der Datenkanal bei der FTP-Anwendung von den Rechnersystemen aufgebaut werden kann.

- Aktive Methode
  Mit dem Kommando »PORT 4321« teilt der Client dem Server mit, über welche Portnummer er die Daten abwickeln möchte. Der Server sendet die Daten von seinem definierten Port 20 auf die Portnummmer 4321 des Clients.

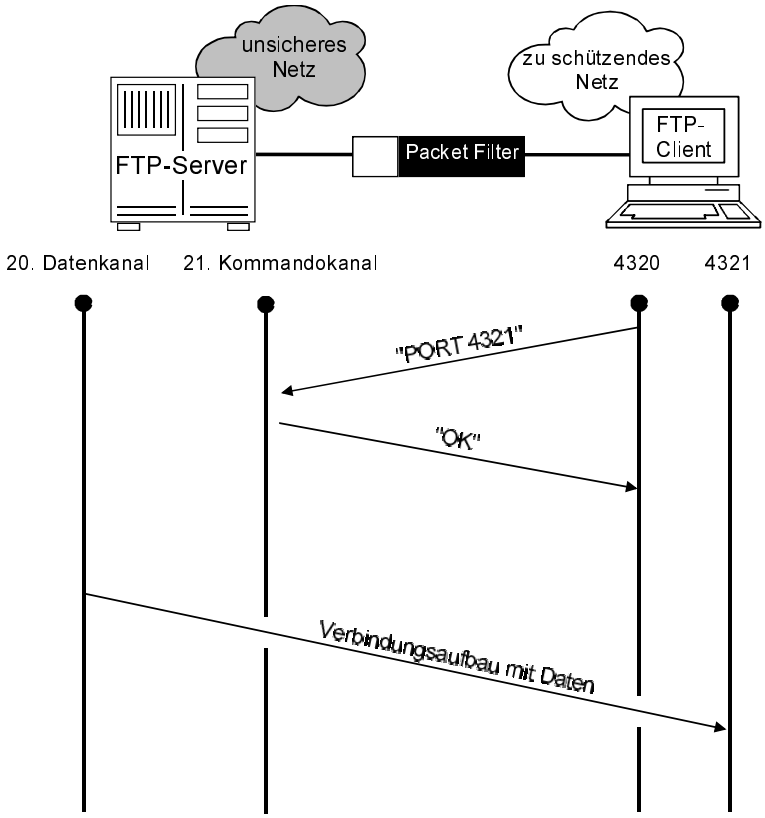


Abb. 12.18: Aktive Methode

Ein Packet Filter, der diese Verbindungen kontrollieren soll, muss für die TCP-Verbindung einen Verbindungsaufbau aus dem unsicheren Netz in das zu schützende Netz ermöglichen. Da dies sicherheitskritisch ist, sollte diese Methode, wenn möglich, nicht verwendet werden. Aus diesem Grund ist es empfehlenswert, die Methode des passiven FTP-Verbindungsaufbaus zu verwenden, bei der der Client den Verbindungsaufbau durchführt.

- Passive Methode
  Bei der passiven Methode baut der Client die TCP-Verbindung auf. Hierdurch kann mit Hilfe eines Packet Filter eine größere Sicherheit erreicht werden. In Abbildung 12.19 ist die passive Methode dargestellt.

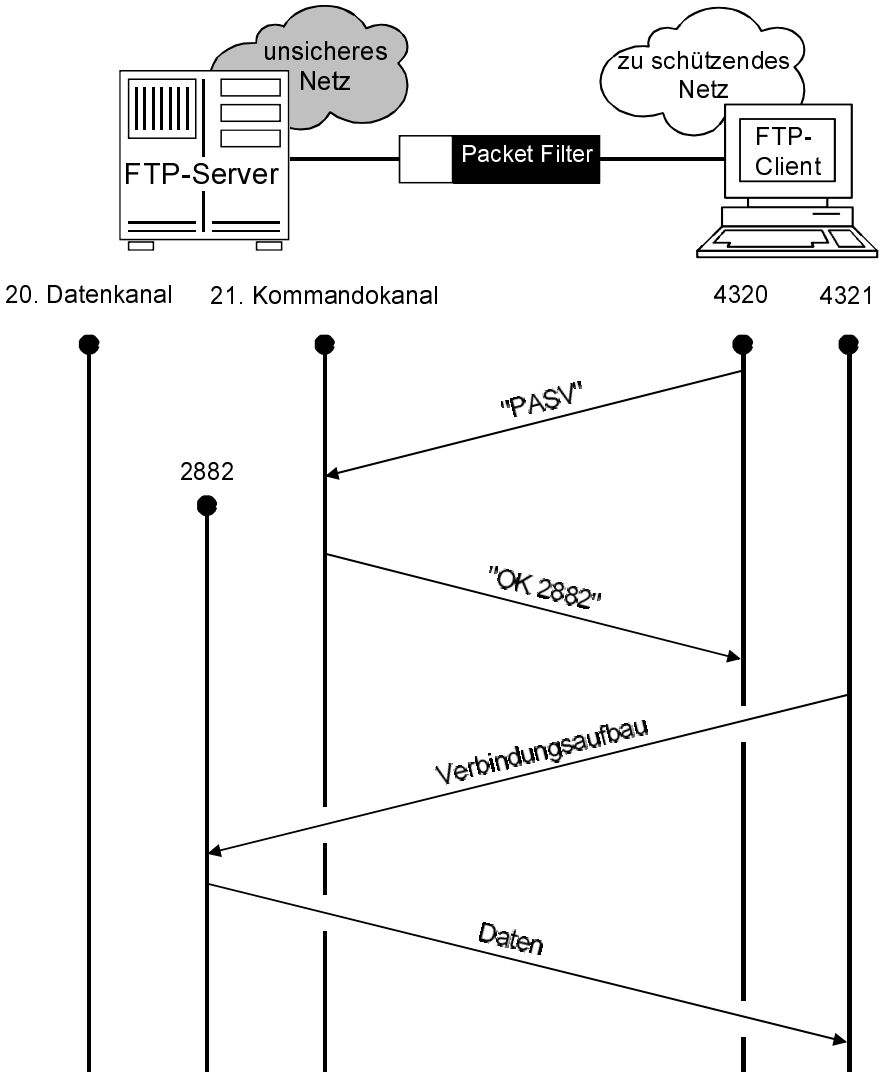


Abb. 12.19: Passive Methode

Aus Sicherheitsgründen ist die passive Methode zu bevorzugen. Dabei ist zu bedenken, dass diese nicht von allen Client- und Server-Realisierungen angeboten wird.

Weitere mögliche Festlegungen:

Zusätzlich sollte in den Packet Filtern pro Filterregel festgelegt werden, zu welchen Zeiten eine Regel (zum Beispiel die Nutzung eines Dienstes) möglich ist, beispielsweise montags bis freitags von 8.00-17.00 Uhr oder samstags von 8.00-12.00 Uhr und sonntags gar nicht.

Strategien für den Aufbau und die Bewertung der Filterregeln

Es gibt unterschiedliche Ansätze, nach denen die Strategie für den Aufbau und die Bewertung von Filterregeln bestimmt werden kann. Im Folgenden sollen zwei Strategien vorgestellt werden.

- Festlegung positiver Filterregeln:
  - Bei dieser Strategie muss genau festgelegt werden, was erlaubt sein soll.
  - Alles, was nicht explizit erlaubt wird, ist automatisch verboten.
  - Das Firewall-Element erlaubt nur das, was explizit in der Access-Liste als »erlaubt« gekennzeichnet ist.
- Festlegung negativer Filterregeln:
  - Zunächst ist alles grundsätzlich erlaubt.
  - Durch spezielle Einträge kann festgelegt werden, was verboten sein soll.
  - Der Packet Filter verhindert nur das, was explizit in der Access-Liste als »nicht erlaubt« gekennzeichnet ist.
- Bewertung:
  Positive Filter sind zu bevorzugen, weil hier nicht durch Unbedachtsamkeit ein Eintrag (Verbot) vergessen werden und dadurch ein Sicherheitsproblem entstehen kann. Negative Filter sind mit Vorsicht zu behandeln, weil durch ungeschickte Festlegungen oder das Vergessen von Einträgen sicherheitskritische Einstellungen auftreten können.

Dynamischer Packet Filter

Im folgenden Abschnitt wird die Arbeitsweise von dynamischen Packet Filtern beschrieben /Bo0l96/. Bei verbindungslosen Kommunikationsverbindungen, wie zum Beispiel UDP, kann nicht festgestellt werden, von wem ein Verbindungsaufbau durchgeführt wird. Dynamische Packet Filter besitzen im Fall der Verwendung des UDP-Protokolls ferner die Eigenschaft, sich für nach »außen« geschickte UDP-Pakete die Quell- und Ziel- IP-Adressen und Ports zu merken, und nur die entsprechenden passenden »Antworten« der virtuellen Verbindung zu erlauben. Das bedeutet, dass nur Antwortpakete durchgelassen werden, die vom gleichen Rechnersystem und dem gleichen Port kommen, an die das ursprüngliche UDP-Paket gesendet worden ist, und die entsprechend zum gleichen Rechnersystem und gleichen Port zurückgesendet werden. Packet Filter, die diese Eigenschaft besitzen, werden als »dynamisch« bezeichnet, weil die Filterregeln intern dynamisch ange-

passt werden. Die angepassten Regeln für die Antwort gelten nur temporär und werden nach einer zu definierenden Zeit, falls keine Antwort kommt, automatisch durch den dynamischen Packet Filter selbst gelöscht.

Der Abbildung 12.20 ist zu entnehmen, welche Informationen (Quelladresse und -port, Zieladresse und -port sowie die Zeit, wann das Paket übertragen wurde) im dynamischen Packet Filter festgehalten werden, damit eine genaue Zuordnung stattfinden kann. Diese Eigenschaft kann auch für TCP-Verbindungen verwendet werden /ChZw96/.

Dienste wie SNMP können über Packet Filter, die diese Eigenschaft besitzen, sicherer angeboten werden.

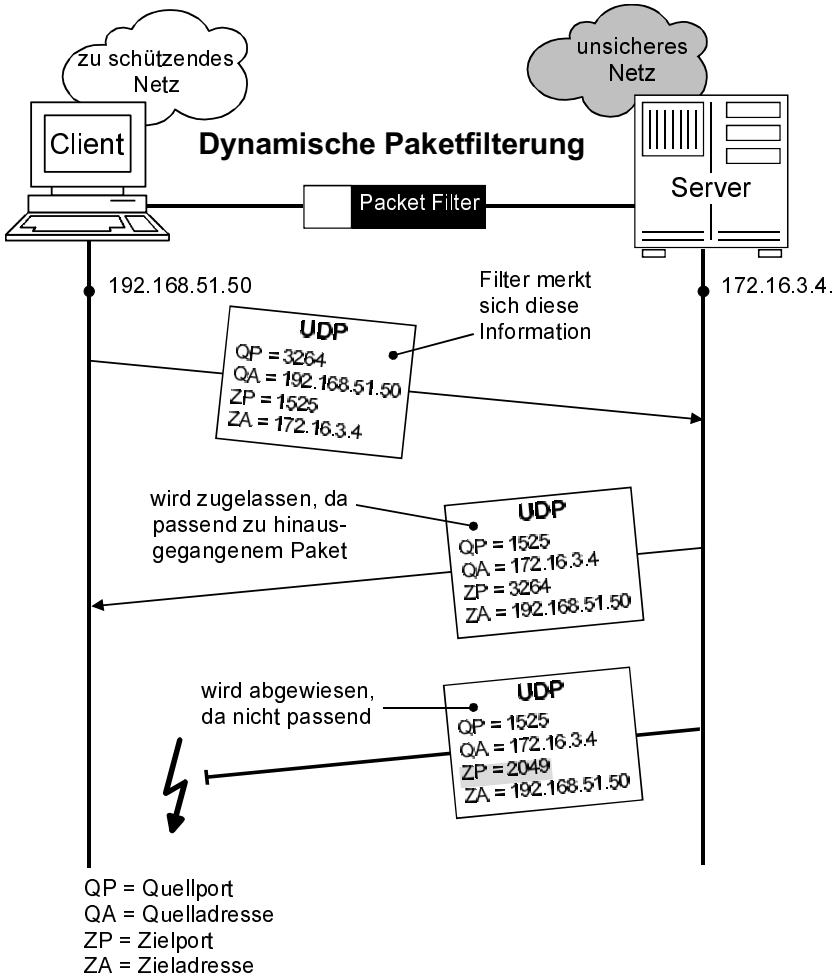


Abb. 12.20: Dynamischer Packet Filter

Anwendungsgebiete von Packet Filtern

Ein Firewall-System, das nur auf Packet Filtern aufbaut, wird sicherlich nicht für die Kopplung eines zu schützenden Netzes an das Internet eingesetzt werden können, da der Schutzbedarf der meisten zu schützenden Netze für die Kontrollmöglichkeiten eines Packet Filter zu hoch ist.

Packet Filter werden zum Aufbau von High-level Security Firewall-Systemen und für die kontrollierte Kommunikation im Intranet verwendet. Für diese Anwendungen ist besonders die Verwendung von Packet Filtern, die gleichzeitig verschlüsseln, eine wirkungsvolle Sicherheitskomponente, mit der Internet- und Intranet-Anwendungen sicher und beherrschbar realisiert werden können.

Möglichkeiten, Vorteile und besondere Aspekte von Packet Filtern

- transparent, das heißt unsichtbar für den Benutzer und die Rechnersysteme und ohne ihre aktive Einwirkung tätig (Ausnahme: wenn eine Authentikation notwendig ist)
- einfach erweiterungsfähig für neue Protokolle
- flexibel für neue Dienste
- für andere Protokollfamilien verwendbar (IPX, OSI, DECNET, SNA, ...)
- hohe Performance durch optimale Mechanismen (Betriebssystem, Treiber usw.)
- leicht realisierbar, da geringere Komplexität

Nachteile und Grenzen von Packet Filtern

- Daten, die oberhalb der Transportebene liegen, werden in der Regel nicht analysiert.
- Für die Anwendungen (FTP, HTTP, ...) besteht keine Sicherheit; so können bei der Freischaltung von SMTP (Port 25) Angriffe über Sendmail auf die Rechnersysteme des zu schützenden Netzes durchgeführt werden.
- Falsch konfigurierte Programme auf Rechnersystemen im zu schützenden Netz können bei erlaubten Kommunikationsverbindungen von außen genutzt werden, da ein direkter Zugriff auf das Rechnersystem besteht.
- Typische Packet Filter können die Struktur des zu schützenden Netzes nicht verbergen.
- Protokolldaten werden nur bis zur Transportebene zur Verfügung gestellt.

12.4.2 Zustandsorientierte Packet Filter (stateful inspection)

Der Leistungsumfang von Packet Filtern kann erweitert werden, indem die Interpretation der Pakete auch auf höheren Kommunikationsebenen durchgeführt wird. In diesem Fall werden die Pakete zum Beispiel auch auf der Anwendungsebene interpretiert und Statusinformationen für jede aktuelle Verbindung auf den unterschiedlichen Kommunikationsebenen bewertet und festgehalten.

Analogie zum Pförtner:

Wenn eine Lieferung ankommt, dann schaut der Pförtner nicht nur auf die Adressen, sondern auch auf den Lieferschein, um zu überprüfen, ob in dem Paket etwas Verbotenes steckt. Das ist eine gute Überprüfung, jedoch nicht so sicher wie das tatsächliche Öffnen des Pakets und die Überprüfung des Inhalts. Wenn das Paket akzeptabel aussieht, dann öffnet der Pförtner das Tor und gestattet dem Fahrer des LKW die Zufahrt auf das Werksgelände.

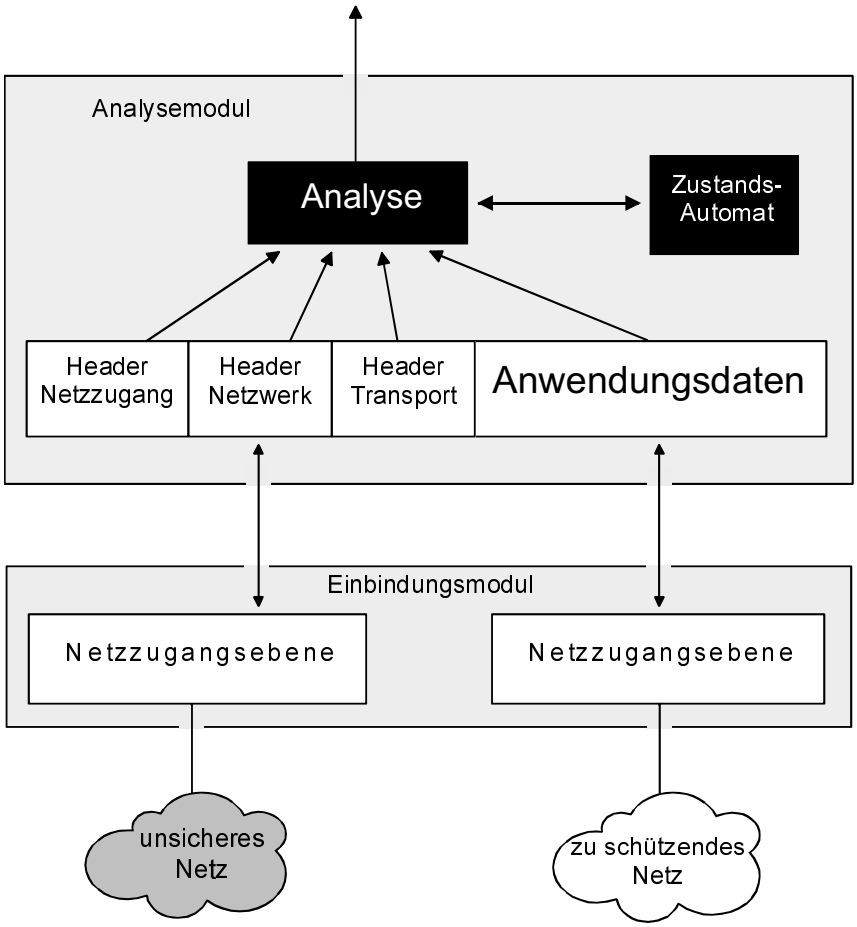


Abb. 12.21: Zustandsorientierte Packet Filter

Die Statusinformationen können in Form von »Zuständen« mit den entsprechenden Informationen festgehalten werden. Zustände sind zum Beispiel Verbindungsaufbau, Transferzustand oder Verbindungsabbau für die jeweilige Kommunikationsebene. In jedem Zustand kann dann eine spezielle Interpretation der

Kommunikationsdaten erfolgen. In der Literatur werden solche erweiterten zustandsorientierten Packet Filter »stateful inspection«, »smart filtering« oder »adaptive screening« genannt. Mit dieser erweiterten Funktionalität werden sie oft als benutzerorientierte Packet Filter angeboten.

Diese zustandsorientierten Packet Filter haben die Vorteile von Packet Filtern, können aber zusätzlich die Anwendungen kontrollieren. Einige Risiken bleiben, weil keine direkte Entkopplung der Dienste realisiert ist (siehe die Beschreibung der Proxies auf Application Gateways und ihrer Vorteile).

Das gleichzeitige Festhalten und Interpretieren der Kommunikationsdaten auf den verschiedenen Kommunikationsebenen ist sehr komplex. Aus diesem Grund haben zustandsorientierte Packet Filter in der Regel eine geringere Tiefe der Analyse oder sind besonders fehleranfällig, da sie eine sehr mächtige Software haben. Prinzipiell ist es auch nicht möglich, die komplexe Software von zustandsorientierten Packet Filtern soweit auszutesten, dass nachweislich in keinem Betriebszustand Fehler auftreten können. Aus diesem Grund muss auch in Zukunft immer wieder damit gerechnet werden, dass die komplexen Programme potentielle Sicherheitsrisiken aufweisen, die für Angriffe verwendet werden können / Kupp99/.

Möglichkeiten, Vorteile und besondere Aspekte von zustandsorientierten Packet Filtern

- Zustandsorientierte Packet Filter arbeiten transparent, das heißt unsichtbar für den Benutzer und die Rechnersysteme und ohne ihre aktive Einwirkung (Ausnahme: wenn eine Authentikation notwendig ist).
- Sie sind einfach erweiterungsfähig für neue Protokolle und flexibel für neue Dienste.
- Eventuell sind sie auch für andere Protokollfamilien verwendbar (IPX, OSI, DECNET, SNA...).

Nachteile und Grenzen von zustandsorientierten Packet Filtern

- Zustandsorientierte Packet Filter stellen eine komplexe Lösung dar.
- Falsch konfigurierte und fehlerbehaftete Programme auf Rechnersystemen im zu schützenden Netz können bei erlaubten Kommunikationsverbindungen von außen genutzt werden, da ein direkter Zugriff auf das Rechnersystem besteht.
- Typische zustandsorientierte Packet Filter können die Struktur des zu schützenden Netzes nicht verbergen.

Ein besseres und sicheres Konzept der Analyse der Anwendungsdaten ist das Konzept von Application Gateways mit Proxies, das im folgenden Abschnitt beschrieben wird.

12.4.3 Application Gateway / Proxy-Technik

Im Folgenden wird die Arbeitsweise des aktiven Firewall-Elements »Application Gateway« beschrieben. Es zeichnet sich dadurch aus, dass es die Netze sowohl logisch als auch physikalisch entkoppeln kann.

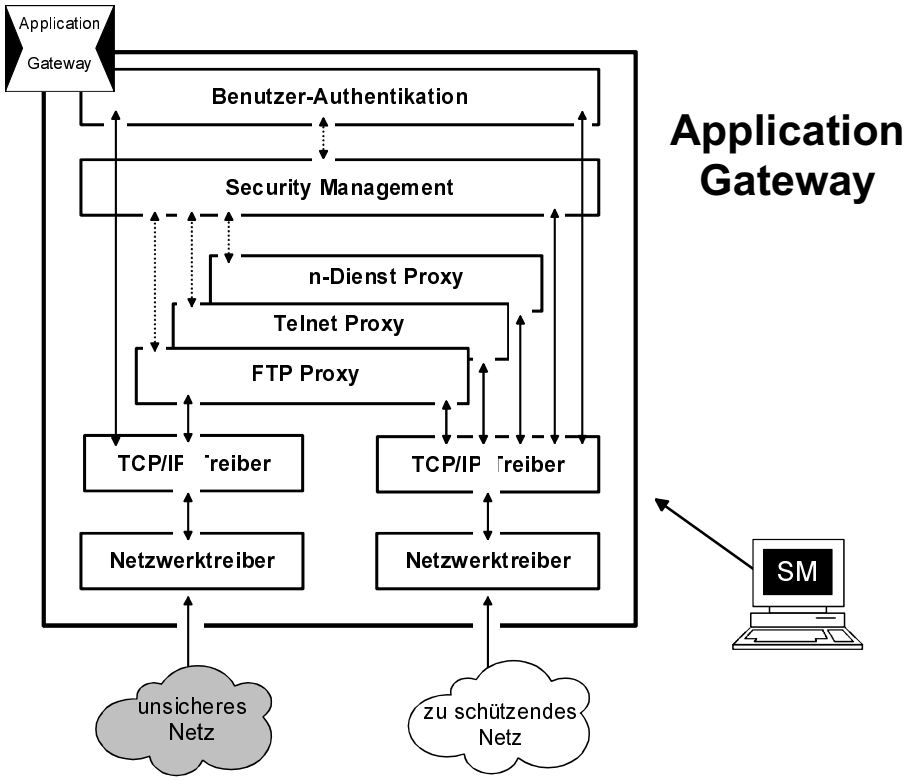


Abb. 12.22: Application Gateway

Da in einigen Firewall-Konzepten das Application Gateway das einzige vom unsicheren Netz (zum Beispiel Internet) aus erreichbare Rechnersystem ist, muss das Application Gateway besonders geschützt werden. Aus diesem Grund wird das Rechnersystem, auf dem das Application Gateway realisiert ist, auch als Bastion bezeichnet.

Das Application Gateway – als Dual-homed Gateway realisiert – arbeitet mit zwei Netzwerk-Anschlüssen. »Dual-homed« bedeutet, daß das Application Gateway die vollständige Kontrolle über die Pakete hat, die zwischen dem unsicheren und dem

zu schützenden Netzwerk übertragen werden sollen. Das Dual-homed Application Gateway besitzt zwei Netzwerkkarten, eine im zu schützenden Netz, eine weitere im unsicheren Netzwerk /SiHa95/.

Das Application Gateway kann auch »Single-homed« mit nur einem Netzwerkanschluss betrieben werden. Dann besteht jedoch die Möglichkeit, daß ein Angreifer das Application Gateway übergeht.

Analogie zum Pförtner:

Der »Application-Gateway-Pförtner« schaut nicht nur die Adressen der eingehenden Lieferungen an, er öffnet auch jedes Paket, prüft den kompletten Inhalt und checkt die Arbeitspapiere des Absenders gegen eine klar festgelegte Reihe von Beurteilungskriterien. Nach der erfolgten detaillierten Sicherheitsüberprüfung unterzeichnet der Pförtner den Lieferschein und schickt den LKW wieder auf seinen Weg. Statt dessen bestellt er einen vertrauenswürdigen Fahrer der eigenen Firma, der nun die Pakete zum eigentlichen Empfänger bringt. Die Sicherheitskontrolle ist an dieser Stelle wesentlich zuverlässiger und der Fahrer der Fremdfirma erhält keinen weiteren Einblick in das Firmengelände. Die Überprüfungen nehmen zwar mehr Zeit in Anspruch, dafür können jedoch sicherheitsgefährdende Aktivitäten ausgeschlossen werden.

Allgemeine Arbeitsweise des Application Gateway

Ein Benutzer, der über das Application Gateway kommunizieren möchte, muss sich zuerst identifizieren und authentisieren. Application Gateways bieten in der Regel unterschiedliche Authentikationsverfahren an.

Aus diesem Grund baut der Benutzer zuerst eine Verbindung mit dem Application Gateway auf. Sein direkter Kommunikationspartner ist nicht das Ziel-Rechnersystem, sondern das Application Gateway. Nach der Identifikation und Authentikation arbeitet das Application Gateway aber transparent, so dass der Benutzer den Eindruck hat, direkt auf dem Ziel-Rechnersystem zu arbeiten.

Ansatz

Über die Netzzugangs- und TCP/IP-Treiber empfängt das Application Gateway die Pakete an den entsprechenden Ports. Soll nur ein Dienst über einen entsprechenden Port möglich sein, muss auf dem Application Gateway eine Software zur Verfügung gestellt werden, die das entsprechende Paket von der einen Netzwerkseite zur anderen Netzwerkseite des Application Gateway überträgt und umgekehrt. Eine solche Software, die die Paketübertragung nur für einen speziellen Dienst (FTP, HTTP, Telnet, usw.) im Application Gateway durchführt, wird als Proxy bezeichnet (siehe Abb. 12.22).

Der Name »Proxy« (=Stellvertreter) wird verwendet, weil es aus Sicht des zugreifenden Benutzers so aussieht, als würde er mit dem eigentlichen Serverprozess des Dienstes auf dem Ziel-Rechnersystem kommunizieren.

Jeder Proxy auf dem Application Gateway kann speziell für den Dienst, für den er zuständig ist, weitere Sicherheitsdienste anbieten. Bedingt durch den jeweiligen speziellen Proxy und das Wissen um den Kontext eines speziellen Dienstes ergeben sich umfangreichere Sicherungs- und Protokollierungsmöglichkeiten im Application Gateway (siehe dazu die Beschreibungen der speziellen Proxies).

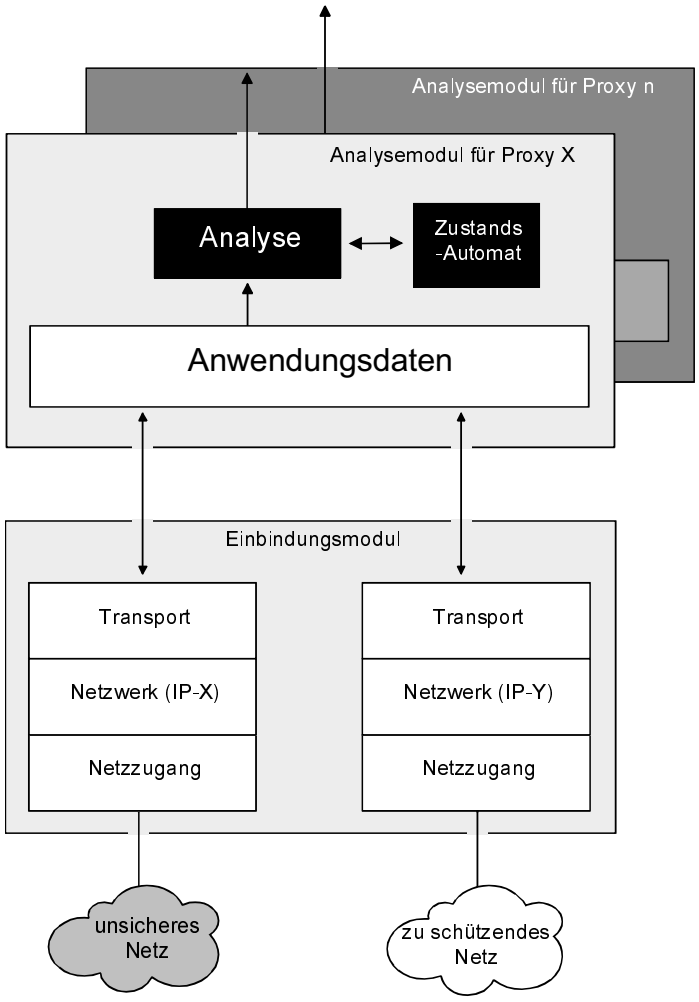


Abb. 12.23: Analysemodule für Proxies auf dem Application Gateway

Die Analyse ist auf dieser Kommunikationsebene besonders intensiv möglich, da der Kontext der Anwendungsdaten für den jeweiligen Dienst klar definiert ist. Die Proxies konzentrieren sich auf das Wesentliche. Der Vorteil ist, dass kleine, überschaubare Module verwendet werden, wodurch die Fehleranfälligkeit durch Implementierungsfehler reduziert wird (siehe Abb. 12.23).

Eventuell wird im Proxy auch eine Umverschlüsselung oder Umcodierung durchgeführt.

Sicherheitskonzept eines Application Gateway:

Für jeden Dienst, der über das Application Gateway möglich sein soll, muss ein spezieller Proxy zur Verfügung gestellt werden.

Sollen bestimmte Dienste generell nicht möglich sein, dann darf für diese Dienste kein Proxy auf dem Application Gateway vorhanden sein, aber auch keine weitere Software, die den Dienst ermöglichen könnte!

Aus diesem Grund ist so wenig Software wie möglich auf dem Application Gateway zu installieren, damit nicht zufällig – oder absichtlich durch einen Angreifer von außen provoziert – eine andere Software die Aufgabe eines Proxy (Paketübertragung im Application Gateway) für einen Dienst übernimmt, der nicht erlaubt sein soll.

Das Sicherheitsmanagement, das dem Benutzer die Arbeit so leicht wie möglich gestalten soll und deshalb mit einer mächtigen Software (X-Terminal, Datenbank etc.) ausgestattet ist, darf aus Sicherheitsgründen nicht auf dem selben Rechnersystem oder zumindest nicht zur gleichen Zeit wie das Application Gateway laufen.

Application Gateways sollen aus Sicherheitsgründen keine Routing-Funktionalität haben, damit nicht an den Proxies vorbeigeroutet werden kann /Stol98/.

Da das Application Gateway bei der Kommunikation jeweils zum Rechnersystem des unsicheren Netzes und zu dem des zu schützenden Netzes eine Kommunikationsverbindung hat, bietet es eine »Network Address Translation«. Dazu hat das Application Gateway eine IP-Adresse im unsicheren Netz (zum Beispiel eine offizielle Internet-IP-Adresse 194.173.3.1) und eine IP-Adresse im zu schützenden Netz (zum Beispiel eine für diesen Zweck reservierte IP-Adresse 192.168.1.60). Bei der Kommunikation mit den Rechnersystemen des unsicheren Netzes verwendet das Application Gateway die IP-Adressen des unsicheren Netzes, bei der Kommunikation mit den Rechnersystemen des zu schützenden Netzes die IP-Adressen des zu schützenden Netzes.

In den Logbüchern des Application Gateway können eine Vielzahl von Informationen festgehalten werden. Schon in der Sicherheitspolitik einer Organisation sollte festgelegt werden, welche Informationen protokolliert werden sollen und welche nicht, da die Datenmenge sonst sehr groß werden kann und einen hohen administrativen Aufwand verursacht.

12.4.4 Proxies

Bei der Realisierung von Proxies wird zwischen Application Level Proxies und Circuit Level Proxies unterschieden.

Außerdem gibt es weitere spezielle Proxies, die für bestimmte Applikationen wiederum zusätzliche, auf diese Dienste zugeschnittene Sicherheitsdienste zur Verfügung stellen. Es können auch für nicht-standardisierte Dienste Proxies realisiert werden.

Application Level Proxies

Application Level Proxies sind für bestimmte Dienste/Anwendungen implementiert. Das heißt, dass sie die Kommandos der Anwendungsprotokolle kennen und diese analysieren und kontrollieren können. Application-Level Proxies arbeiten mit der gängigen, unveränderten Client-Software für FTP oder Telnet oder auch mit Browsern zusammen. Bei Application Level Proxies ist aber für die benutzerorientierten Dienste oft eine veränderte Vorgehensweise notwendig, zum Beispiel ist zuerst eine Identifikation und Authentikation mit dem Application Level Proxy notwendig und anschließend wird dem Benutzer eine transparente Kommunikation zur Verfügung gestellt (siehe hierzu auch die Kommunikation über Application Level Proxies).

Im Folgenden werden einige Application Level Proxies am Beispiel bestimmter Realisierungsarten näher beschrieben, um das Grundprinzip der Proxy-Technik darzustellen. Einige Proxies funktionieren nach dem Store-and-Forward-Prinzip (SMTP), andere interaktiv und benutzerorientiert (Telnet, FTP, HTTP, ...).

SMTP Proxy

Abbildung 12.24 zeigt, wie ein SMTP Proxy, der nach dem Store-and-Forward-Prinzip arbeitet, aufgebaut werden kann. Store-and-Forward-Prinzip bedeutet, dass der MTP Proxy die Mail vollständig annimmt, zwischenspeichert und dann weitersendet. Hierfür ist keine End-to-End-Beziehung zwischen dem eigentlichen Sender und Empfänger notwendig.

Analogie zum Sammelbriefkasten (Mail Proxy):

Ein Mail Proxy kann mit einem Sammelbriefkasten einer Organisation verglichen werden. Möchte jemand einer Organisation einen Brief senden, so wirft er diesen direkt oder indirekt in den Sammelbriefkasten der Organisation. Die Briefe wer-

den dort von der internen Poststelle entgegengenommen und mit einem Boten der eigenen Organisation verteilt. Die externen Briefboten brauchen die Organisation also nicht zu betreten und stellen somit auch kein Risiko dar. Der Schlitz nach außen definiert die potenzielle Angriffsfläche.

Bei SMTP Proxies gibt es Lösungen, die ohne oder mit einem auf dem gleichen System vorhandenen MTA (Message Transfer Agent) arbeiten. In diesem Beispiel wird ein SMTP Proxy mit vorhandenem MTA beschrieben.

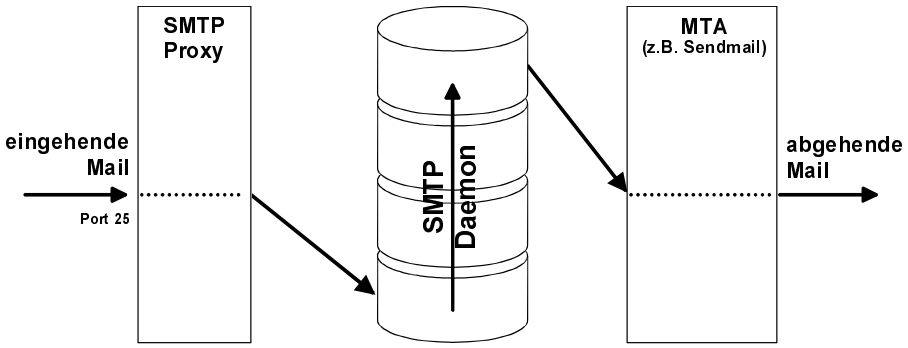


Abb. 12.24: SMTP Proxy

Beschreibung:

Der SMTP Proxy arbeitet nicht benutzerorientiert. Aus diesem Grund ist hier auch keine Benutzerauthentikation erforderlich.

Eine eingehende Mail wird von einem SMTP Proxy auf Port 25 entgegengenommen und nach Überprüfung des Absenders (IP-Adresse und Rechnername des Mail-Servers) auf dem Application Gateway in einem speziellen Verzeichnis abgelegt. Der SMTP Daemon prüft periodisch, ob Mails eingegangen sind. Das Mail Transfer Agent (MTA) stellt dem Adressaten die Mail direkt oder über einen oder mehrere MTAs zu. Der SMTP Proxy verhindert damit, dass der MTA direkt vom unsicheren Netz angesprochen werden kann.

Ein solches MTA ist zum Beispiel »Sendmail«, das häufig eingesetzt wird und das bekanntlich eine Vielzahl von Sicherheitslücken und Implementierungsfehlern aufweist.

Ein SMTP Proxy verarbeitet nur die folgenden Befehle, die nicht sicherheitskritisch sind: `helo, mail, rcpt, data, quit, rset, noop.`

Einige weitere Befehle werden mit Standardantworten bedient, damit eine Kommunikation ermöglicht werden kann: `help, vref, expn.`

Bei sicherheitsrelevanten Befehlen wie debug wird eventuell direkt eine Spontane Meldung an das Sicherheitsmanagement gesendet.

Falls der Befehl debug in einem SMTP-Proxy erkannt wird, kann dadurch kein Fehler auftreten, weil der SMTP-Proxy darauf nicht reagiert. Wenn aber ein Fremder versucht, diesen Befehl auszuführen, kann die Tatsache dahingehend interpretiert werden, dass sich dahinter ein Angriffsversuch verbirgt. Diese Information über einen Angriffsversuch kann wichtig sein.

Durch die Verwendung des Store-and-Forward-Prinzips wird zum Beispiel eine Entkopplung des komplexen und fehlerbehafteten Programms Sendmail (MTA) erreicht. So werden bekannte Angriffe über Sendmail verhindert, denn mit Hilfe der Befehle kann Sendmail nicht direkt angesprochen werden, sondern nur die Stellvertreter-Software der SMTP Proxies. Der SMTP Proxy ist überschaubar und damit gut testbar Software.

Logbuch:

Durch den SMTP Proxy können im Logbuch des Application Gateway die folgenden Protokolldaten festgehalten werden:

- IP-Adresse und Rechnername des Quell-Rechnersystems
- Uhrzeit und Datum des Verbindungsaufbaus
- Absender der Mail (wie im Kopf der Mail angegeben)
- Adressat der Mail (wie im Kopf der Mail angegeben)
- Anzahl der übertragenen Bytes
- Uhrzeit und Datum des Verbindungsabbaus

Durch den Message Transfer Agent (MTA) werden im Logbuch des Application Gateway die folgenden Protokolldaten festgehalten:

- IP-Adresse und Rechnername des Ziel-Rechnersystems
- Uhrzeit und Datum des Verbindungsaufbaus
- Absender der Mail (wie im Kopf der Mail angegeben)
- Adressat der Mail (wie im Kopf der Mail angegeben)
- Anzahl der übertragenen Bytes
- Uhrzeit und Datum des Verbindungsabbaus

Wenn ein Problem auftritt, können die umfangreichen Protokolldaten der Ereignisse im SMTP Proxy verwendet werden, um es zu lösen.

Benutzerorientierte Application Level Proxies

Die folgenden Proxies für Telnet, FTP und HTTP sind benutzerorientierte Proxies, die – ähnlich wie ein Pförtner – selbst eine Authentikation mit dem entsprechenden Benutzer durchführen. Im Falle einer erfolgreichen Identifikation und Authentikation eines Benutzers mit dem Proxy gilt diese Authentikation auch nur für diesen speziellen Proxy. Falls der Benutzer einen anderen Dienst, das heißt

einen anderen Proxy, nutzen möchte, muss eine erneute Identifikation und Authentikation stattfinden. Benutzerorientierte Proxies haben den Vorteil, dass die Zuordnung zwischen Benutzer und IP-Adresse und dem gewünschten Dienst eindeutig und lückenlos ist.

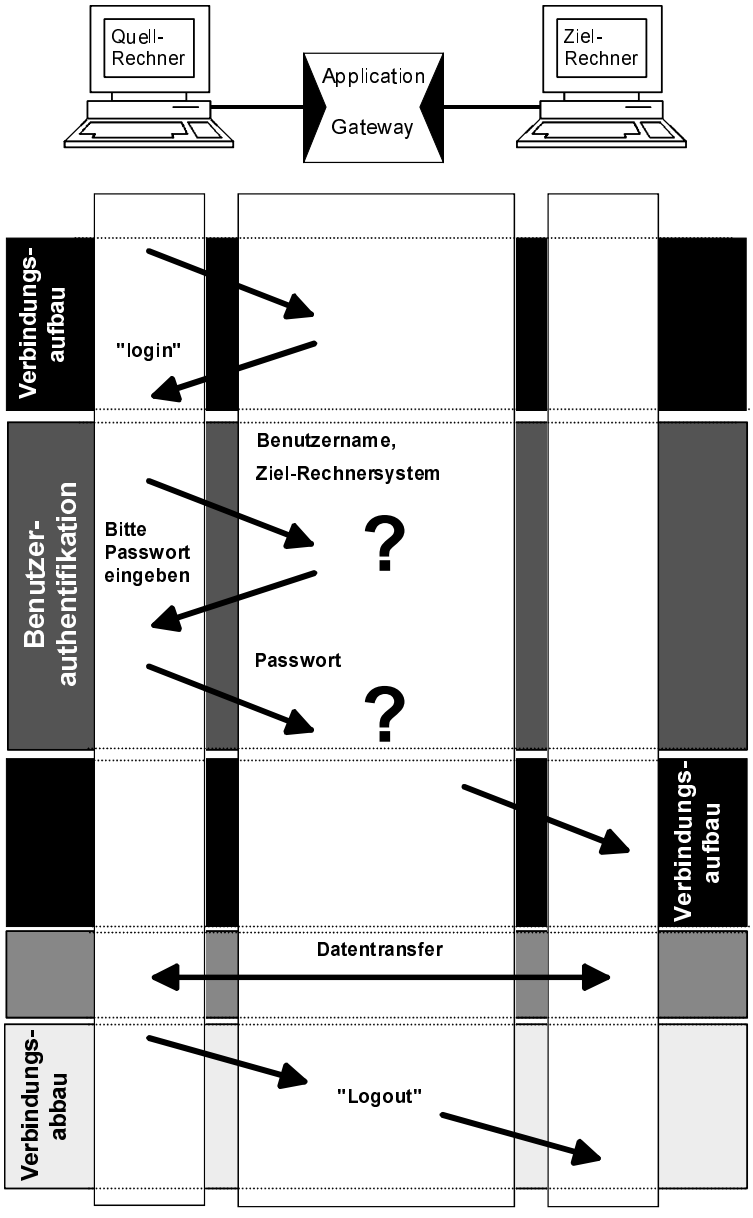


Abb. 12.25: Kommunikation über einen Application Level Proxy

Im Folgenden wird der Verbindungsaufbau über das Applikation Gateway mit Hilfe eines einfachen Passwortverfahrens für benutzerorientierte Dienste exemplarisch dargestellt.

- **1. Phase: Verbindungsaufbau zum Application Gateway**
  Der Benutzer versucht, über das Application Gateway eine Verbindung von seinem Quell-Rechnersystem zu einem gewünschten Ziel-Rechnersystem aufzubauen. Das Application Gateway nimmt den Verbindungsaufbau an und fordert den Zugreifenden auf, eine Identifikation und Authentikation durchzuführen.

- **2. Phase: Benutzerauthentikation**
  Der Zugreifende gibt seine Benutzer-Identifikation und sein Ziel-Rechnersystem an. Auf dem Application Gateway wird überprüft, ob der Benutzer von seinem Quell-Rechnersystem auf das angestrebte Ziel-Rechnersystem zugreifen darf und welche Restriktionen für den Zugriff bestehen. Anschließend wird der Benutzer in diesem Beispiel aufgefordert, sein Passwort einzugeben. Auf dem Application Gateway wird dann überprüft, ob der Benutzer das richtige Passwort eingegeben hat (wie beim Pförtner).

  Die Authentikation bei Firewall-Systemen kann in der Regel unterschiedlich realisiert werden, zum Beispiel durch Passwortverfahren, Einmal-Passwortverfahren oder Challenge-Response-Verfahren. Die Authentikationsverfahren, die mit Hilfe von kryptographischen Algorithmen arbeiten, nutzen für den Benutzer Security Tokens, Chipkarten usw. Welches Authentikationsverfahren verwendet wird, hängt in der Regel vom Schutzbedarf und der Richtung der Kommunikation über das Firewall-System ab. Von einem zu schützenden Netz in ein unsicheres Netz kann die Kommunikation über das Firewall-System mit einem einfachen oder sogar ohne ein Authentikationsverfahren realisiert werden. Bei der Kommunikation von einem unsicheren Netz in ein zu schützendes Netz sollte immer ein kryptographisches Verfahren (zum Beispiel mit Security Token oder Chipkarte) verwendet werden.

- **3. Phase: Verbindungsaufbau zum Ziel-Rechnersystem**
  Wenn sich der zugreifende Benutzer erfolgreich identifizieren und authentisieren konnte, wird durch den Proxy auf dem Application Gateway eine zweite Verbindung vom Application Gateway zum gewünschten und erlaubten Ziel-Rechnersystem aufgebaut.

- **4. Phase: Datentransfer**
  Dann findet der Datentransfer statt. Abhängig vom jeweiligen Proxy wird der Datentransfer über den Proxy auf dem Application Gateway überwacht, kontrolliert und protokolliert. Diese Phase ist für den Benutzer transparent.

- **5. Phase: Verbindungsabbau**
  In der letzten Phase wird die Verbindung über das Application Gateway abgebaut.

Telnet Proxy

Der Telnet Proxy ist für die kontrollierte Kommunikation über Telnet verantwortlich und stellt entsprechende spezielle Sicherheitsfunktionen für diesen Dienst zur Verfügung.

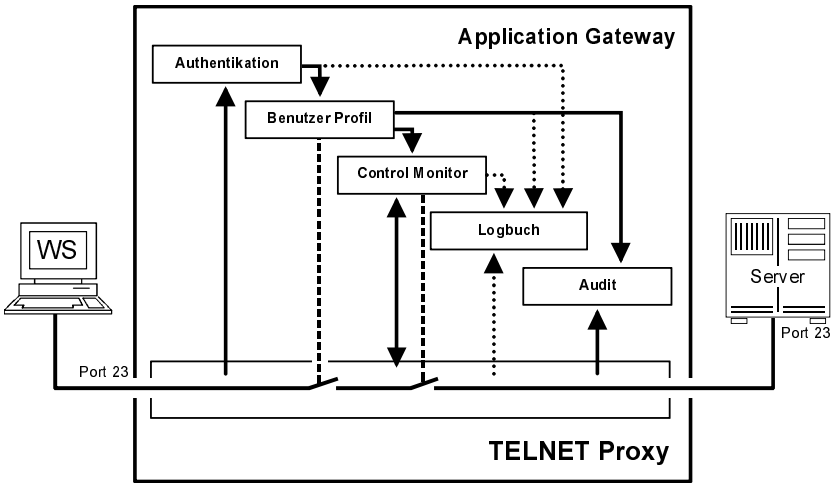


Abb. 12.26: Telnet Proxy

Der Verbindungsaufbau erfolgt vom Quell-Rechnersystem (Client) auf Port 23 (Port für den Telnet-Dienst) des Application Gateway. An Port 23 übernimmt der Telnet Proxy die Verbindung. Der Benutzer auf dem Quell-Rechnersystem identifiziert und authentisiert sich unter Angabe des Verbindungsziels gegenüber dem Telnet Proxy. Nach erfolgreicher Identifikation und Authentikation wird ein den folgenden Bedingungen entsprechendes Benutzerprofil aktiviert:

- IP-Adresse des Quell-Rechnersystems, das die Verbindung aufbauen möchte
- Benutzername, mit dem die Identifikation und Authentikation erfolgte
- IP-Adresse des Ziel-Rechnersystems

Nun baut der Telnet Proxy eine zweite Verbindung vom Application Gateway auf Port 23 des Ziel-Rechnersystems auf. Jetzt kann der Benutzer vom Quell-Rechnersystem über den Telnet Proxy den Telnet-Dienst des Ziel-Rechnersystems nutzen (siehe Abb. 12.26).

Control Monitor:

Bei der Telnet-Session ist es zum Beispiel möglich, mit Hilfe eines »Control Monitors« zu überprüfen, ob der Benutzer unerlaubterweise vom Quell-Rechnersystem auf ein anderes Rechnersystem als das erlaubte Ziel-Rechnersystem zugreift.

Dabei überprüft der Monitor den Datenstrom auf Bytefolgen, die unter Umständen für ein Hopping genutzt werden können. Es ist auch möglich, nach anderen Informationen zu suchen, zum Beispiel nach Steuerzeichen, die nicht verwendet werden sollen (`Ctrl-C etc.`)

Logbuch:

In das Logbuch des Application Gateway können durch den Telnet Proxy die folgenden Protokolleinträge vorgenommen werden:

- IP-Adresse und Rechnername des Quell-Rechnersystems
- IP-Adresse und Rechnername des Ziel-Rechnersystems
- Uhrzeit und Datum des Verbindungsaufbaus
- Name des Benutzers
- Anzahl der übertragenen Bytes
- Uhrzeit und Datum des Verbindungsabbaus

Bei der Telnet-Verbindung ist es oft sinnvoll, einen Mitschnitt der kompletten Kommunikation aufzuzeichnen (Audit). Neben der Möglichkeit, diesen Mitschnitt später auszuwerten, hat diese Sicherheitsfunktion einen nicht zu unterschätzenden Warneffekt.

Anwendungsbeispiel für Audit:

Der Sicherheitsmechanismus »Audit« kann zum Beispiel vertraglich mit einer Firma vereinbart werden, die Remote-Service durchführt.. Dadurch ist dem Mitarbeiter der Servicefirma bewusst, dass alles, was er tut, protokolliert wird. Allein das Wissen um diese Überwachung wird den Serviceleistenden motivieren, nur das zu tun, was er für seine Aufgabenstellung wirklich benötigt. Im Fall eines Schadens kann dann das Protokoll aufklären, ob über den Remote-Zugriff unerlaubte oder nicht notwendige Aktionen durchgeführt worden sind. Der Mitarbeiter der Service-Firma kann für seine Handlungen im Nachhinein dezidiert verantwortlich gemacht werden.

FTP Proxy

Der FTP Proxy ist für die kontrollierte Kommunikation über FTP verantwortlich und stellt entsprechende spezielle Sicherheitsfunktionen für diesen Dienst zur Verfügung.

Der Verbindungsaufbau für den Kommandokanal erfolgt vom Quell-Rechnersystem (Client) auf Port 21 (FTP-Kommando-Port) des Application Gateway. Der Benutzer auf dem Quell-Rechnersystem identifiziert und authentisiert sich nun unter Angabe des Verbindungsziels gegenüber dem FTP-Dienst. Nach erfolgreicher Identifikation und Authentikation wird ein den folgenden Bedingungen entsprechendes Benutzerprofil aktiviert:

- IP-Adresse des Quell-Rechnersystems, das die Verbindung aufbauen möchte

- Benutzername, mit dem die Authentikation erfolgte
- IP-Adresse des Ziel-Rechnersystems

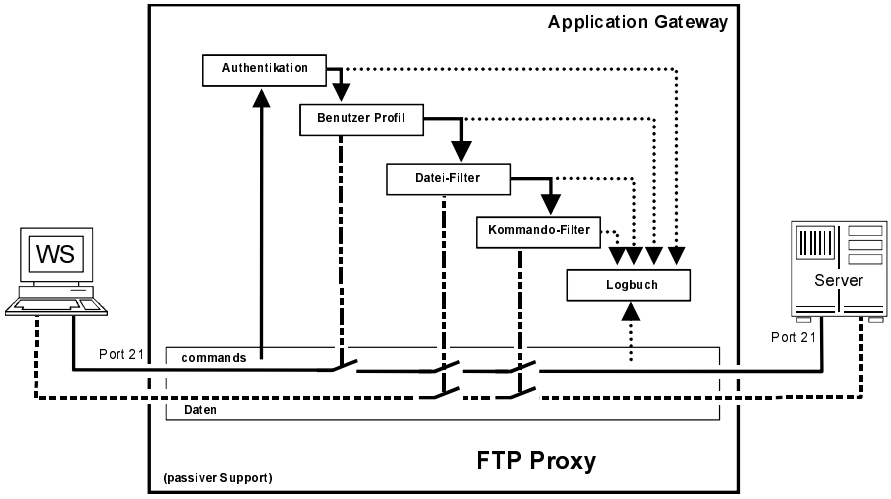


Abb. 12.27: FTP Proxy

Nun baut der FTP Proxy einen zweiten Kommandokanal vom Application Gateway auf Port 21 des Ziel-Rechnersystems auf (siehe Abb. 12.27).

Kommando-Filter:

Der Kommando-Filter analysiert und überprüft alle vom Benutzer eingegebenen FTP-Kommandos hinsichtlich ihres Eintrags in der Rechtedatei (Benutzerprofil). Für den FTP Proxy kann zum Beispiel definiert werden, welche Befehle (`cd, put, get, del` usw.) verwendet werden dürfen und welche nicht.

Gibt der Benutzer ein Kommando ein, zu dem er berechtigt und bei dem ein Datentransfer erforderlich ist, erfolgt der Verbindungsaufbau des Datenkanals abhängig davon, ob auf dem Quell-Rechnersystem (Client-Seite) eine aktive oder eine passive FTP-Verbindung gewünscht wurde.

Wird ein Kommando von einem nicht dazu berechtigten Benutzer verwendet, wird dies dem Benutzer angezeigt, der unberechtigte Versuch wird in das Logbuch des Application Gateway eingetragen und, falls definiert, als Spontane Meldung an das Security Management gesendet.

Datei-Filter:

Außerdem kann bei FTP Proxies durch einen Datei-Filter in der Regel eine Namensrestriktion für die Dateien vorgenommen werden, die übertragen werden dürfen. Beispiele für solche Regeln sind:

- Es dürfen nur Dateien mit dem Namen »Input.neu« und »Output.neu« transferiert werden.
- Es dürfen keine Dateien mit der Endung ».exe« übertragen werden.

Logbuch:

In das Logbuch des Application Gateway können durch den FTP Proxy die folgenden Protokolleinträge standardmäßig vorgenommen werden:

- IP-Adresse und Rechnername des Quell-Rechnersystems
- IP-Adresse und Rechnername des Ziel-Rechnersystems
- Uhrzeit und Datum des Verbindungsaufbaus
- Name des Benutzers
- Anzahl der übertragenen Bytes
- Name der übertragenen Dateien
- verwendete Befehle
- Uhrzeit und Datum des Verbindungsabbaus

Anwendungsbeispiel für den FTP Proxy:

Mit Hilfe des FTP Proxy kann genau definiert werden, welche Befehle verwendet werden dürfen. Falls zum Beispiel ein Softwarehaus auf einen bestimmten Server ein Update senden möchte, wird einem Mitarbeiter des Softwarehauses erlaubt, die Befehle `cd` und `put` zu verwenden. Diese Befehle reichen aus, um die Arbeit durchführen zu können.

Die Reduzierung der erlaubten Befehle verhindert, dass bei dieser Aktion versehentlich oder absichtlich Schaden angerichtet wird. Falls zum Beispiel versucht wird, den Befehl `del` (Löschen) auszuführen, wird dies im FTP Proxy des Application Gateway erkannt und dem Benutzer angezeigt. Das Ereignis wird in das Logbuch eingetragen und, falls im Regelwerk definiert, eine Spontane Meldung mit den entsprechenden Protokolldaten an das Security Management gesendet.

HTTP Proxy

Der HTTP Proxy ist für die kontrollierte Kommunikation über HTTP verantwortlich und stellt spezielle Sicherheitsfunktionen für diesen Dienst zur Verfügung.

Der Verbindungsaufbau erfolgt vom Quell-Rechnersystem (Client) auf Port 80 (Port für den HTTP-Dienst) des Application Gateway. Der Benutzer auf dem Quell-Rechnersystem (Client-Seite) identifiziert und authentisiert sich nun unter Angabe des Verbindungsziels gegenüber dem HTTP-Dienst. Nach erfolgreicher Identifikation und Authentikation wird ein den folgenden Bedingungen entsprechendes Benutzerprofil aktiviert:

- IP-Adresse des Quell-Rechnersystems, das die Verbindung aufbauen möchte
- Benutzername, mit dem die Authentikation erfolgte
- IP-Adresse des Ziel-Rechnersystems

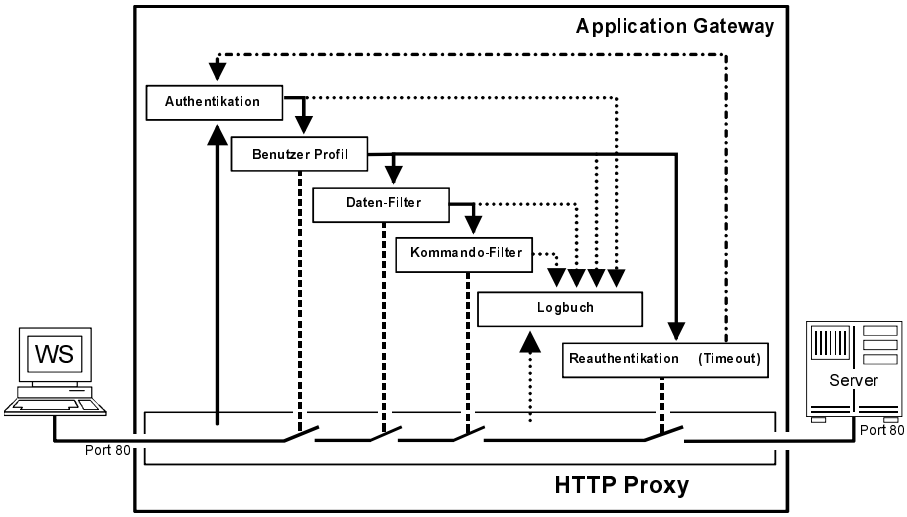


Abb. 12.28: HTTP Proxy

Nun baut der HTTP Proxy eine zweite Verbindung vom Application Gateway auf Port 80 des Ziel-Rechnersystems auf. Jetzt kann der Benutzer vom Quell-Rechnersystem über das Application Gateway (HTTP Proxy) den HTTP-Dienst des Ziel-Rechnersystems nutzen (siehe Abb. 12.28).

Re-Authentikation:

Das HTTP-Protokoll arbeitet nicht Session-orientiert, das heißt, der HTTP Proxy ist nicht in der Lage, von sich aus das Ende einer Session zu erkennen. Jedes Mal, wenn eine WWW-Seite angefordert wird, wird eine Verbindung über das Firewall-System aufgebaut, die WWW-Seite übertragen und wieder abgebaut. Beim ersten Mal wird vor der Übertragung die Authentikation durchgeführt. Dabei wird ein Timer gesetzt, der den Beginn der Session festhält. Nach Ablauf des Timers beendet der HTTP Proxy die zugehörige HTTP-Session automatisch. Sobald eine Benutzeraktivität in dieser Session stattfindet, wird der Timer erneut gestartet. Läuft der Timer ab, muss – falls eingestellt – bei einer erneuten Kommunikation wieder eine Identifikation und Authentikation stattfinden.

Kommando-Filter:

Der Kommando-Filter analysiert und überprüft die verwendeten Methoden (FTP, HTTP, NNTP, SMTP) und die verwendeten Befehle (zum Beispiel `put`, `get`, `post`).

Bei jedem Versuch, eine nicht gültige Methode oder einen nicht erlaubten Befehl zu verwenden, wird dem Benutzer eine entsprechende Meldung angezeigt und es erfolgt ein Eintrag in das Logbuch des Application Gateway. Falls im Regelwerk

definiert, wird in diesem Fall auch eine Spontane Meldung mit den Protokolldaten an das Sicherheitsmanagement gesendet.

Daten-Filter:

Mit Hilfe eines Daten-Filters im HTTP Proxy ist es auch möglich, nur definierte URLs zuzulassen (URL-Blocker). Zum Beispiel kann festgelegt werden, dass die Benutzer nur HTTP-Server mit der Länderkennung ».de« nutzen dürfen. Durch den Daten-Filter kann der Proxy aber auch bekannte unerwünschte Dateien oder HTTP-Seiten ausfiltern. Dies kann zum Beispiel bei bekannten Dateien, die Viren enthalten, oder bei HTTP-Seiten, auf denen pornographische Bilder zu sehen sind, genutzt werden.

Content Security:

Unter den Begriff Content Security werden hier die Sicherheitsmechanismen verstanden, die gegen die Gefährdungen durch aktive Inhalte innerhalb von HTML-Seiten wirken /Fuhr98//Koke97/.

- Applet-Filter
  Mit Hilfe eines Applet-Filters kann die Nutzung von Java, Java Scripts und ActiveX verhindert werden. Dies ermöglicht, die Sicherheitspolitik einer Organisation in bezug auf die Nutzung von dynamischen Programmteilen durchzusetzen. Ein mögliches Beispiel ist, Java im zu schützenden Netz für die Intranet-Anwendungen zuzulassen, aber bei der Kommunikation mit Rechnersystemen im unsicheren Netz über das Firewall-System zu verhindern.
- Malware-Filter
  Mit Hilfe eines Malware-Filters können Viren, Würmer und Trojanische Pferde aufgespürt und mögliche Schäden verhindert werden.

Logbuch:

Durch den HTTP Proxy können zum Beispiel die folgenden Protokolleinträge in das Logbuch des Application Gateway vorgenommen werden:

- IP-Adresse und Rechnername des Quell-Rechnersystems
- IP-Adresse und Rechnername des Ziel-Rechnersystems
- Uhrzeit und Datum des Verbindungsaufbaus
- Name des Benutzers
- Anzahl der übertragenen Bytes
- Name der übertragenen Datei oder der übertragenen HTML-Seite (Name der Seite und IP-Adresse des Servers/Ziel-Rechnersystems)
- Uhrzeit und Datum des Verbindungsabbaus

Authentication Proxy (Global Authentication)

Ein etwas anderes Konzept für ein Application Gateway dient dazu, dass der Benutzer eine Identifikation und Authentikation mit einem sogenannten Authentication Proxy durchführt.

Diese Art der Identifikation und Authentikation wird bei Firewall-Systemen auch »globale Authentikation« genannt. Der Authentication Proxy führt die Rechteverwaltung für die unterschiedlichen Dienste durch, zum Beispiel für FTP, Telnet, HTTP. In diesem Fall muss keine erneute Authentikation durchgeführt werden, wenn der Benutzer einen Dienst wechseln möchte. Ein Nachteil dieser Methode, der sich besonders bei Multiuser-Systemen zeigt, ist die nicht eindeutige Verbindung zwischen Dienst und Benutzer. Außerdem kann der Dienst während der Zeit zwischen der Freischaltung der Verbindung auf dem Application Gateway und dem Connect des Clients von Angreifern benutzt werden /uti99/.

Der Authentication Proxy regelt die Identifikation und Authentikation eines Clients auf einem Server über das Application Gateway. Anschließend können die erlaubten Dienste über das Firewall-System kontrolliert genutzt werden.

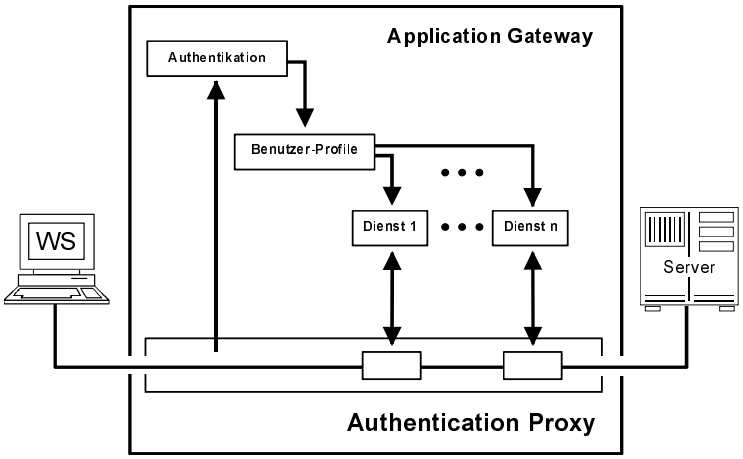


Abb. 12.29: Authentication Proxy

Transparent Proxy

Unter »Transparent Proxies« werden Proxies verstanden, die in der Lage sind, sich aus der Sicht der Clients transparent zu verhalten. Diese Proxies sorgen zum Beispiel dafür, dass aus dem zu schützenden Netz direkt Rechnersysteme im unsicheren Netz (zum Beispiel dem Internet) adressiert werden können. Der Vorteil dieser Proxies, die sich transparent von innen nach außen verhalten, liegt darin, dass die Client-Software bei der Integration eines Firewall-Systems nicht verändert werden

braucht. Bestimmte Anwendungen, wie zum Beispiel Home-Banking-Lösungen, die über Java-Applets feste IP-Adressen mitsenden, können dann auch über Firewall-Systeme realisiert werden.

Circuit Level Proxies

Da bei Application Gateways ein Routing auf der Netzwerkebene aus Sicherheitsgründen nicht möglich sein darf, könnten für Dienste, für die kein Application Level Proxy zur Verfügung steht, sogenannte Circuit Level Proxies zur Verfügung gestellt werden, wenn eine Kommunikation über das Application Gateway realisiert werden soll. Circuit Level Proxies sind eine Art generische Proxies, die für eine Mehrzahl von Diensten mit verschiedenen Protokollen verwendet werden können /BoW097/.

Diese Circuit Level Proxies, die auch als generische Proxies, Port-Relays oder Plug-Gateways bezeichnet werden, können in der Regel für TCP und UDP-Anwendungen verwendet werden.

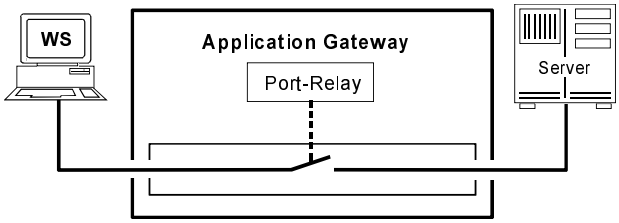


Abb. 12.30: Port-Relay

Mit einem Port-Relay kann eine Kommunikation über das Application Gateway kontrolliert über einen definierten Port auf eine definierte IP-Adresse erfolgen. Da die Kommunikation über die Port-Nummer des Port-Relay adressiert wird, kann die Kommunikation über das Application Gateway nur auf eine IP-Adresse auf der »anderen Seite« erfolgen. Aus diesem Grund sind Port-Relays immer n:1. Das heißt, dass viele Rechnersysteme (IP-Adressen) von der einen Seite auf ein Rechnersystem (eine IP-Adresse) auf der anderen Seite zugreifen können, während der umgekehrte Weg nicht möglich ist.

Im folgenden werden zwei Anwendungsbeispiele dargestellt, die aufzeigen, welche Möglichkeiten mit den Circuit Level Proxies – Port Relays – realisiert werden können.

Beispiel eines n:1 Port-Relay:

In diesem Beispiel wird ein Mail-Server vor dem Application Gateway im unsicheren Netz positioniert. Mit Hilfe eines POP3-Servers können Mails in das zu schüt-

zende Netz übertragen werden. Auf dem Application Gateway wird dann ein Port-Relay definiert, über den mehrere Clients (IP-Adressen) über eine bestimmte Portnummer (hier 110) auf die IP-Adresse des Mail-Servers zugreifen dürfen.

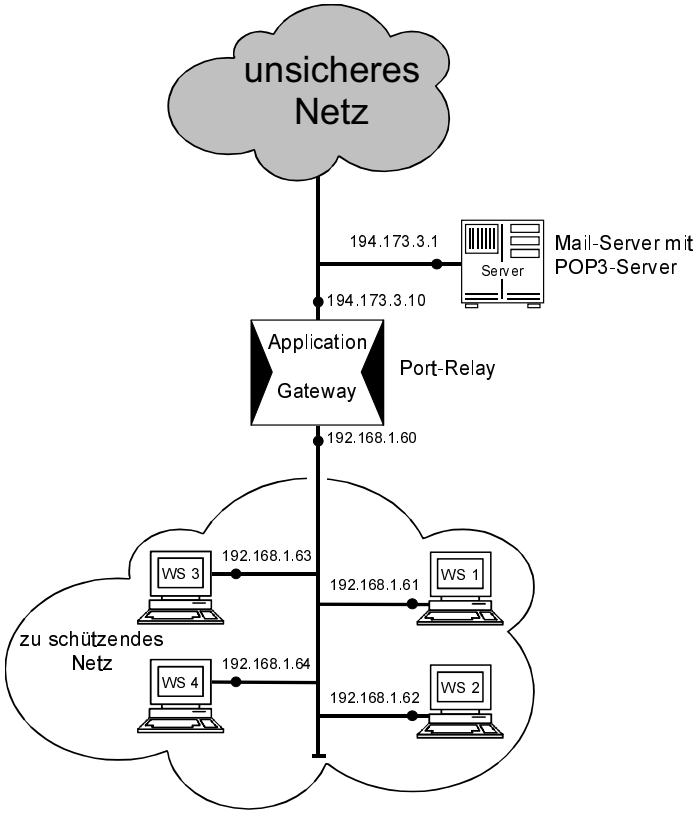


Abb. 12.31: Beispiel eines n:1 Port-Relay

Somit können die Clients (Quell-Rechnersysteme) über den definierten Port auf den Mail-Server (Ziel-Rechnersystem) zugreifen, um ihre Mail abzurufen. Das Port-Relay überprüft, ob von den zugelassenen IP-Adressen über den erlaubten Port auf die IP-Adresse des Mail-Servers zugegriffen wird. Der umgekehrte Weg ist nicht möglich.

Die n:1 Port-Relays sind sehr starr und können nicht für jede mögliche Anwendung verwendet werden. Es gibt aber die Möglichkeit, aus vielen n:1 Port-Relays einen n:m Port-Relay zu gestalten.

Quell-IP-Adressen (n) zu schützendes Netz	Ziel-IP-Adresse des Application Gateway zu schützendes Netz	Portnummer	Quell-IP-Adresse des Application Gateway unsicheres Netz	Ziel-IP-Adresse (1) unsicheres Netz
192.168.1.1 192.168.1.2 192.168.1.3 192.168.1.4	192.168.1.60	110	194.173.3.10	194.173.3.1

Tabelle 12.1: Beispiel für einen n:1 Port-Relay

Beispiel eines n:m Port-Relay

In diesem Beispiel wird beschrieben, wie die Möglichkeit geschaffen werden kann, aus dem unsicheren Netz über verschiedene IP-Adressen des unsicheren Netzes (zum Beispiel Internet) auf unterschiedliche Rechnersysteme im zu schützenden Netz (zum Beispiel Intranet) zuzugreifen. Das Application Gateway kann dann über mehrere IP-Adressen aus dem unsicheren Netz angesprochen werden. Dabei sollen die IP-Adressen der Rechnersysteme des zu schützenden Netzes verborgen bleiben.

Dazu wird m-mal ein n:1 Port-Relay für die unterschiedlichen IP-Adressen definiert, die aus dem unsicheren Netz auf das zu schützende Netz zugreifen können, und es wird festgelegt, auf welche Rechnersysteme im zu schützenden Netz sie zugreifen dürfen.

Aus der Sicht der Rechnersysteme im unsicheren Netz werden die IP-Adressen der Server im zu schützenden Netz wie IP-Adressen des unsicheren Netzes betrachtet.

Dabei wird auch genau definiert, über welchen Port dies ermöglicht wird (siehe Tabelle 12.2: Port 2000). Durch den n:m Port-Relay wird erreicht, dass die IP-Adressen des zu schützenden Netzes verborgen bleiben, weil sich nur die externen IP-Adressen darstellen, und dass die Kommunikation über den Port nur mit definierten Rechnersystemen in eine Richtung ermöglicht wird.

Logbuch der Port Proxies:

Durch den Port Proxy können folgende Einträge in das Logbuch des Application Gateway vorgenommen werden:

- IP-Adresse und Rechnername des Quell-Rechnersystems
- IP-Adresse und Rechnername des Ziel-Rechnersystems
- Uhrzeit und Datum des Verbindungsaufbaus
- Anzahl der Bytes, die übertragen wurden
- Uhrzeit und Datum des Verbindungsabbaus

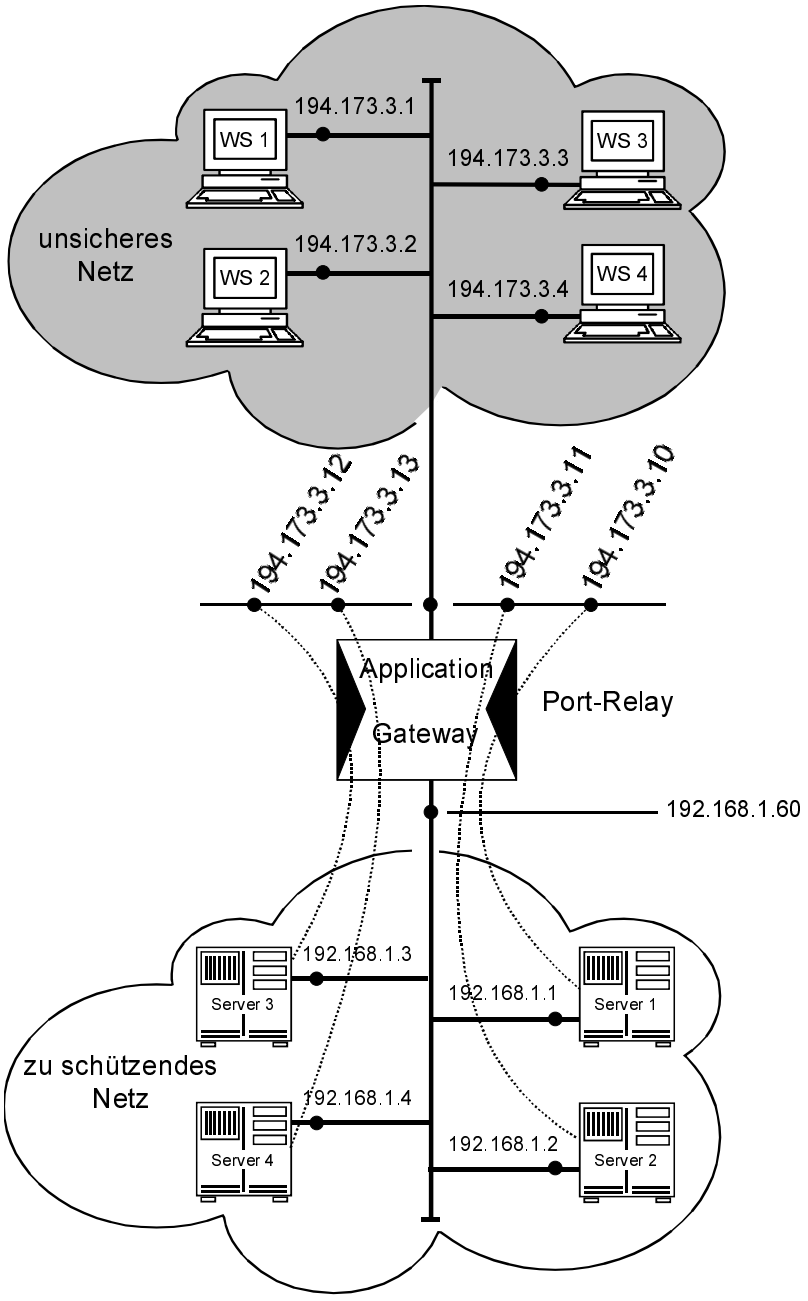


Abb. 12.32: Beispiel eines n:m Port-Relay

Quell-IP-Adressen unsicheres Netz	Ziel-IP-Adresse des Application Gateway unsicheres Netz	Portnummer	Quell-IP-Adresse des Application Gateway zu schützendes Netz	Ziel-IP-Adresse zu schützendes Netz
194.173.3.1 194.173.3.2 194.173.3.3 194.173.3.4	194.173.3.10	2000	192.168.1.60	192.168.1.1
194.173.3.1 194.173.3.2 194.173.3.3 194.173.3.4	194.173.3.11	2000	192.168.1.60	192.168.1.2
194.173.3.1 194.173.3.2 194.173.3.3 194.173.3.4	194.173.3.12	2000	192.168.1.60	192.168.1.3
194.173.3.1 194.173.3.2 194.173.3.3 194.173.3.4	194.173.3.13	2000	192.168.1.60	192.168.1.4

Tabelle 12.2: Beispiel für einen n:m Port-Relay

Beispiel eines speziellen Circuit Level Proxies:

Im folgenden soll exemplarisch ein spezielles Circuit Level Proxy dargestellt werden, wie es von manchen Application Gateways angeboten wird.

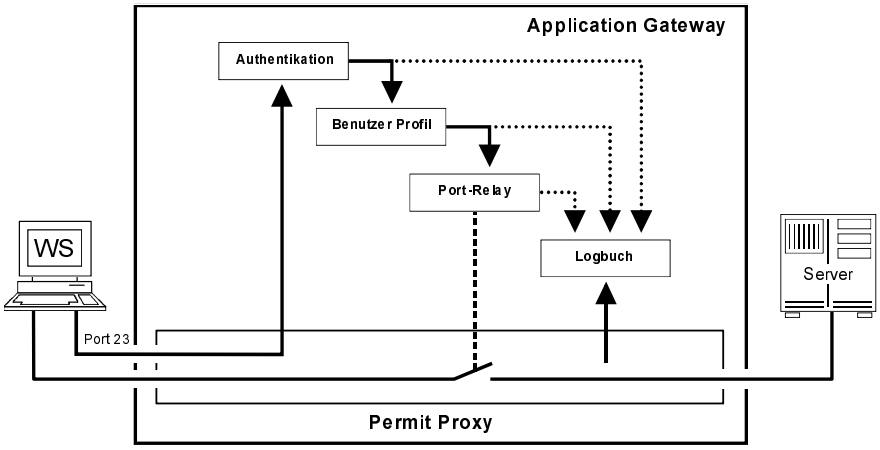


Abb. 12.33: Permit Proxy

Ein Permit Proxy regelt den Zugriff eines Client auf einen Server über das Application Gateway für TCP-basierte Dienste, die keinerlei Identifizierungs- und Authentisierungsmöglichkeiten bieten. Ein gutes Beispiel dafür sind NetBios-Protokolle, die per IP getunnelt werden. Für solche Protokolle können keine speziellen Proxies eingesetzt werden, weil bei den Programmen auf der Client-Seite kein Login-Mechanismus vorgesehen ist. Um dennoch den Zugriff auf bestimmte Rechnersysteme und Benutzer einzugrenzen, kann ein sogenannter Permit Proxy eingesetzt werden.

Dazu muss der Benutzer auf einem externen Rechnersystem zuerst eine Telnet-Verbindung (beziehungsweise eine HTTP-Verbindung) zum Application Gateway aufbauen, bevor er seine eigentliche Applikation starten kann. Nach einer erfolgreichen Identifikation und Authentikation kann der Benutzer den eigentlichen Dienst über einen »Port-Proxy« in Anspruch nehmen /uti98/.

Mit Hilfe des Permit Proxy kann dann festgelegt werden, über welchen Port, mit welchen Rechnersystemen (IP-Adressen) aus dem unsicheren Netz und mit welchem Rechnersystem (IP-Adresse) im zu schützenden Netz eine Kommunikation stattfinden darf. In diesem Beispiel wäre es auch möglich, über die Telnet-Verbindung weitere Verabredungen mit dem Application Gateway durchzuführen, zum Beispiel die Festlegung der IP-Adresse, mit der die Kommunikation stattfinden soll (wie ein flexibler n:m Port-Relay).

Die Telnet-Sitzung wird automatisch durch das Beenden der Applikation geschlossen. Falls das Telnet-Progamm vor der Anwendung beendet wird, unterbricht der Permit Proxy die Verbindung zur Applikation.

Logbuch:

Durch den Permit Proxy können folgende Einträge in das Logbuch des Application Gateway vorgenommen werden:

- IP-Adresse und Rechnername des Quell-Rechnersystems
- IP-Adresse und Rechnername des Ziel-Rechnersystems
- Uhrzeit und Datum des Verbindungsaufbaus
- Name des Benutzers
- Uhrzeit und Datum des Verbindungsabbaus

Der Permit Proxy ist im Prinzip ein Circuit Level Proxy mit Authentikation.

12.4.5 Adaptive Proxy

Einige Sicherheitshersteller versuchen, in einem sogenannten »Adaptive Proxy« die Vorteile von Packet Filter und Application Gateway zu kombinieren /NAI98/. Die Idee bei diesem Ansatz ist, dass der »Adaptive Proxy« in der Phase des Verbindungsaufbaus wie ein Application Proxy arbeitet und sich in der Phase des Datentransfers wie ein Packet Filter verhält. Der Vorteil dieser Methode liegt auf der Hand: In der ersten Phase wird eine sehr hohe Sicherheit erreicht, erst danach wer-

den die schnellen Tests der Packet Filter durchgeführt. Unter der Annahme, dass alle Angriffe die erste Phase, also den Aufbau einer Kommunikationsverbindung, betreffen, würde man mit diesem Ansatz eine hohe Sicherheit erreichen.

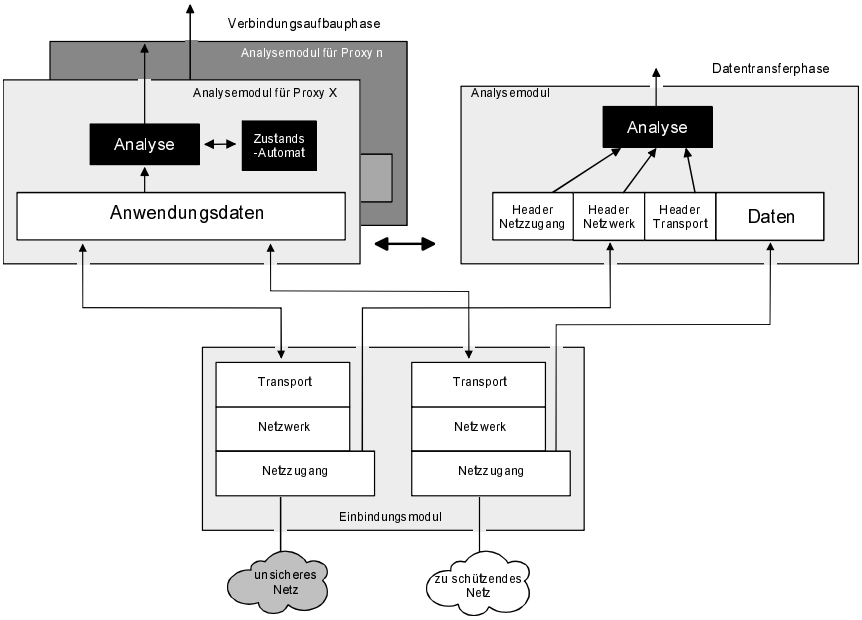


Abb. 12.34: Adaptive Proxy

Analogie zum Pförtner:

Der »Adaptive-Proxy-Pförtner« arbeitet in der ersten Phase (Verbindungsaufbau) wie der »Application-Proxy-Pförtner«: Er schaut sich nicht nur die Adresse der eingehenden Pakete an, er öffnet auch das Paket und überprüft den gesamten Inhalt. Wenn der »Adapive-Proxy-Pförtner« den Lieferanten seit langem kennt, dann sendet er den LKW des Lieferanten durch das Tor, damit dieser die Lieferung direkt zustellt. Kennt er den Lieferanten jedoch nicht, dann schickt er den LKW-Fahrer nach dem Ausladen der Lieferung weg und bestellt den firmeneigenen Fahrer, der im eigenen LKW das Paket zum Empfänger bringt.

Möglichkeiten und Grenzen eines Adative Proxy

Da ein elektronischer Pförtner aber nicht auf persönliche, menschliche Bindung aufbauen kann, scheint der Adaptive Proxy eher in der Theorie interessant zu sein als in der Praxis, da er kaum die Qualität eines Application Proxy erreichen kann. Soll das Äquivalent der persönlichen, menschlichen Bindung mit Hilfe von vertrauenswürdigen Netzen und/oder der Nutzung von Verschlüsselungssystemen

realisiert werden, muss eine genaue Analyse der Bedrohungen und der Einsatzumgebung durchgeführt werden.

12.4.6 Anwendungsgebiete von Application Gateways

Immer dann, wenn es notwendig ist, Schutzmaßnahmen für die Anwendungen zur Verfügung zu stellen, ist ein Application Gateway ein ideales aktives Firewall-Element. Die Möglichkeit der Protokollierung auf der Anwendungsebene kann ebenfalls ein besonderer Grund sein, ein Application Gateway in einem Firewall-Konzept zu berücksichtigen.

Für die Ankopplung an das Internet ist auf jeden Fall ein Application Gateway in der Firewall-Konstellation zu berücksichtigen, wenn die Rechnersysteme im zu schützenden Netz einen hohen Schutzbedarf haben (siehe auch Kapitel 3.2).

Außerdem können Organisationseinheiten, die sich innerhalb eines Intranet abschotten wollen, hiermit einen besonderen Schutz erzielen.

Möglichkeiten, Vorteile und besondere Aspekte von Application Gateways

- Das Design-Konzept ist sicher, da kleine, gut überprüfbare Module (Proxies) verwendet werden.
- Eine Konzentration auf das Wesentliche findet statt.
- Durch die ausnahmslose Übertragung aller Pakete durch den Proxy wird eine höhere Sicherheit erreicht.
- Der Kommunikationspartner der Rechnersysteme, die über das Application Gateway kommunizieren, ist der Proxy; dadurch kann eine echte Entkopplung der Dienste erreicht werden.
- Verbindungsdaten und Applikationsdaten können protokolliert und dadurch die Handlungen der Benutzer, die über das Application Gateway kommunizieren, nachvollzogen werden.
- Die interne Netzstruktur bleibt nach außen hin verborgen.
- Sicherheitsfunktionen für die Anwendungen werden zur Verfügung gestellt (Kommando-, Datei- und Daten-Filter usw.)
- Eine Network Address Translation findet statt.

Nachteile und Grenzen von Application Gateways

- Die Flexibilität ist gering, da für jeden neuen Dienst ein neuer Proxy zur Verfügung gestellt werden muss.
- Die Kosten für ein Application Gateway sind in der Regel höher.
- Die Kommunikation über das Application Gateway ist nicht transparent und erfordert daher eine veränderte Vorgehensweise.
- Einige Application Gateways können kein IP-Spoofing erkennen (dies ist kein generelles Problem).

12.4.7 Firewall-Elemente und das Verhältnis von Geschwindigkeit zu Sicherheit

Diese Abbildung stellt eine Art der Klassifizierung von Firewall-Elementen dar. Es wird das Verhältnis der unterschiedlichen Firewall-Elemente bezüglich Speed und Security qualitativ dargestellt.

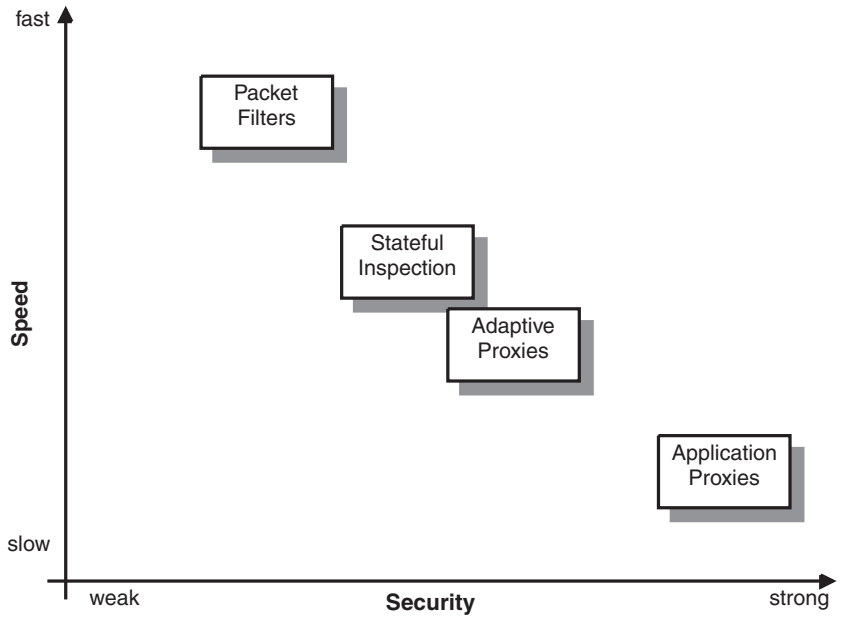


Abb. 12.35: Speed/Security

Durch den parallelen Einsatz mehrerer Application Gateways mit Application Proxies ist insgesamt eine höhere Leistungsfähigkeit (Durchsatz) zu erreichen und der dargestellte Nachteil in der Praxis zu kompensieren.

12.4.8 Unterschiedliche Firewall-Konzepte

Packet Filter, Application Gateway oder ein High-level Firewall-Konzept haben unterschiedliche Wirksamkeiten, wie sie die Kommunikation nach außen kontrollieren und wie sie einen Übergriff aus einem fremden auf das eigene Netz verhindern können.

Welches Firewall-Konzept nun bei der Etablierung eines VPN über öffentliche Kommunikationsinfrastrukturen verwendet werden sollte, hängt auch von der Kommunikationsinfrastruktur selbst ab.

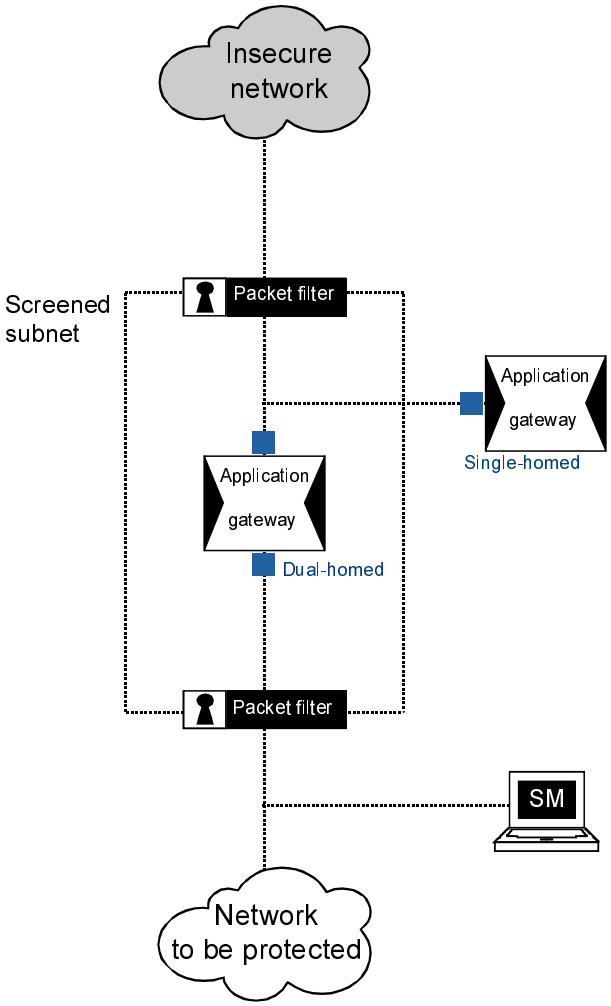


Abb. 12.36: Firewall-Konzepte

Wenn die Kommunikationsinfrastruktur an sich schon ein Höchstmaß an Sicherheit und Vertrauenswürdigkeit bietet, das heißt, wenn alle angeschlossenen Teilnehmer ungefähr die gleichen Sicherheitsbedürfnisse haben, kann auch mit einer einfachen Firewall-Lösung (zum Beispiel einem Packet-Filter) eine ausreichende Sicherheit erreicht werden /Pohl2001a/,/Pohl2000a/.

Wird aber beispielsweise ein VPN über das Internet realisiert, wo beliebig viele Teilnehmer mit äußerst heterogenen Zielen die gleiche Kommunikationsinfrastruktur benutzen, sollte ein Teilnehmer mit einem hohen Schutzbedarf bei der Ankopplung auf jeden Fall einen hohen Widerstand gegen Angriffe (mit einem High-level Security Firewall-System) realisieren.

Weiterführende Aufgabenstellungen bei VPN-Systemen

In diesem Kapitel werden einige weiterführende Aufgabenstellungen behandelt, die mit dem Betrieb von VPN-Systemen verbunden sind. Dazu gehören die Verfügbarkeit der Netzwerkdienste, mögliche Realisierungsformen von VPN-Systemen ...

13.1 Verfügbarkeit

Der Anwender muss sich darauf verlassen können, dass die Services, die er für die Erledigung seiner Aufgaben benötigt, »immer« verfügbar sind. Dies betrifft alle Komponenten, die ein VPN-System ausmachen, aber auch die Verfügbarkeit des Netzes, insbesondere der Kommunikationsverbindungen über das Internet.

Inwieweit Organisationen (ASPs) in der Lage sind, »Quality of Service« im Internet zu garantieren, hängt wesentlich davon ab, ob die Internet Provider (ISPs) dies zukünftig global anbieten können.

Bezüglich der Verfügbarkeit der Komponenten des VPN-Systems muss ein Verfügbarkeitskonzept erarbeitet werden. Dementsprechend müssen die wichtigsten Komponenten in einem VPN-System redundant ausgelegt werden. Außerdem ist Loadbalancing notwendig, damit eine angemessene Verfügbarkeit realisiert werden kann, um den für die Anwendung notwendigen Grad an »Quality of Service« zu erreichen /Harl2000/.

Aus der Sicht des Anwenders müssen Mindestanforderungen im Bereich »Quality of Service« garantiert werden, damit das Risiko der Nichtverfügbarkeit sinnvoll abgeschätzt werden kann.

13.2 Redundanzsysteme

Um beim Ausfall eines VPN-Gateways die Verfügbarkeit des Netzwerks nicht zu gefährden, werden üblicherweise Redundanzsysteme eingereichtet. Hierzu gibt es verschiedene Möglichkeiten, die im Folgenden erläutert werden.

13.2.1 Parallele VPN-Gateways

Werden zwei VPN-Gateways parallel geschaltet, erhält jeder VPN-Gateway die Verbindungsregeln des parallel geschalteten Geräts. Alle anderen Daten – wie IP-Adresse und Schlüssel – differieren. Diese Betriebsart kann zur Lastverteilung zwischen zwei oder mehreren VPN-Gateways, angewendet werden, die beispielsweise zwischen zwei Netzen positioniert sind.

13.2.2 Passives Redundanzsystem

Ein passives Redundanzsystem dient dazu, ein defektes VPN-Gateway auszutauschen, ohne dass Verzögerungen durch die Personalisierung des neuen Geräts entstehen. Dies ist besonders dann von Vorteil, wenn das zentrale Sicherheitsmanagement-System sich an einem anderen Ort befindet als das ausgefallene VPN-Gateway.

Das »passive Redundanzgerät« wird in der Regel wie jedes andere Gerät personalisiert, aber als »passiv redundant« erfasst. Anschließend wird dieses Gerät wird nicht im Netz installiert, sondern als Ersatzgerät am jeweiligen Einsatzort gelagert. Wenn das im Netz befindliche VPN-Gateway ausfällt, kann es schnell gegen das Redundanzgerät ausgetauscht werden.

13.2.3 Aktives Redundanzsystem

In einem aktiven Redundanzsystem sind üblicherweise zwei parallel geschaltete VPN-Gateways (ein »aktives« und ein »redundantes« Gerät) über ein Kabel miteinander verbunden. Bei Ausfall des »aktiven VPN-Gateways« übernimmt das Redundanzgerät selbstständig dessen Funktion. Abbildung 13.1 verdeutlicht den Aufbau eines aktiven Redundanzsystems.

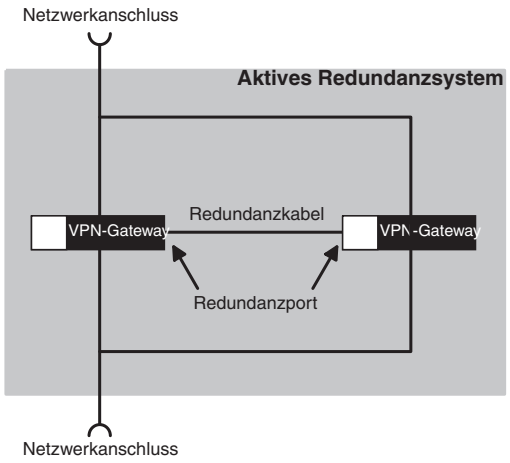


Abb. 13.1: Aktives Redundanzsystem

13.2.4 Redundanzsystem im »Spanning Tree«

Um die Verfügbarkeit eines Netzwerks zu erhöhen, werden in manchen Systemen zwei oder mehrere Switches parallel integriert. Das daraus resultierende Problem der »Schleifenbildung« wird durch ein Protokoll umgangen, das zwischen zwei Kommunikationspartnern einen eindeutigen Weg durch einen dieser Switches bzw. durch alle im Netzwerk befindlichen Switches berechnet. Der Weg wird in regelmäßigen Abständen überprüft und bei einem Ausfall eines Switches wird dieser aus dem Baum entfernt.

Diesen das Netzwerk umfassenden Baum bezeichnet man als »Spanning Tree«, das Protokoll zur Berechnung des Baums als »Spanning Tree Protocol«.

Abbildung 13.2 zeigt, wie ein Redundanzsystem aus zwei VPN-Gateways in eine derartige Netzwerkstruktur integriert werden kann. Die Switches bestimmen mithilfe des »Spanning Tree Protocols«, über welches VPN-Gateway der Netzwerkverkehr geleitet wird.

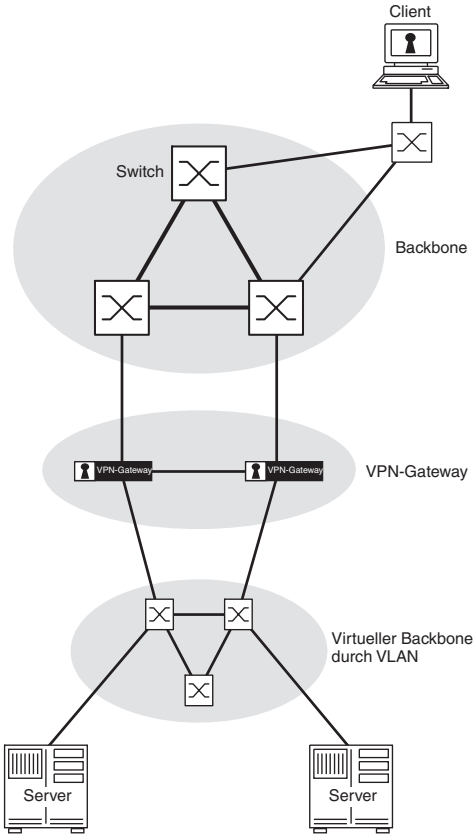


Abb. 13.2: VPN-Redundanzsystem im »Spanning Tree«

13.3 Realisierungsformen für VPN-Gateways

Es gibt unterschiedliche Möglichkeiten, eine VPN-Funktionalität zur Verfügung zu stellen. Die gängigsten Realisierungen bestehen darin, die VPN-Funktionalität in einem Router zu integrieren oder als separate Sicherheitskomponente anzubieten.

13.3.1 VPN-Realisierung im Router

Viele Router, die für die Sicherung der Netze verwendet werden sollen, bieten heute VPN-Funktionalität an. Die in solchen Geräten integrierten Sicherheitsfunktionalitäten sind hinreichend für interne Anwendungen, die nicht besonders sicherheitsrelevant sind, und bieten für diese Fälle eine preiswertere Lösung als separate Sicherheitskomponenten.

Router mit VPN-Funktionalitäten haben jedoch einige Schwächen:

- Die meisten Router bieten, weil sie keine Sicherheitsprodukte sind, nur eine unzureichende Administration der Sicherheitsfunktionen an. Weil das Security Management fehlt, werden dabei immer wieder Fehleinstellungen gemacht, die Sicherheitslöcher verursachen können.
- Router haben in der Regel nur unvollständige Protokollierungsmöglichkeiten und keinen Alarmierungsmechanismus für sicherheitsrelevante Ereignisse.
- Router sind schlecht gegen Angriffe gerüstet, die auf die Sicherheitsmechanismen selber gerichtet sind. Es fehlen Schutzmaßnahmen gegen solche Angriffe, so dass oft die Möglichkeit besteht, von außen über Management-Funktionen die VPN-Funktionalitäten auszuschalten oder das Regelwerk zu ändern.
- In der Praxis nimmt die Performance bei einigen Routern so stark ab, dass die eigentlichen Routing-Aufgaben nicht in der erforderlichen Geschwindigkeit durchgeführt werden können.
- Ein neuer Router, der für diese Aufgabe erst angeschafft werden muss, ist teurer als eine separate Sicherheitskomponente.
- Oft liegt die Verantwortung für den Betrieb der Router in einem anderen Bereich (andere Abteilung oder andere Firma, zum Beispiel Netzdienstanbieter), was die Einhaltung der Sicherheitspolitik schwierig bis unmöglich machen kann.

13.3.2 VPN-Gateways als separate Sicherheitskomponenten

VPN-Gateways als separate Sicherheitskomponenten haben die Hauptaufgabe, die vertrauenswürdige Kommunikation über eine unsichere Netzwerkverbindung zu ermöglichen.

Diese Realisierungsform von VPN-Produkten bietet mehrere wesentliche Vorteile:

- VPN-Gateways können die sicheren Designkriterien leichter erfüllen als Router, weil sie keine zusätzliche Software für andere Aufgabenstellungen benötigen.
- Mit separaten VPN-Gateways wird eine klare Abgrenzung zwischen Kommunikations- und Sicherheitsanforderungen geschaffen.
- VPN-Gateways bieten in der Regel ein separates Sicherheitsmanagement, das auch zentral für die Verwaltung mehrerer VPN-Gateways verwendet werden kann. Dadurch kann eine einheitliche und kontrollierbare Sicherheitspolitik einfach umgesetzt werden.
- Separate Sicherheitskomponenten sind flexibler als Router mit VPN-Funktionalität, weil sie unabhängig von anderen Funktionalitäten sind.

Aber auch die Nachteile separater VPN-Gateways sollen nicht verschwiegen werden:

- VPN-Gateways sind oft teurer als Software-Erweiterungen im Router.
- Die Integration einer zusätzlichen Hardwarekomponente – hier: eines VPN-Gateway – reduziert prinzipiell die Verfügbarkeit der Netzdienste.

13.4 Verwaltung großer VPN-Netzwerke

Bei großen VPN-Netzwerken kommt der Frage, wie eine optimale Konfiguration des Regelwerks durchgeführt werden kann, eine besondere Bedeutung zu. Das folgende Beispiel zeigt, wie komplex das Regelwerk in einem solchen Fall sein kann und wie mithilfe eines zentralen Sicherheitsmanagements sowie »virtueller Komponenten« die Administration wesentlich vereinfacht werden kann.

Abbildung 13.3 zeigt ein großes Netzwerk, das mithilfe von VPN-Gateways abgesichert werden soll. Das VPN-Netzwerk besteht aus 10 IP-Netzwerken [N] mit jeweils 45 Subnetzwerken [S]. Jedes Subnetzwerk soll durch ein VPN-Gateway geschützt werden, insgesamt werden 450 VPN-Gateways eingesetzt. Die Kommunikation zwischen allen Netzwerken bzw. Subnetzwerken soll nur in verschlüsselter Form erlaubt sein.

Wie groß ist die Anzahl der benötigten Regeln [R]?

Aus der Sicht eines VPN-Gateways muss für jedes vorhandene Subnetz (d.h. für jedes andere VPN-Gateway) eine Regel eingetragen werden (z.B. »Subnetz_X darf mit Subnetz_Y in verschlüsselter Form kommunizieren«). Die Summe aller notwendigen Regeln für alle VPN-Gateways wird mit der folgenden Formel berechnet:

$$\mathbf{R}_1 = S*(S-1)/2 = 450*(450-1)/2 = \mathbf{101\ 025}$$

R: Anzahl der Regeln
S: Anzahl der Subnetze

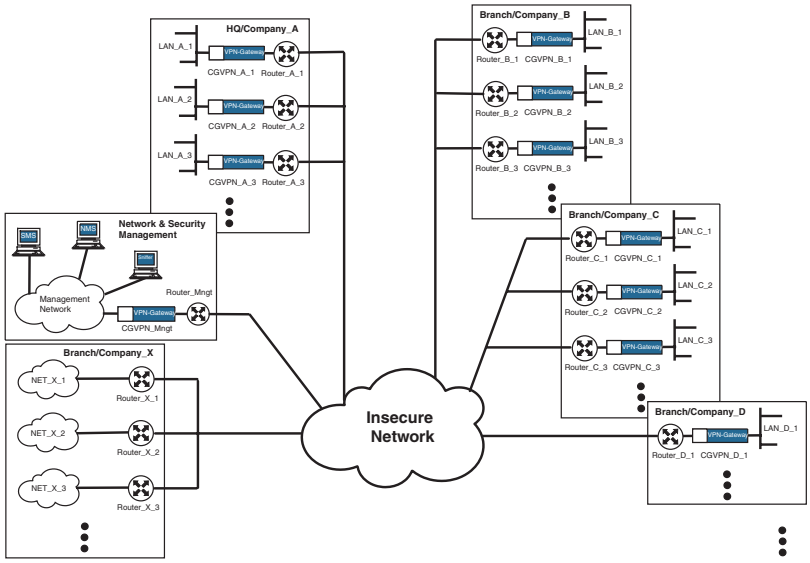


Abb. 13.3: Beispiel für ein großes VPN-Netzwerk

Die Einrichtung und Pflege eines solchen Gesamtnetzwerks mit 101.025 Regeln ist sehr komplex. Abbildung 13.4 verdeutlicht die Komplexität des notwendigen Regelwerks.

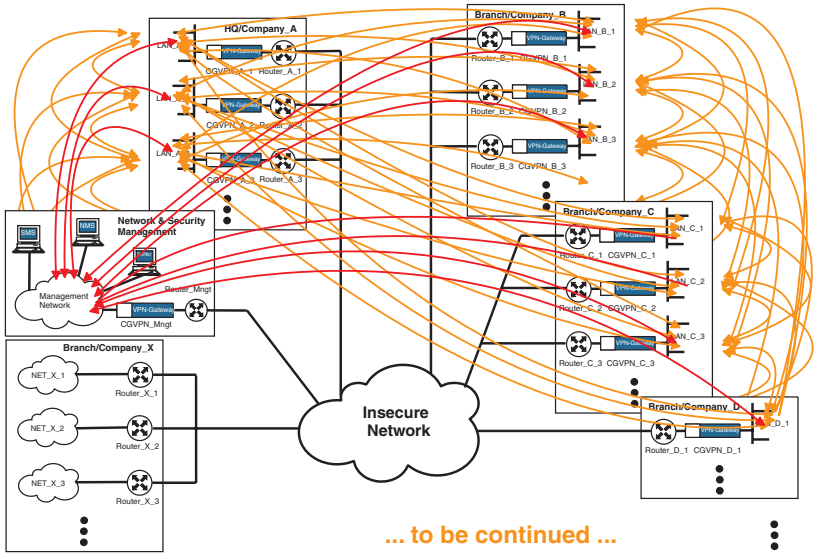


Abb. 13.4: Komplexität des Regelwerks in einem großen VPN-Netzwerk

Welche Alternativen gibt es, um die Anzahl der Regeln zu reduzieren?

Im Folgenden wird beschrieben, mit welchen Hilfsmitteln die Komplexität des Regelwerks minimiert werden kann. Dazu werden im zentralen Sicherheitsmanagement »virtuelle Komponenten« definiert, die die Formulierung von Regeln vereinfachen.

Voraussetzung dafür ist, dass im Sicherheitsmanagement die Möglichkeit, solche »virtuellen Komponenten« zu verwenden, herstellerseitig vorgesehen ist.

- **»Virtual Box«:**
  Die »Virtual Box« ist ein Hilfsmittel, mit dem alle Bestandteile eines IP-Netzwerks N in der Darstellung als ein Objekt zusammengefasst werden können.
  - »Virtual Boxes« dienen der Bildung von Gruppen in der Topologie.
  - Im zentralen Management werden 10 solcher »Virtual Boxes« eingerichtet.
  - Diese sind nicht mit Funktionen verknüpft (d.h., ihnen werden keine Regeln zugewiesen).
  - Ihre Bezeichnung beginnt mit »V_<sector id>«.
  - Wenn möglich, sollten ihre IP-Adressen besonders gekennzeichnet werden, damit die Administration vereinfacht wird.
  - Ort ist »virtual«.

Abb. 13.5: Symbol für eine »Virtual Box«

- **»Dummy Box«:**
  Die »Dummy Box« ist ein (ebenfalls virtuelles) Hilfsmittel, mit dem die Netzwerke aus der Sicht der Endgeräte in den Subnetzen als ein Objekt zusammengefasst werden können.
  - »Dummy Boxes« werden niemals konfiguriert oder installiert.
  - Im zentralen Management werden 10 solcher »Dummy Boxes« eingerichtet. Dies ergibt den Vorteil, dass man die 10 IP-Netzwerke über je einen IP-Adressbereich ansprechen kann, anstatt die jeweils 45 Subnetze einzeln anzusprechen.
  - »Dummy Boxes« werden in virtuellen Verbindungen (Verbindungsregeln) verwendet (z.B. »LAN_A zum S_NET_A«).
  - Ihre Bezeichnung beginnt mit »D_<sector id>«, wobei nur reale Sektoren verwendet werden dürfen.

- Wenn möglich, sollten die IP-Adressen besonders gekennzeichnet werden, damit die Administration vereinfacht wird.
- Ort ist »virtual«.

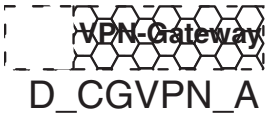


Abb. 13.6: Symbol für eine »Dummy Box«

- **»Super Net«:**
  - »Super Nets« dienen der logischen Gruppierung von Sektornetzwerken.
  - Im zentralen Management werden 10 solcher »Super Nets« eingerichtet, die jeweils den IP-Adressbereich der 45 Subnetze eines IP-Netzwerkes N abbilden.
  - »Super Nets« werden in virtuellen Verbindungen genutzt.
  - Ihre Bezeichnung beginnt mit »S-<sector id>-«.
  - Die Organisationseinheit ist <sector id>, z.B. S_NET_A für Supersektor von A.
  - Um einen Sektor zu beschreiben, sollen so wenige »Super Nets« wie möglich verwendet werden.

Abb. 13.7: Symbol für ein »Super Net«

In Abbildung 13.8 wird aufgezeigt, wie das Gesamtbild des VPN-Netzwerks mithilfe von »virtuellen Komponenten« beschrieben werden kann.

Wie groß ist die Anzahl der benötigten Regeln [R] bei Verwendung »virtueller Komponenten«?

Aus der Sicht eines VPN-Gateways muss für jedes vorhandene »Super Net« eine Regel eingetragen werden (z.B. »Subnetz_X darf mit dem Super Net in verschlüsselter Form kommunizieren«).

Wird das VPN-Netzwerk aus dem oben genannten Beispiel (10 IP-Netzwerke [N] mit jeweils 45 Subnetzwerken [S], insgesamt 450 VPN-Gateways, Kommunikation zwischen allen Netzwerken bzw. Subnetzwerken nur in verschlüsselter Form erlaubt) mithilfe virtueller Komponenten eingerichtet, errechnet sich die Summe aller benötigten Regeln folgendermaßen:

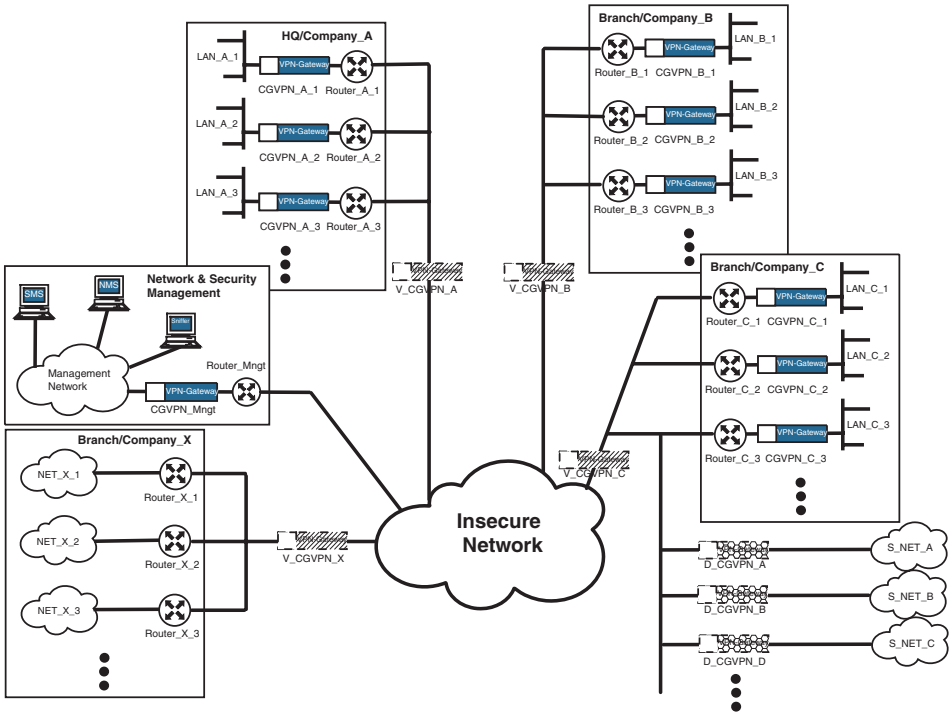


Abb. 13.8: Beschreibung eines großen VPN-Netzwerks mithilfe »virtueller Komponenten«

$\mathbf{R_2}$ = S*N = 450*10 = **4 500**

Ergebnis:

R_1/R_2 = 0,044 = **4,4 %**

Vergleicht man die beiden Varianten, so reduziert sich in diesem Beispiel die Anzahl der notwendigen Regeln bei Verwendung »virtueller Komponenten« auf nur 4,4 % gegenüber der ersten Variante.

Abbildung 13.9 verdeutlicht die Komplexität des Regelwerks. Mit einem zentralen Sicherheitsmanagement, das das oben beschriebene Verfahren unterstützt, und den Hilfsmitteln »Virtual Boxes«, »Dummy Boxes« und »Super Nets« kann die Anzahl der notwendigen Regeln deutlich reduziert werden. Auch komplexe VPN-Netzwerke können auf diese Weise einfacher verwaltet werden.

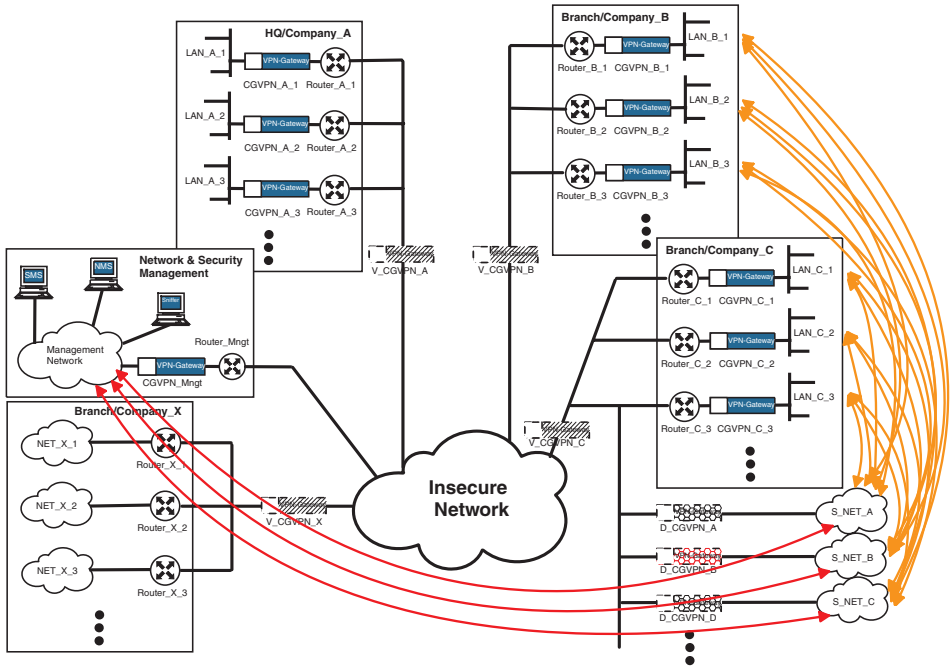


Abb. 13.9: Durch »virtuelle Komponenten« reduzierte Komplexität des Regelwerks

13.5 Zukünftige Entwicklungen bei VPN-Systemen

VPN-Systeme werden sich, wie auch die Kommunikationsanwendungen selbst, in Zukunft weiterentwickeln. In diesem Abschnitt werden schlaglichtartig einige heute schon absehbare Entwicklungen beschrieben.

Innovationen im Bereich der Internet-Anwendungen

Der Bereich der Internet-Anwendungen entwickelt sich ständig weiter. Dementsprechend müssen neue Wege gefunden werden, die VPN-Systeme schnell, dynamisch und ohne Sicherheitsverluste den neuen Anforderungen anzupassen.

Zunahme von Geschwindigkeit und Schutzbedarf

Immer mehr Geschäftsprozesse werden über Kommunikationssysteme abgewickelt. Der Umfang der ausgetauschten Informationen steigt damit stetig. Deshalb werden in naher Zukunft höhere Bandbreiten benötigt, die sich je nach Einsatzzweck unterscheiden werden: Für öffentliche Anschlüsse werden sie zunächst bei 34 bzw. 155 MBit/s, später bei 622 MBit/s liegen, im lokalen Bereich mit Fast Ethernet bei 100 MBit/s, bei Gigabit Ethernet bis zu 1 GBit/s. Um derart hohe Datendurchsätze bewältigen zu können, müssen VPN-Systeme entsprechende Geschwindig-

keiten erbringen. Zugleich wird die Menge der übertragenen und verarbeiteten Informationen mit hohem bis sehr hohem Schutzbedarf steigen.

Damit die zukünftigen Anforderungen an Geschwindigkeit und Schutzbedarf erfüllt werden können, müssen Konzepte erarbeitet werden, wie beispielsweise IPSec-Funktionalitäten optimiert und sicher in Hardwarekomponenten integriert werden können.

Sicherheit als Dienstleistung

Um Sicherheit als Dienstleistung anbieten zu können, wird neben Clustering und Loadbalancing zur Steigerung der Übertragungsraten auch eine Steigerung der Verfügbarkeit von VPN-Systemen (High Availability) erforderlich sein.

Secure Multicast and Group Communication

Eine Herausforderung für VPN-Systeme stellt aus heutiger Sicht unter anderem das Thema »Secure Multicast and Group Communication« dar. Eine Vielzahl neuer Anwendungen, die in Zukunft auch durch VPN-Systeme abgesichert werden sollen (z. B. Multimedia-Anwendungen wie Video-Konferenzen), basieren auf Multicast-Kommunikation (»one-to-many«).

Integratives zentrales Management aller Sicherheitsmechanismen

Damit ein Höchstmaß an Sicherheit garantiert werden kann, wird es in Zukunft immer wichtiger sein, dass unterschiedliche Sicherheitsmechanismen in ein Gesamtsystem mit einem zentralen Sicherheitsmanagement integriert werden können.

Universelle Identifikations- und Authentikationsverfahren

Auf Grundlage des Signaturgesetzes wird in Europa eine Sicherheitsinfrastruktur aufgebaut, die zum Vorbild einer weltweiten Regelung werden könnte. Diese Infrastruktur macht Zertifikate (»elektronische Ausweise«) mit öffentlichen Schlüsseln für alle verfügbar und sorgt für eine eindeutige Identifikation aller Beteiligten. Die Zertifikate der Teilnehmer sind bei den öffentlichen Zertifizierungsinstanzen (TrustCenter) zugänglich und können durch eine einfache Abfrage überprüft werden.

Damit ist es möglich, ein einheitliches Identifikations- und Authentikationsverfahren unter anderem für VPN-Systeme, Rechnersysteme, den Zugang zu Gebäuden etc. zu verwenden. Mit der Chipkarte, über die jeder Teilnehmer dieser Infrastruktur verfügt, kann die Identifikation und Authentikation gegenüber den verschiedenen Systemen durchgeführt werden, wodurch sich wesentliche Vereinfachungen erreichen lassen.

Interoperabilität (IPSec, PKI usw.)

Da die Notwendigkeit sicherer Kommunikation zwischen unterschiedlichen Organisationen immer weiter zunimmt, müssen die bestehenden Interoperabilitätsprobleme dringend gelöst werden. Aus technischer Sicht muss dazu die Kompatibilität der verwendeten Standards (z. B. IPSec) sowie der Sicherheits-Token (z. B. Smart-Cards für unterschiedliche Anwendungen) sichergestellt werden. Zunehmend ist auch die Kompatibilität der Sicherheitsmanagement-Systeme von Bedeutung, damit Sicherheitskomponenten verschiedener Hersteller im Verbund betrieben werden können. In organisatorischer Hinsicht ist die Interoperabilität zwischen verschiedenen Public-Key-Infrastrukturen ein wesentlicher Faktor.

Einen pragmatischen Lösungsansatz auf der technischen Ebene zeigt die Spezifikation »ISIS-MTT«. Auf der organisatorischen Ebene verfolgt die Initiative »European Bridge-CA« das Ziel, eine »Brücke des Vertrauens« zwischen verschiedenen PKIs weltweit herzustellen. Dazu definiert sie Mindestanforderungen an die Policy und die eingesetzte Technik, die eine sichere Kommunikation über organisatorische Grenzen hinweg erlauben.

Anhang A

Computerkriminalität – Fakten und Zahlen

Vorbemerkung

Der etablierte Fachbegriff »Computerkriminalität« umfasst die Kriminalität im gesamten Bereich der Informationstechnologie. Von IT-Kriminalität zu sprechen, ist noch nicht üblich.

Auch beim Deliktsbereich Informations-»Diebstahl« ist die Terminologie unscharf: Meist wird Information zwar unerlaubt kopiert, aber an der Quelle selbst nicht gelöscht. Nach klassischer Definition ist aber Diebstahl »Entwenden einer fremden, beweglichen Sache«. Treffender ist daher der Begriff »Ausspähen von Daten« .

A.1 Kriminalitätsstatistik des BKA

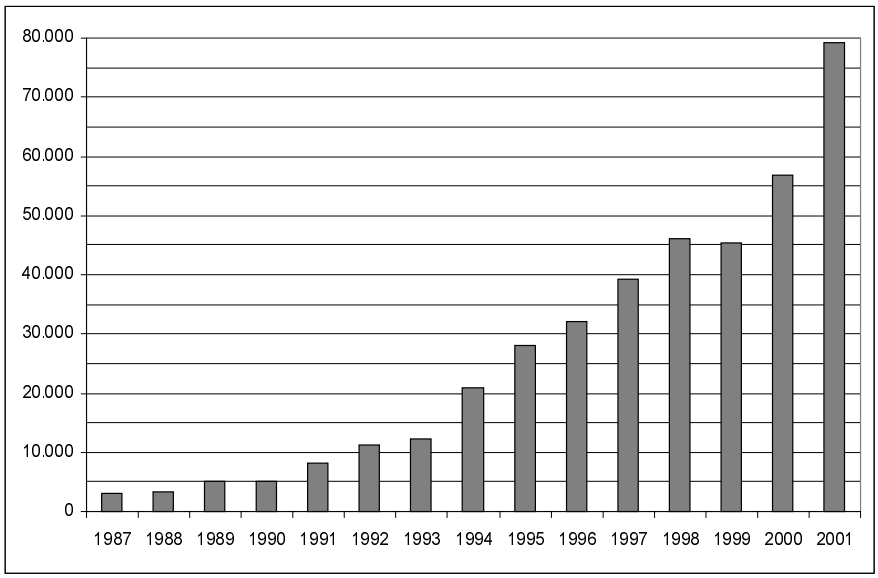


Abb. A.1: Erfasste Fälle von Computerkriminalität in Deutschland

Erfassung der Computerkriminalität in Deutschland

Seit 1987 werden in Deutschland Computerstraftaten in der Polizeilichen Kriminalitätsstatistik des Bundeskriminalamts (BKA) erfasst und vom Innenministerium im Mai des Folgejahrs als Bulletin und im Internet unter www.bka.de publiziert.

Die nachfolgende Auswertung der für den Teilbereich Computerkriminalität relevanten Daten aus dem Jahr 2001 basiert auf dem im Mai 2002 veröffentlichten Bericht.

Dunkelziffer

In der BKA-Statistik fehlen allerdings alle Fälle, die nicht angezeigt bzw. den Ermittlungsbehörden nicht bekannt wurden – wie bei jeder Form von Kriminalität. Über die Höhe dieser so genannten Dunkelziffer ist keine seriöse Schätzung möglich. Sie ist im Bereich Computerkriminalität sicherlich hoch, denn viele betroffene Organisationen und Unternehmen schweigen, um ihr Renommee nicht zu gefährden. Außerdem bleiben Manipulationen und »IT-Einbrüche« durch hoch qualifizierte Industrie- und Wirtschaftsspione oder durch Mitarbeiter (Innentäter) oft unbemerkt.

Bei einigen Deliktsbereichen – beispielsweise bei der Software-Piraterie, die nahezu ein »Massenphänomen« ist – lassen bereits die Zahl der erfassten Fälle und die angegebene Aufklärungsquote erkennen, dass zwischen Statistik und Realität erhebliche Differenzen bestehen können.

Auswertung der BKA-Kriminalitätsstatistik für das Jahr 2001

- 2001 wurden 79 286 Computerstraftaten bekannt, das sind 1,2 % der registrierten Gesamtkriminalität.
- Während die erfasste Gesamtkriminalität in Deutschland seit 1993 stagniert bzw. leicht rückläufig ist, stieg die Computerkriminalität bis 1998 im zweistelligen Prozentbereich und war damit der bei weitem am stärksten wachsende Kriminalitätsbereich überhaupt. Nach einem Rückgang um 1,5 % im Jahr 1999 setzte sich in den folgenden Jahren der Anstieg weiter fort. Im Jahr 2000 lag der Zuwachs im Mittel bei 25 %, 2001 bei knapp 40 %. Für die letzten zwei Jahre ergibt sich somit ein Anstieg der Computerkriminalität um insgesamt 75 %.
- Auffallend ist die heterogene Entwicklung der einzelnen Deliktsbereiche, die im Jahr 2001 von einem Rückgang um 56 % bei der »Software-Piraterie in Form gewerbsmäßigen Handelns« bis zu einem Anstieg um 266 % beim »Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten« reichte (siehe nachfolgende Tabelle).
- Die Aufklärungsquote lag 2001 bei 57 % und damit um knapp 4 % über dem Durchschnitt der Gesamtkriminalität.

Deliktsbereiche, Fallentwicklung und Aufklärungsquoten

Bereiche der Computerkriminalität	Fälle 2001	Änderung zu 2000	Aufklärungs-quote
Betrug mittels rechtswidrig erlangter Karten für Geldausgabe- bzw. Kassenautomaten	48 610	+ 10 %	42 %
Computerbetrug (§ 263 a StGB)	17 310	+162 %	78 %
Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	8 039	+266 %	84 %
Computer-Software-Piraterie			
– zur privaten Anwendung	1 672	+ 23 %	99 %
– in Form gewerbsmäßigen Handelns	410	- 56 %	96 %
Fälschung beweiserheblicher Daten oder Täuschung im Rechtsverkehr bei Datenverarbeitung	920	+243 %	96 %
Ausspähen von Daten	1 463	+172 %	83 %
Datenveränderung oder Computersabotage	862	+ 68 %	45 %

- Über 60 % aller erfassten Computerstraftaten fielen 2001 in den Bereich **Kredit-, Bank- und Geldkartenbetrug**, das sind mehr als 48 000 Fälle. Betrug in diesem Bereich wird meistens angezeigt, so dass die Dunkelziffer als eher klein einzuschätzen ist. Die Aufklärungsquote betrug lediglich 42 %.
  Zu diesem Deliktsbereich schreibt das BKA:

  »Bei weiter fortschreitender Technisierung (elektronische Geldbörse) und Expansion des Einsatzes neuer Techniken durch Straftäter wird dieses Deliktsfeld in den nächsten Jahren weiter an Bedeutung gewinnen. Deshalb bedarf es weiterhin gemeinsamer Anstrengungen von Politik, Wirtschaft und Polizei sowie der Förderung der fachlichen Spezialisierung. Gefordert sind insbesondere Präventionsleistungen der Industrie durch technische Sicherung ihrer Produkte. [...] Durch zwingende Benutzung einer PIN könnten in diesem Bereich durchgreifende Verbesserungen erzielt werden.«

- Mehr als jede fünfte Computerstraftat fiel 2001 in den Bereich **Computerbetrug**. Beispiele dafür sind Manipulationen von Programmen oder Daten im Abrechnungswesen und Veränderungen der Programme von Geldspielautomaten zur Erhöhung der Gewinnchancen.
- **Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten** umfasste über 8 000 Fälle. Dazu gehört das Einloggen bei Internet-Providern mit fremden oder gefälschten Zugangsdaten, aber auch das unbefugte Entsperren von so genannten SIM-Locks bei Mobiltelefonen sowie »Zugangserschleichungen zu Telefonanschlüssen mit illegalem Anwählen von mit hohen Kosten verbundenen 0190er-Nummern« (BKA). Die Aufklärungsquote von 84 % deutet dar-

auf hin, dass solche Fälle überwiegend dann angezeigt wurden, wenn es Hinweise auf den Täter gab. Die Dunkelziffer ist als beträchtlich höher einzuschätzen.

- Bei der **Software-Piraterie** (Raubkopieren) fällt auf, dass wesentlich mehr Delikte im privaten Bereich als im Rahmen »gewerbsmäßigen Handelns« registriert wurden. Zusammen mit dem Rückgang der Fallzahlen in der zweiten Kategorie um 56 % und der sagenhaften Aufklärungsquote von im Mittel 98 % deutet dies stark darauf hin, dass fast ausschließlich aufgeklärte Fälle erfasst wurden. Die Gesamtzahl von 2 082 Fällen liegt mit Sicherheit weit unter den tatsächlichen Verhältnissen.
- Der Gesamtbereich **Fälschung/Täuschung/Ausspähung/Veränderung/Sabotage** umfasste insgesamt 3 245 Fälle und damit 'nur' 4 % aller Computerdelikte, allerdings ist je nach den Umständen von erheblichen Schadenshöhen pro Delikt auszugehen.

A.2 Schätzungen der Schadenshöhe

Das Bundeskriminalamt nennt keine Schadenshöhen durch Computerkriminalität.

Für den Teilbereich Wirtschaftsspionage gibt es Schätzungen von verschiedenen Institutionen: Der Verlust, den deutsche Unternehmen durch Wirtschaftsspionage erleiden, wird zwischen 4,25 und 20 Milliarden EUR pro Jahr taxiert.

Computer-Hacker kosteten europäische Firmen laut Omni Consulting Group im Jahr 2000 über 9 Milliarden DM Umsatz:

»Hackers cost firms billions of dollars

Computer hackers cost European businesses $ 4.3 bn in lost revenue last year, according to recent research. A study of 3,000 businesses worldwide found that lapses in security cost companies between 5.7 and 7 per cent of their annual revenue, or six cents for every dollar in sales.

Frank Bernhard, managing principal of Omni Consulting Group, which carried out the study, said online security problems are growing faster than anyone could imagine. »That whole issue could explode,« he said, adding that when hackers break into company source code, »you're into billions of dollars that just walked out the door.« Bernhard believes that companies need to consider their intellectual property assets and cited Microsoft's recent denial-of-service attacks, which crippled most of its major web properties, as an example.

»The answer is clear: [Microsoft] did not have a corporate policy body looking at security [and] now it does,« he said. Bernhard believes that although European companies are less stringent about introducing security policies and are more relaxed about intrusion threats, they are beginning to recognise the implications

> of hack attacks and the need for protection. »European organisations are more adapt and inclined to scale up towards network security,« he said. He stressed that companies need to put security measures in place and implement policies to protect their intellectual properties. He gave the example of someone walking into an office building and stealing a photocopier. »How can you miss someone walking out with the equipment and how can you miss someone walking away with your source code?«
>
> The study found that non-IT organisations and manufacturing companies were best at protecting their intellectual properties. »The ones that we'd think have the security tools are the weakest link in the puzzle,« he said.«
>
> (Quelle: `www.vnunet.com/News/1117559`)

Die 1998er Studie vom US Computer Security Institute und FBI taxiert den Schaden durch IT-Kriminalität in den USA auf 10 Milliarden US-Dollar jährlich. Schätzungen für den Bereich Industriespionage allgemein in den USA reichen von 63 bis 300 Milliarden Dollar pro Jahr.

Weil der Schaden für Unternehmen existenzbedrohend sein kann, bietet Lloyds seit 1999 erstmals eine Versicherung an, die bis zu einer Höhe von 50 Millionen Dollar vor Risiken des Informationsverlustes durch Cracker, Viren, Computersabotage oder Datenverlust schützt.

A.3 Fallbeispiele

Zum Abschluss sollen einige Fallbeispiele belegen, dass IT-Kriminalität eine reale Bedrohung ist. Kaum ein Tag vergeht, ohne dass die Presse und Online-Informationsdienste, zum Beispiel der Newsticker des Heise-Verlags (`www.heise.de/newsticker`), entsprechende Delikte melden.

Betrug, Erpressung

Der Bereich Kreditkartenbetrug wird von den Geldinstituten verschleiert, um die Kundenakzeptanz nicht zu beeinträchtigen. Der Verlust, den die Banken stillschweigend ertragen, mindert die enormen Rationalisierungsgewinne durch Informationstechnologie nicht wesentlich. Jedoch sind die geschädigten Kunden oft in Beweisnot.

Grundsätzlich sind alle Unternehmen im E-Commerce-Bereich durch IT-Kriminalität gefährdet, wie zwei exemplarische Fallbeispiele zeigen sollen:

- Im Dezember 1999 erpresste ein zunächst »unbekannter Russe« ein Unternehmen mit gestohlenen Kreditkarteninformationen – 300 000 Kreditkartennummern – und publizierte diese teilweise im Web, um seiner Forderung

Nachdruck zu verleihen. Schlagzeile der WELT vom 13.1.2000: »Der größte Datendiebstahl aller Zeiten«.

- Im Januar 2000 berichteten Zeitungen, dass britische Cracker in Systeme von mindestens zwölf internationalen Firmen – unter anderem des Kreditkartenunternehmens Visa – eindrangen, Quellcodes kopierten und Erpressungsgeld in Höhe von insgesamt 31 Millionen Mark forderten. Ein Scotland-Yard-Ermittler sprach von »der bisher schwersten systematischen Verletzung von Sicherheitssystemen«.

Site-Hacking

- Am 5.11.1999 meldeten die Tageszeitungen Site-Hacking beim rumänischen Finanzministerium. Auf dessen Internetseite wurden »Steuern auf Dummheit« angekündigt.
- Im Januar 2000 gelang es chinesischen Hackern, systematisch die Internetseiten verschiedener japanischer Behörden zu hacken und Protest gegen das Nanking-Massaker von 1937 anzubringen, was im »High-Tech-Land Japan« als große Blamage empfunden wurde (Quelle: FAZ vom 28.1.2000).
- Unbekannte veränderten vor einigen Jahren die Homepage des amerikanischen Justizministeriums in »U.S. Department of Injustice«. Schwedische Hacker änderten die CIA-Homepage in »Central Stupidity Agency« und legten »Hot«-Links zu Sex- und Musikangeboten. Eine weitere Blamage: Unbekannte änderten das CIA-Logo in »Central Idiots Agency« und dieses Fake stand volle vier Tage im Web.
- Zunehmend werden auch politische Auseinandersetzungen zum Anlass für Hackerangriffe genommen. So kam es zu einem mehrwöchigen »Schlagabtausch« zwischen chinesischen und US-amerikanischen Hackern, nachdem am 1.4.2001 ein chinesischer Pilot beim Zusammenstoß seines Kampfjets mit einem US-Aufklärungsflugzeug über dem Pazifik getötet worden war.
  Auch nach den Terroranschlägen in New York und Washington am 11.9.2001 traten Hacker in Aktion; in diesem Fall waren Webseiten islamischer Organisationen Ziel diverser Attacken.

Mehr Informationen über solche zweifelhaften »Erfolge« finden Sie im Archiv von »2600 – The Hacker Quarterly« unter `www.2600.com/hacked_pages` und unter `www.ccc.de` (Chaos Computer Club Hamburg e.V.) sowie unter `www.alldas.de`, wo gezeigt wird, was Cracker und »Scriptkiddies« angerichtet haben.

Täuschung durch Manipulation von Information

- Im Dezember 1999 meldeten die Tageszeitungen ein Beispiel dafür, dass die Veränderung von Informationen auf der Site eines großen US-Wirtschaftsdienstes die Börse beeinflusste: »Pairgain Technologies wird übernommen«, lautete dort eine illegal platzierte Meldung.

Informationsbeschaffung

- Eine Milliarde Dollar Streitwert hat das Gerichtsverfahren eines Erdöl-Konzerns gegen einen IT-Dieb, der die Ergebnisse von Testbohrungen in einem neuen Ölfeld crackte (Quelle: Verbrauchermagazin DM 1/2000).
- 1993 wurde der General Motors Manager Lopez mit einem Teil seiner »Warriors« genannten Managerriege von VW abgeworben. Neben 23 000 Blatt vertraulicher Unterlagen brachten sie auch Informationen auf Datenträgern bei VW ein. Die IT-Spezialisten der Staatsanwaltschaft Darmstadt fanden bei einer – zuvor verratenen – Hausdurchsuchung trotz frisch formatierter Festplatten im IT-System von VW Hinweise auf den Informationsraub. Nach außergerichtlicher Einigung leistete VW an GM einen sehr hohen Schadensersatz.
- Jahrelang wurde das Rechnersystem der EU von US-Geheimdienststellen online angezapft und vor wichtigen internationalen Wirtschaftskonferenzen wurden die jeweiligen nationalen Strategien ausspioniert.
- 1997 wurde die Entwicklungsdatenbank der BASF »geknackt und möglicherweise komplett ausgeräumt« (laut Verbrauchermagazin DM 1/2000).
- 1999 wurden im PDS-Parteibüro Laptops und Festplatten gestohlen. BILD-Schlagzeile am 30.7.1999: »Einbrecher stehlen Gysis Computerdaten«.
- Am 4.1.2000 meldete die Frankfurter Rundschau, das gesamte Nuklearwaffenprogramm der USA – ein virtueller Katalog, der 800 000 Seiten entspricht – sei von einem Innentäter auf Datenträger kopiert worden.
- Im Januar 2000 wurde bekannt, dass ein 16-Jähriger aus Kalifornien 27 Internet Service Provider gehackt hat und dabei über 200 000 Passwörter erbeutete.
- Ein ähnlicher Fall ereignete sich 2001 in Deutschland: Eine Gruppe von etwa 30 Personen hatte die Passwörter von mehreren tausend Internetnutzern ausspioniert und auf einschlägigen Webseiten veröffentlicht. Die Zugangsdaten wurden vermutlich in mehreren tausend Fällen von Dritten missbraucht, um auf fremde Kosten im Internet zu surfen oder falsche Online-Verträge mit Internet-Providern abzuschließen (Quelle: Spiegel Online, 3.11.2001).

Industrie- und Wirtschaftsspionage

Nach Ende des Kalten Kriegs betreiben die Geheimdienste Wirtschaftsspionage als neuen Schwerpunkt. Sie verfügen über das Know-how und die beste verfügbare personelle und technische Ausstattung für »elektronische Raubzüge« ohne Spuren.

Aufschlussreich ist der Bericht des Scientific and Technological Options Assessment (STOA) des Europäischen Parlaments: »An Appraisal of the Technologies to Political Control«; Download und aktuelle Ergänzungen siehe `www.europarl.eu.int/dg4/stoa/en` oder `http://cryptome.org/stoa-atpc.htm`.

Durch den weltweit verschärften Wettbewerb wird Industriespionage für Unternehmen Gewinn bringend. Beauftragte High-Tech-Spione stehlen gezielt Know-how und Strategiepläne der Konkurrenz. Forschungs- und Entwicklungskosten können so drastisch reduziert werden. Dabei existiert kein Unrechtsbewusstsein, Konkurrenten werden mit allen verfügbaren Mitteln ausgebootet:

- Siemens verlor den ICE-Auftrag in Korea, weil der französische Geheimdienst das endgültige Angebot ausspionierte. Siemens-Deutschland hatte unverschlüsselt an seine Niederlassung gefaxt, das Angebot wurde daraufhin vom TGV-Konsortium unterboten.
- Enercon konnte seine Windkraftanlagen nicht in die USA exportieren, weil die Technologie bereits durch gezielten Informationsdiebstahl von der Konkurrenz patentgeschützt war.
- Airbus verlor 1994 einen Großauftrag an Boeing, weil die staatlichen Lauscher des NSA über das Echelon-System – siehe `www.echelonwatch.org` – alle Faxe und Telefonate zum Verhandlungspartner in Saudi-Arabien abhörten.

Software-Piraterie

Der »Diebstahl« von Software (Raubkopieren, Software-Piraterie) ist inzwischen ein großer Bereich der Schattenwirtschaft:

- Im Januar 2000 meldeten die Zeitungen, dass eine Düsseldorfer Bande für geschätzte 1,5 Milliarden DM CD-Sets mit Raubkopien von begehrten Programmen in Auflagen von bis zu 20 000 Stück vertrieben hatte.

Virus-Schäden

- Selbst Viren ohne Schadensfunktionen können zu beträchtlichen finanziellen Schäden führen:
  Im November 1999 kam es laut Pressemeldungen beim PC-Hersteller DELL in Irland nach der Installation eines Updates der Anti-Viren-Software zur Meldung, dass Geräte mit dem Virus »FunLove«, einem harmlosen Windows-Virus, infiziert seien. Es wurden rund 12 000 Computer überprüft. Diese waren zum Teil schon ausgeliefert und mussten für diesen Zweck zurückgerufen werden. Der Gesamtschaden wird auf rund 22 Mio. US$ geschätzt.
- Seit dem Auftreten des »ILOVEYOU«-Virus am 4.5.2000, der mithilfe eines »Viren-Baukastens« konstruiert worden war, vergeht kaum eine Woche ohne einen neuen oder »mutierten« Skriptvirus. Besonders dreist gingen Virenprogrammierer in zwei Fällen im Herbst 2001 vor, indem sie ihre Machwerke als Sicherheits-Patch für Microsoft-Produkte (»Redesi«-Wurm) bzw. als »neuen kostenlosen Trojanerscanner« (»Ants«-Wurm) getarnt hatten. Viele Anwender ließen sich durch diese Spielart des Social Engineerings täuschen und trugen mit einem Doppelklick auf das vermeintliche Sicherheitsprodukt zur Weiterverbreitung der Schädlinge bei.

- Gleich mehrere Verbreitungswege nutzte im September 2001 der Wurm »Nimda« aus und infizierte dadurch eine große Zahl von Rechnern: Er verbreitete sich als E-Mail-Attachment, über Web-Server, in deren Webseiten er JavaScript-Code einschleuste, sowie innerhalb von lokalen Windows-Netzwerken über freigegebene Laufwerke und Ordner. Zu seinen Schadensfunktionen gehörte neben der Manipulation von System- und Programmdateien die Einrichtung eines Gast-Accounts mit Administrator-Rechten auf Windows-NT/2000-Systemen, der als Hintertür für andere Angreifer aus dem Internet dienen kann.
  Verbreitung und Schadenshöhe lassen sich nur schwer erfassen, US-amerikanische Medien schätzen jedoch, dass allein 2,2 Millionen Server infiziert wurden, wodurch ein Schaden von über 500 Millionen Dollar entstand.

Anhang B

Recht im Internet

Das Vordringen der Informations- und Kommunikationstechnik in fast alle Lebensbereiche hat neue IT-Delikte hervorgebracht und die Computerkriminalität insgesamt vielfältiger und gefährlicher gemacht. Mit der Verbreitung der weltweiten Netze sind Veränderungen der Täter- und Opferprofile einhergegangen: Computerdelikte können heute von jedermann vom Wohnzimmersessel aus begangen werden und jeder kann Opfer werden. Die elektronische Datenverarbeitung ist mit der Telekommunikation zusammengewachsen, so dass die Delikte zunehmend über Telekommunikationsnetze, auch vom Ausland aus, begangen werden und neue Formen angenommen haben. /Pohl 2000/

In kaum einem anderen Bereich zwischenmenschlicher Kommunikation gibt es so viele Verstöße gegen geltendes Recht wie im Internet: Beleidigungen, Verleumdungen, Boykotte, Namens- und Markenrechtsverletzungen, Verstöße gegen das Urheberrecht usw. sind an der Tagesordnung. Mit der wachsenden Bedeutung der Kommunikation in und über Netze wird offensichtlich, dass rechtliche Regelungen unumgänglich sind. Wo immer mehr Menschen im und mit dem Netz Geld verdienen wollen, verstärkt sich der Handlungsbedarf, im zwar nicht »rechtsfreien«, aber bisher fast »rechtsfolgenfreien« Raum rechtsverbindliche und auch in der Praxis durchführbare Orientierungshilfen zur Verfügung zu stellen.

Die neuen Kommunikationsmöglichkeiten bringen dabei eine ganz neue Dimension von Rechtsverstößen mit sich. Das hängt zum einen mit der nie dagewesenen weltweiten Relevanz von Handlungen zusammen, die es jedem einfachen Benutzer einer Mailbox ermöglicht, in einem anderen Teil der Welt für Unruhe zu sorgen, ohne dass er sich der Verantwortung bewusst ist, die mit solchen Befugnissen normalerweise verbunden ist.

B.1 Aktuelle Formen des Delikts »Computerkriminalität«

Bei den neuen Rechtsverstößen im Internet handelt es sich nicht um Delikte, die vor der Vernetzung unbekannt waren, sondern um altbekannte Rechtsverletzungen, die sich in neuem Gewand präsentieren. Gesetzgeber und Justiz stehen ihnen daher nicht hilflos gegenüber, sondern sie müssen altbewährtes Recht den neuen Dimensionen anpassen. Die häufigsten Missbräuche wie Persönlichkeitsrechtsverletzungen und vor allem Wirtschaftsdelikte sind ja keine gänzlich neuen Delikte, sondern aktuelle Formen von Verstößen, die seit jeher geahndet werden und spätestens seit Erfindung der EDV die Rechtsprechung beschäftigt haben.

B.1.1 Persönlichkeitsrechtsverletzungen

Das Persönlichkeitsrecht des Bürgers ist gesetzlich geschützt und kann durch Sammlung, Speicherung, Weitergabe oder Verknüpfung personenbezogener Daten verletzt werden. In heutigen Statistiken spielen Persönlichkeitsrechtsverletzungen nur eine geringe Rolle. Allerdings kann sich dies durch die neuen Möglichkeiten im Internet schnell ändern: Delikte wie die Benutzung unrichtiger Daten (zum Beispiel falsche Adressangabe bei E-Mail), die unbefugte Erlangung von Daten, die unbefugte Sammlung, Speicherung, Weitergabe oder Verwendung personenbezogener Daten und der Verstoß gegen die Formalvorschriften des Datenschutzrechts finden hier einen neuen, fruchtbaren Nährboden.

Elektronischen Nachrichten fehlt so etwas wie ein »digitaler Briefumschlag«. Mit entsprechendem technischem Know-how können Filter in die Transportserver (MTAs) eingebaut werden, die den Datenfluss analysieren und bestimmte E-Mails herausfischen können. Auf diese Weise können zum Beispiel die E-Mails an einen bestimmten Empfänger abgefangen, auf ein anderes Rechnersystem umgeleitet und dort eingesehen werden.

Ein Beispiel besonders unverfrorener und vor allem professioneller Beschaffung von Daten lieferte 1996 ein Unbekannter beim US-amerikanischen Internet-Provider Prodigy: Eingeloggten Mitgliedern wurde während des Surfens die Aufforderung zugestellt, sich umgehend bei ihrem Provider zu melden. Unter der angegebenen Telefonnummer meldete sich eine Voicebox, die mit dem Hinweis auf Probleme bei der letzten Beitragsrechnung um den Namen, die Adresse, die Kreditkartennummer, Telefonnummer und den Geburtstag bat. Diese Auskünfte wurden von etlichen Benutzern geliefert, die erst Wochen später bei der nächsten Abrechnung merkten, dass man sie hereingelegt hatte.

B.1.2 Wirtschaftsdelikte

Das Internet hat mit seinem rasanten Wachstum auch die Möglichkeiten von Wirtschaftsdelikten aller Art enorm gesteigert. Computermanipulationen, Sabotage und Erpressung, Hacking, Spionage, Softwarediebstahl und andere Formen der Produktpiraterie breiten sich schneller aus, als Politik und Gesetzgebung ihnen mit entsprechenden Gesetzen, Verboten oder Strafen Einhalt gebieten könnten.

Computermanipulationen

Zu den klassischen Computermanipulationen zählen Abrechnungsmanipulationen wie Gehalts- und Rechnungszahlungen von Industrieunternehmen, Bilanzmanipulationen und Kontostandsmanipulationen bei Banken. Die derzeit noch vorherrschende Sorglosigkeit der Organisationen lädt Hacker geradezu ein, sich an ihren Rechnersystemen zu versuchen.

Seit einigen Jahren sind Kartenmissbräuche das häufigste Computerdelikt. Geschichten von findigen Tüftlern, die wiederaufladbare Telefonkarten konstruiert

oder Kreditkarten gefälscht haben, liest man immer wieder in der Presse. Neue Möglichkeiten des Missbrauchs bieten elektronische Zahlungsmittel. Für diese Systeme gewinnt die Sicherung durch Chipkarten-Technologie an Bedeutung.

Im Internet soll sich jetzt der elektronische Geldverkehr bewähren, der mit Electronic Sales, Cybermoney und Electronic Banking auf dem Vormarsch ist und nicht nur für Banken und Geschäfte im Internet, sondern auch für kriminelle Aktivitäten reichlich neue Perspektiven bietet.

Während das Telefonnetz früher allenfalls manipuliert wurde, um die eigene Telefonrechnung zu verfälschen, hat inzwischen eine qualitative Veränderung der Manipulationen im Telefonnetz stattgefunden. Seit unzureichend geschützte und nicht zu diesem Zweck entwickelte Telefonnetze in unvorsichtiger Weise zur Abrechnung von Dienstleistungen eingesetzt werden, finden auch zunehmend finanzielle Manipulationen mit dem Ergebnis der Überweisung von Geldern statt.

Computersabotage und -erpressung

Viren- und Wurmprogramme, die vor allem über raubkopierte Software oder in Netzwerken verbreitet werden, verursachen massenhaft Schäden. Im Internet bietet sich die neue Möglichkeit, im Hintergrund von Programmen, vom Benutzer unbemerkt, eine Art Zeitbombe zu installieren, die nach einer bestimmten Zeit Programme zerstört oder die Festplatte gründlich »aufräumt«.

Die Abhängigkeit der Informationsgesellschaft von Rechnersystemen macht Computererpressung zu einer gefährlichen Angriffsform. Mit der Drohung, Rechnersysteme und Datenbestände unbrauchbar zu machen, lassen sich Organisationen erpressen, die sich nicht ausreichend abgesichert haben.

Hacker

Beim klassischen Computerhacking stand vor allem die Freude an der Überwindung technischer Sicherheitsmaßnahmen im Vordergrund, die das angegriffene Unternehmen schädigte und bei der Spätschäden drohten, wenn die erlangten Kenntnisse zur Begehung von Spionage- und Sabotagehandlungen genutzt wurden. Rechtlich waren die Geheimnissphäre und die Integrität des betroffenen Rechnersystems beeinträchtigt.

Im Telefonnetz gibt es massenhaft Missbräuche durch Phreaker in Telefonleitungen, Anrufbeantwortern und Voice-Boxen, zum Beispiel das Mithören von Gesprächen und die Nummern von Telefonberechtigungskarten. Durch das digitale ISDN-Netz und die Verbindung von Telefon- und Computertechnik sind neue Möglichkeiten des Missbrauchs entstanden.

So erlaubt der neue Dienst »leistungsfähiger Messaging Service für Netware-LANs« computergenerierte Telefonanrufe, die dazu missbraucht werden können, gezielt Telefonterror zu betreiben: mit entsprechender Botschaft und per Knopf-

druck eingestellter Stimme (beispielsweise Flüstern) kann man ein Telefon zu einer beliebigen Uhrzeit klingeln lassen und am anderen Ende der Leitung Angst und Schrecken verbreiten.

Wirtschaftsspionage

Schon die klassische Wirtschaftsspionage versprach hohe Gewinne, die heute durch den Reiz großer Datenmengen auf kleinstem Raum, schnell und einfach zu kopieren, um ein Vielfaches gewachsen sind. Tatobjekte sind Programme, Forschungs- und Rüstungsdaten, Daten des kaufmännischen Rechnungswesens sowie Kundenadressen. Die Täter sind meist jugendliche Hacker, konkurrierende Organisationen und zunehmend auch Nachrichtendienste.

Zur Spionage zählt auch das Abhören von Telefongesprächen. Autotelefone, Richtfunksender und Satellitenverbindungen sind bei unverschlüsselter Kommunikation leichte Angriffsziele.

Softwarediebstahl und andere Formen der Produktpiraterie

Die unbefugte Kopie und Nutzung fremder Computerprogramme betraf früher vor allem Individualsoftware, während heute die rechtswidrige Kopie von massenhaft vertriebener Standardsoftware dominiert. Datenbanken und andere Datensammlungen sowie die unbefugte Nutzung von Multimedia-Produkten und ähnlichem erfreuen sich zunehmender Beliebtheit. Wenn Pay-TV-Sender ihren auf Verschlüsselung beruhenden Bildsignalton ändern, vergehen immer nur wenige Tage, bis der elektronische Nachschlüssel auf einschlägigen Internetseiten auftaucht. Software-, Musik-, Video-, und Multimediapiraterie werden durch die Verbreitung von Geräten zum Abspielen und Herstellen von CDs und DVDs erleichtert.

B.1.3 Sonstige Delikte

Die Verbreitung von gewaltverherrlichenden, rassistischen oder pornografischen Informationen sowie der zunehmende Einsatz von Rechnersystemen bei der organisierten Kriminalität und die Gefahr möglicher Manipulationen in Kernkraftwerken, Rüstungssystemen usw. sind die stärksten Argumente von Befürwortern einer »Cyberpolizei«. Computermissbrauch ist zu einer globalen Bedrohung geworden und die Sicherheit moderner Rechnersysteme hat für die heutige Informationsgesellschaft zentrale Bedeutung gewonnen.

B.2 Rechtsfragen

Der Gesetzgeber in Deutschland hat auf die neuen Kriminalitätsformen in vier Wellen computerspezifischer Reformen reagiert: Persönlichkeitsschutz, Wirtschaftsstrafrecht und der Schutz des geistigen Eigentums wurden in verschiedenen Reformwellen in den 70er und 80er Jahren erfaßt, wobei unter anderem der zivilrechtliche Urheberrechtsschutz, das Urheberstrafrecht und der Rechtsschutz

von Topografien sowie die allgemeinen Regelungen zur Produktpiraterie den neuen Anforderungen angepaßt wurden. Die entsprechenden Reformgesetze umfassen öffentlich-rechtliche und zivilrechtliche Maßnahmen mit Schwerpunkt im Strafrecht.

In Deutschland bereits gültige Bestimmungen, die im Internet den gesetzlichen Rahmen bilden, sind im Einzelnen:

- das Gesetz über das Urheberrecht und verwandte Schutzrechte,
- der Staatsvertrag über Bildschirmtext,
- das Gesetz über Fernmeldeanlagen (FAG),
- das Telekommunikationsgesetz (TKG), die Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen,
- die Verordnung über den Datenschutz bei Dienstleistungen der Deutschen Bundespost/Telekom,
- das Gesetz über die Verbreitung jugendgefährdender Schriften (GjS),
- das Strafgesetzbuch (StBG) und
- das Grundgesetz (GG).

In den meisten westlichen Staaten war die Reaktion ähnlich. Internationale Organisationen wie OECD, Europarat, EU, WIPO, WTO und AIDP begleiteten die nationalen Reformmaßnahmen. Der Druck der Industrie förderte die Rechtsvereinheitlichung, wodurch es zu raschen Lösungen kam, die aber ad hoc und isoliert waren und denen keine grundsätzlichen Überlegungen zur Rolle des Strafrechts in der Informationsgesellschaft zugrunde lagen.

B.3 Paradigmenwechsel und Perspektiven

Der Wandel von der Industrie- zur Informationsgesellschaft hat Folgen für das Rechtssystem und die aus der entstehenden Risikogesellschaft resultierenden Veränderungen des Strafrechts.

Dieser Wandel (»zweite industrielle Revolution«) bedeutet vor allem eine Verlagerung menschlicher Geistestätigkeit auf Maschinen. Neben körperlichen Dingen gewinnen zunehmend unkörperliche Werte wie elektronisches Geld, Urheberrechte, Geschäftsgeheimnisse und sonstiges Know-how an Bedeutung. Information ist ein neuer Wert, der auch Machtfaktor und Gefährdungspotential bedeutet.

Der gesellschaftliche Paradigmenwechsel hat das Strafrecht bereits erreicht, aber es fehlt eine allgemeine Theorie für den Schutz von Informationen, die zu der dritten Grundgröße neben Materie und Energie geworden sind. Information ist ein neues wirtschaftliches, kulturelles und politisches Gut, das aber auch neue Probleme schafft. Die moderne Informationstechnik steigert den Wert von Information: Information wird zu einem aktiven Faktor, der in automatischen Datenverarbeitungssystemen ohne weiteres menschliches Zutun Veränderungen

vornimmt, und in manchen Bereichen ersetzen informationstechnische Systeme menschliche Entscheidungen.

Bei der rechtlichen Beurteilung materieller und immaterieller Güter gibt es einige Unterschiede zu beachten: Während Eigentum oder Besitz an materiellen Gütern geschützt werden können, handelt es sich beim immateriellen Gut Information um ein öffentliches Gut, das nicht durch Ausschließlichkeitskriterien geschützt werden kann. Das grundlegende Prinzip der Informationsfreiheit und des freien Informationsflusses ist eine wesentliche Vorausssetzung für ein freies wirtschaftliches und politisches System.

Außerdem betrifft der Schutz von Information nicht nur die wirtschaftlichen Interessen ihres Besitzers, sondern auch die Interessen derjenigen, die von ihrem Inhalt betroffen sind. Das bedeutet rechtlich eine neue Anforderung an den Persönlichkeitsrechtsschutz im IT-Bereich.

Zum dritten gewinnen die Zugangsrechte zu Informationen für den privaten und den öffentlichen Bereich an Bedeutung (Access to Information Rights), zum Beispiel bezüglich des Datenschutzrechtes und für Strafverfolgungsbehörden. Aus diesen Unterschieden ergibt sich, dass Rechtsregeln für Informationen nicht auf dem Wege einer Analogie aus Vorschriften über materielle Gegenstände entwickelt werden können, sondern einer eigenständigen Grundlage und Theorie bedürfen.

Die Entwicklung der Technikgesellschaft und des Technikrechts in der postindustriellen Informationsgesellschaft wird auch unter dem Stichwort »Risikogesellschaft« diskutiert. Damit sind insbesondere die Technikgefahren der Chemie, der Kernenergie, der Gentechnik und anderer Anlagen mit schädlichem Einwirkungspotential auf den Menschen und die Umwelt gemeint. Bei Betrachtung der neuen Risiken muss berücksichtigt werden, dass sie oft vergesellschaftet sind und nicht mehr auf einen Urheber zurückgeführt werden können, vor allem aber, dass sie schwerwiegende Folgen haben können, die nach Ort, Zeit und Kreis der Betroffenen nicht eingrenzbar sind. Gleichzeitig werden Komplexität und Entwicklungsgeschwindigkeit der gesellschaftlichen und technischen Veränderungen immer größer.

Rechtlich ergibt sich aus der Betrachtung der Risiken die Forderung nach einer besseren gesellschaftlichen Kriminalitätsprophylaxe, von der die Informationstechnik als Teil der Risikogesellschaft ebenfalls betroffen ist. Zur Bekämpfung der Computerkriminalität sind vor allem außerstrafrechtliche Maßnahmen gefordert: technische Sicherheitsstandards mit Zugriffskontrollsystemen, Aufklärung der betroffenen Benutzer und geeignete zivilrechtliche und öffentlich-rechtliche Rahmenbedingungen. Das Strafrecht muss an die neuen Risiken angepasst werden. Eine Voraussetzung für rechtliche Regelungen in diesem Bereich ist ein strukturelles Denken: Statt bei zufälligen technischen Veränderungen anzusetzen, müssen Funktionen beschrieben werden, die auch in Zukunft der veränderten Technik standhalten können.

Das bedeutet vor allem, dass nationale Grenzen ihre Bedeutung verlieren und eine internationale Harmonisierung des Rechts stattfinden muss. Bei der Nutzung internationaler Telekommunikationsnetze wie dem Internet können Daten in Sekundenbruchteilen über internationale Netze übertragen werden, ohne dass eine Kontrolle möglich ist. Mit Hilfe von Rechnersystemen können Straftaten begangen werden, deren Konsequenzen im Ausland eintreten.

Unterschiedliche nationale Gesetze würden dagegen zu »Data Havens« oder »Computer Crime Havens« führen, die nationale Beschränkungen des freien Informationsflusses zur Folge hätten. Zudem wären nationale Barrieren wirkungslos, da Informationen über internationale Netze auch in verschlüsselter Form ins Ausland übertragen werden können. Nationale Beschränkungen und Überwachungsmaßnahmen würden Persönlichkeitsrechte der Bürger und Geschäftsgeheimnisse von Organisationen gefährden sowie die wirtschaftliche Entwicklung eines internationalen Informationsmarktes behindern. Daher ist die internationale Harmonisierung des Informationsrechts durch EU, Europarat, OECD, UN, WIPO, TWTO und AIDP zu begrüßen, wenngleich noch eine Verstärkung von Kontakten und verbesserte Zusammenarbeit zwischen den einzelnen Staaten erforderlich ist.

1997 haben die Justiz- und Innenminister der G-8-Länder einen Plan ausgearbeitet, um mit internationaler Kooperation die wachsende IT-Kriminalität zu bekämpfen. US-Generalstaatsanwältin Janet Reno äußerte, Informations-technologie habe eine neue grenzüberschreitende »Frontier« der Kriminalität eröffnet. Nötig sei, den Cyberkriminellen nicht länger hinterherzuhinken, sondern ihnen einen Schritt voraus zu sein. Der Plan sieht unter anderem vor, dass in jedem Land eine ausreichende Zahl von Spezialisten zur Bekämpfung der IT-Kriminalität angestellt werden, dass die Staaten enger zusammenarbeiten und Täter, beispielsweise bei Angriffen auf Netzwerke, schnelle identifiziert werden sollen, dass ein Straftäter auch in dem Land zur Rechenschaft gezogen werden kann, in das er geflohen ist, wenn eine Auslieferung nicht möglich ist, und dass entsprechende Gesetze für eine leichtere Strafverfolgung geschaffen werden müssen.

Ende Januar 2001 legte die Europäische Kommission einen Forderungskatalog zur Bekämpfung der Computerkriminalität vor. Die FAZ berichtete am 31.1.2001 in dem Beitrag »Programm gegen Computerkriminalität – Brüssel im Zwiespalt zwischen Sicherheit und Grundrechtssicherung«:

»Die Europäische Kommission hat am Dienstag einen Forderungskatalog zur Bekämpfung der Computerkriminalität vorgelegt. Zur Vorbeugung und zur Bekämpfung müsse die Sicherheit der Informationsinfrastruktur verstärkt und dafür Sorge getragen werden, daß die Behörden in der Europäischen Union über geeignete Mittel verfügten. Dabei müßten aber die Grundrechte der Bürger gewahrt bleiben, heißt es.

Ein auch von den Regierungen der EU-Mitgliedstaaten gefordertes, abgestimmtes Handeln sei notwendig, weil man mit Hilfe der Computersysteme jederzeit von jedem Ort der

Welt aus illegale Handlungen begehen könne, heißt es in der Kommissionsmitteilung. Die Zahl der aufgedeckten und gemeldeten Übergriffe verschleiert nach Ansicht der Kommission das wahre Ausmaß des wachsenden Problems.

Nach den ersten, vor rund drei Jahren eingeleiteten Vorhaben zur Bekämpfung des wachsenden Mißbrauchs der neuen Informations- und Kommunikationstechniken fordert die Kommission jetzt weitere Schritte, zum Beispiel die zügige Verabschiedung eines gemeinschaftlichen Rechtsinstruments. Dies soll den EU-Mitgliedstaaten erlauben, mit wirksamen Sanktionen beispielsweise gegen Kinderpornographie vorzugehen. Längerfristig will die Kommission Gesetzesvorschläge zur weiteren Angleichung der materiellen Strafrechtsvorschriften auf dem Feld der sogenannten High-Tech-Kriminalität vorlegen, heißt es in der Mitteilung. Die Erklärung der »Cyberkriminalität« zur Straftat böte einen besseren Opferschutz und erleichtere die grenzüberschreitende Zusammenarbeit der Behörden. Mit der von der Kommission empfohlenen Angleichung des Rechts auf europäischer Ebene fiele die Computerkriminalität unter das Gemeinschaftsrecht. Damit würden gemeinschaftliche Zwangsmaßnahmen möglich, heißt es in der Mitteilung. Die E-Partner sollten sich auf eine wirkungsvollere Politik zur Bekämpfung der Computerkriminalität verständigen. Damit will sich die Gemeinschaft mit ihren Plänen positiv von einem geplanten Abkommen des Europarates abheben, das lediglich Mindestvorschriften enthalten soll.

Die Kommission will darauf hinwirken, daß auf nationaler Ebene in allen EU-Ländern spezialisierte Polizeidienste eingerichtet werden. In diesem Zusammenhang will sie auch europäische Schulungsprogramme für Mitarbeiter der Strafverfolgungsbehörden und Veranstaltungen zum Thema Informationssicherheit fördern. Zur Stärkung der Zusammenarbeit will die Kommission sämtliche mit dem Thema befaßten Stellen in einem »EU-Forum« zusammenführen. Am 7. März 2001 findet in Brüssel eine öffentliche Anhörung dazu statt.«

B.4 Zusammenfassung

Das Zusammenwachsen von Datenverarbeitungs- und Datenübertragungstechnik hat die Computerkriminalität vielfältiger und gefährlicher gemacht. Die Möglichkeiten und Gefahren, die sich schon heute und in Zukunft verstärkt im Internet ergeben, sind derzeit kaum abzuschätzen. Zentralen Einfluss auf die Zukunft haben aus rechtlicher Sicht vor allem drei grundsätzliche soziale Veränderungen in unserer Gesellschaft: Die Entstehung der Informationsgesellschaft mit ihren neuen strafrechtlichen Rechtsgütern, die Veränderung der Risikogesellschaft, in der außerstrafrechtlichen Maßnahmen größere Bedeutung zukommt als strafrechtlichen und strafprozessualen Maßnahmen, und das Zusammenwachsen der Bürger in einer Informationsgesellschaft, in der sich die neuen Herausforderungen nur durch gemeinsame internationale Anstrengungen bewältigen lassen.

Anhang C

TCP/IP-Technologie für Internet und Intranet

Der Begriff Internet, das »Netz der Netze«, verkörpert eine einzigartige, weltumspannende Infrastruktur vernetzter Netzwerke und die Software-Technologien, auf denen diese Netzwerke aufbauen. Die TCP/IP-Technologie (Transmission Control Protocol/Internet Protocol) ist das eigentliche Herz des Internet. Erst die hohe Verbreitung der TCP/IP-Protokolle ermöglichte die weltweite Vernetzung der Rechnersysteme bis hin zum »kleinsten« PC im letzten Winkel dieser Erde /Hamp96/.

Die TCP/IP-Technologie ist kein feststehendes Gebilde, sondern besteht aus unterschiedlichen Diensten und Anwendungen, die im Laufe der Jahre ständig weiterentwickelt wurden. TCP- und IP-Protokoll sind streng genommen nur zwei Komponenten der gesamten Kommunikations-Architektur, haben sich aber als übergeordneter Begriff im Sprachgebrauch durchgesetzt.

C.1 Von den Anfängen bis heute

Ursprünglich hatte das Internet, wie viele Produkte der Hochtechnologie, militärische Zielsetzungen. Die ersten Gedanken machte man sich bereits Ende der fünfziger Jahre, als die amerikanische *»RAND Corp.«* ein Konzept für ein Kommando- und Überwachungsnetzwerk militärischer Einrichtungen entwickelte. Der Kern dieses Konzepts bestand aus einem dezentralen Aufbau, der auch nach teilweiser Zerstörung der Infrastruktur, beispielsweise nach einem Atomschlag, die Funktionsfähigkeit der amerikanischen Militäreinrichtungen gewährleisteten sollte.

Um im technologischen Wettstreit mit der Sowjetunion die amerikanische Militärtechnologie in eine führende Position zu bringen, rief die US-Regierung unter anderem die *»Advanced Research Projects Agency«* (ARPA) ins Leben. Deren Aufgabe war es, neue Technologien zu entwikkeln. Aus den ursprünglichen Konzepten der *»RAND Corp.«* entwickelten die ARPA-Ingenieure die paketorientierte Datenübertragung, die die Datenkommunikation in den folgenden Jahren revolutionieren sollte. Ende 1969 wurde zwischen der *»University of California at Los Angeles«*, der *»University of California at Santa Barbara«*, der *»University of Utah«* und dem *»Stanford Research Institute«* (SRI) in Menlo-Park in Kalifornien das erste experimentelle Netz (ARPANET) in Betrieb genommen. Für den Erfolg des ARPA-

NET sorgten vor allem die auf allen angeschlossenen Rechnern zur Verfügung gestellten Dienstleistungen wie Terminalsitzung (Remote Login), Dateiübertragung (File Transfer) und Elektronische Post (Electronic Mail).

Im Jahr 1973 begann die inzwischen in *»Defense Advanced Research Projects Agency«* (DARPA) umbenannte Organisation ein weiteres Projekt, um die zwischenzeitlich neben dem ARPANET entstandenen, unterschiedlichen Übertragungsmechanismen zu verbinden. So entstand auf der Basis des TCP/IP-Konzepts das Internet. Die Grundzüge dieser Technologie wurden 1974 von *Victor Cerf* (Stanford University) und *Bob Kahn* (DARPA) erstmals in einem veröffentlichten Artikel festgelegt. Ein erstes Testnetz wurde 1977 in Betrieb genommen und in den kommenden Jahren ständig erweitert. 1983 hatte das immer noch experimentelle ARPANET eine derartige Ausdehnung erreicht, dass man beschloss, die Kontrolle über dieses Netz an die *»Defense Communication Agency«* (DCA) abzugeben. Gleichzeitig wurden sämtliche Netzknoten auf das TCP/IP-Protokoll umgestellt und das bisherige Netz in einen militärischen Bereich (MILNET) und einen forschungsorientierten Bereich (ARPANET) aufgeteilt.

In den letzten Jahren hat sich das Internet sehr stark gewandelt. Die Fortschritte der Kommunikationstechnologie und das stetig wachsende Informationsbedürfnis haben das Internet explosionsartig anwachsen lassen. Waren früher fast ausschließlich Universitäten, Forschungsinstitute und deren Wissenschaftler ans Internet angeschlossen, so ist es heute zu einem Informationsforum für die breite Öffentlichkeit geworden. Ende 2001 waren schätzungsweise 500 Millionen Benutzer in über 240 Ländern an das Internet angeschlossen.

Als Anfang der neunziger Jahre das World Wide Web (WWW) eingeführt wurde, bot sich erstmals die Möglichkeit, unter einer einheitlichen Darstellung unterschiedliche Dienste mit multimedialen Inhalten, beispielsweise Bildern, Tönen, Animationen und Videos, zu transportieren. Einige Strategen erkannten das Potential dieses Mediums, und innerhalb weniger Jahre wurde das World Wide Web zu einem globalen Marktplatz, auf dem fast alle großen, aber auch immer mehr mittlere und kleine Organisationen vertreten sind. Die meisten Internet-Provider stellen für ihre Kunden heute, bis zu einem gewissen Umfang kostenlos, Platz auf ihren Servern zur Verfügung. Damit bietet sich für jeden privaten Anwender die Möglichkeit, auf einer eigenen Homepage sich selbst, seine Hobbies, Interessen und Neigungen weltweit zu präsentieren und Kontakt mit Gleichgesinnten aufzunehmen.

Die elektronische Post (E-Mail) ist heute im geschäftlichen und privaten Umgang ein fester Bestandteil unserer täglichen Kommunikation geworden. Die meisten Mitarbeiter in Firmen und Behörden sind heute per E-Mail zu erreichen und auf Visitenkarten ist die Angabe einer E-Mail-Adresse mittlerweile obligatorisch.

Die rasante Entwicklung des Internet hat aber auch Schattenseiten: Die TCP/IP-Technologie war nicht für ein solches globales Netz vorgesehen. Durch die in den Anfangsjahren auf wenige Teilnehmer begrenzte Ausdehnung des Internet waren Sicherheitskonzepte wie Zugriffsberechtigung, Vertraulichkeit der Daten während der Übertragung und Schutz von Netzsegmenten vor unberechtigten Zugriffen nicht in solchem Maße erforderlich wie heute. Da sich inzwischen jeder von fast jedem Ort auf der Welt in das Internet einschalten kann, sind damit natürlich auch Sicherheitsmaßnahmen unumgänglich geworden.

C.2 Vorteile der TCP/IP-Technologie

Die TCP/IP-Technologie bietet entscheidende Vorteile:

- Für jeden Benutzer besteht die Möglichkeit, auf jede für ihn freigegebene Information innerhalb des gesamten Netzwerks zugreifen zu können. Zusätzlich kann jeder angeschlossene Benutzer mit jedem anderen angeschlossenen Rechnersystem kommunizieren. Es gibt bereits Anwendungen, die weltweites Telefonieren oder Videokonferenzen von einem Rechnersystem zum nächsten ermöglichen. Dadurch wird der Informationsaustausch zwischen den Benutzern gewährleistet, der das Internet in Zukunft zum globalen Informationsmedium schlechthin machen wird.
- Bereits bei der Konzeption Anfang der siebziger Jahre legte man fest, dass die Protokolle unabhängig von der verwendeten Netzwerktechnologie sein sollten. Durch diese Forderung ist die Kommunikation zwischen unterschiedlichen Rechner- und Netzwerktypen, wie z. B. im Internet, möglich geworden. Gleichzeitig bietet dies die Möglichkeit, neue technologische Entwicklungen mit bereits vorhandenen Strukturen zu verknüpfen. Durch die permanente Weiterentwicklung der Technik im Computer- und Kommunikationsbereich lässt sich die bewährte Technologie ohne weiteres auf neue Entwicklungen übertragen, ist dann aber immer noch in der Lage, mit älteren Systemen zu kommunizieren.
- Durch die ständige Weiterentwicklung ist das Internet zu einer ausgereiften Technologie geworden, die sich im alltäglichen Einsatz bewährt hat.
- Die Internet-Technologie ist heute weit verbreitet, daher gibt es auch ein breites Angebot kompatibler Netzkomponenten. Da die meisten Softwarevarianten auch durch Implementierungen anderer Hersteller ersetzbar sind, bedeutet das eine geringe Herstellerabhängigkeit. Durch die starke Verbreitung innerhalb des Internet werden die Produkte auch zunehmend billiger.
- Die einzelnen Protokollspezifikationen sind standardisiert und für jedermann frei zugänglich. Dadurch sind Implementierungen für neue oder spezielle Systeme jederzeit leicht zu entwickeln oder anzupassen.

C.3 Das OSI-Referenzmodell

Um eine einheitliche Struktur für gegenwärtige und zukünftige Entwicklungen von Netzwerktechnologien festzulegen, einigte man sich auf das so genannte OSI-Referenzmodell (Open System Interconnection), das 1983 von der »International Organisation for Standardization« (ISO) als Standard festgelegt wurde. Es hat eine klare Architektur und eignet sich daher besonders gut für die Darstellung einer Kommunikationsarchitektur und der Prinzipien des Schichtenmodells. In diesem Modell wird davon ausgegangen, dass ein Kommunikationsprotokoll aus mehreren Modulen besteht, von denen jedes einzelne Modul während einer Kommunikation unterschiedliche Aufgaben zu erfüllen hat /Tann 98/.

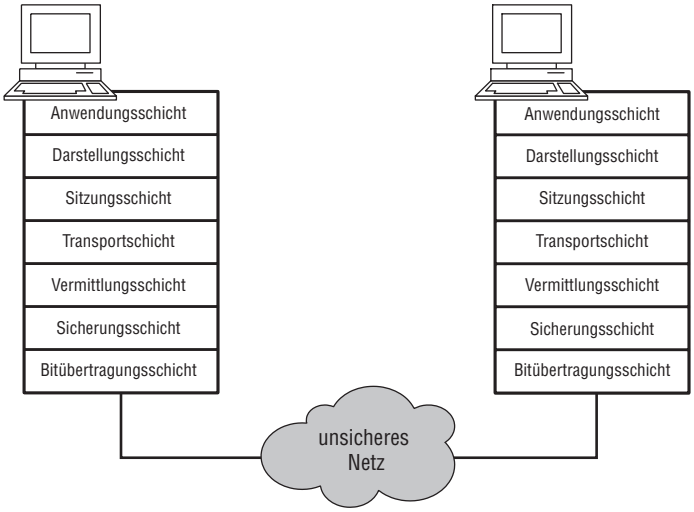


Abb. C.1: Das OSI-Referenzmodell

Das OSI-Referenzmodell besagt, dass bei einer Verbindung beispielsweise zwischen zwei Rechnersystemen jede Schicht des Rechnersystems A mit der gleichen Schicht des Rechnersystems B kommunizieren kann. Dazu werden den Daten in jeder Schicht bestimmte Bitmuster in einem Header vorangestellt oder in einem Trailer am Ende angefügt. Diese Bitmuster enthalten so genannte Protokollinformationen, die zum Beispiel darüber Auskunft geben,

- wer die Daten abgesandt hat,
- wer die Daten empfangen soll,
- welchen Weg die Daten während der Übertragung nehmen sollen,
- wie die Daten weiterverarbeitet werden dürfen oder
- wie sie vom Empfänger behandelt werden sollen.

Jede weitere Schicht übernimmt die Datenpakete der übergeordneten Schicht und fügt, falls dies für den Ablauf der Kommunikation notwendig sein sollte, ihre eigenen Protokollinformationen in einem weiteren Header oder Trailer hinzu. Die Auswertung der Protokolldaten erfolgt beim Empfänger nur auf der jeweils gleichen Schicht, das heißt die Daten einer übergeordneten Schicht werden von einer niedrigeren Schicht nicht ausgewertet.

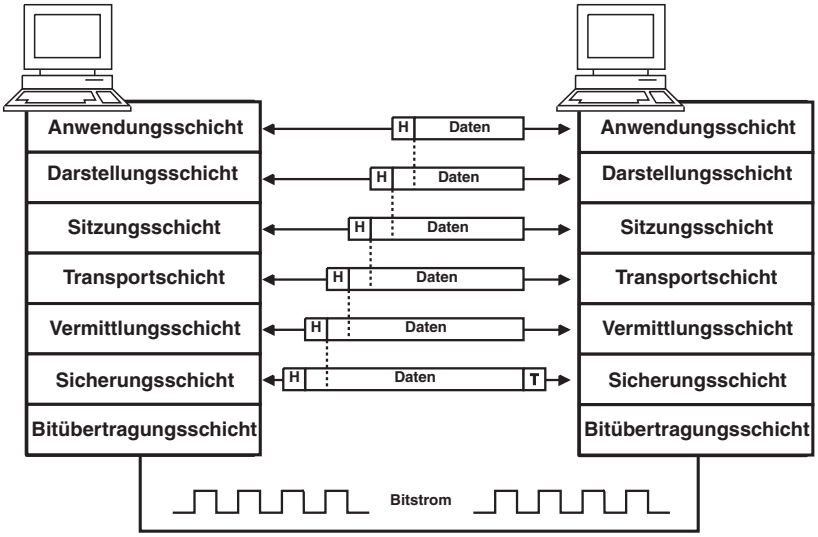


Abb. C.2: Kommunikation zwischen zwei Rechnern

Im folgenden Abschnitt soll kurz erläutert werden, welche Aufgaben die jeweiligen Schichten übernehmen:

1. Die Bitübertragungsschicht (Physical Layer) legt fest, wie die Daten physikalisch übertragen werden. Zu den Parametern dieser ersten Schicht gehören Informationen über die verwendeten Übertragungsmedien wie Kupferkabel, Glasfaser, Infrarot- oder Funkübertragung, und die Spezifikation von Schnittstellen mit Spannungspegeln, Steckverbindern und Datenübertragungsraten.
2. Die Aufgabe der Sicherungsschicht (Data Link Layer) ist die sichere Datenübertragung zwischen zwei benachbarten Stationen, zum Beispiel zwei Routern, innerhalb eines Netzwerks. Dazu werden die zu übertragenden Bits in Rahmen (Frames) zusammengefasst und mit einer Prüfsumme versehen. Wird ein solcher Rahmen unvollständig übertragen oder zerstört, so fordert der Empfänger nach einem Vergleich der Prüfsumme den entsprechenden Rahmen erneut beim Absender an.

3. Die Vermittlungsschicht (Network Layer) legt die Übertragungswege (Routen) für die Daten zwischen zwei Rechnersystemen fest. Dazu werden Informationen, wie die Übertragungszeit, die Auslastung des Übertragungsweges usw. benutzt, um nach den in Routing-Protokoll festgelegten Regeln eine Verbindung herzustellen. Die innerhalb dieser Schicht transportierten Daten werden in Datenblöcken übertragen, die man als Pakete bezeichnet.
4. Die Transportschicht (Transport Layer) stellt eine Art virtueller Verbindung zwischen den beiden Rechnersystemen bereit. Sie sorgt vor allem für eine Korrektur von Übertragungsfehlern und ist sehr stark von den untergeordneten Schichten abhängig.
5. Die Sitzungsschicht (Session Layer) dient der Verwaltung von Kommunikationsprozessen. Dabei wird die Verbindung mit einem oder mehreren Kommunikationspartnern kontrolliert und gleichzeitig dafür gesorgt, dass die jeweilige Kommunikation synchron abläuft, das heißt, dass bei einem aufgetretenen Fehler die Daten wieder in der richtigen Reihenfolge zusammengefügt werden.
6. In der Darstellungsschicht (Presentation Layer) werden die zu übertragenden Daten in ein einheitliches Format gebracht. Dies ist vor allem bei der Verwendung von unterschiedlichen Zeichensätzen, zum Beispiel ASCII und EBCDIC, notwendig. Zusätzlich können in dieser Schicht weitere Funktionen zur Umwandlung, Verschlüsselung oder Komprimierung der zu übertragenden Daten enthalten sein.
7. Die Anwendungsschicht (Application Layer) beinhaltet schließlich die eigentlichen Anwendungs- und Dienstprogramme für die unterschiedlichen Funktionen, die über die Netzwerkverbindung ausgeführt werden sollen.

C.4 TCP/IP-Protokollarchitektur

Obwohl es keine generelle Vereinbarung über ein spezielles TCP/IP-Schichtenmodell gibt, kann man sagen, dass es aus weniger Schichten aufgebaut ist als das OSI-Referenzmodell. In den folgenden Kapiteln wollen wir uns deshalb auf ein Vier-Ebenen-Modell beziehen.

In diesem Modell gibt es analog zum OSI-Referenzmodell unterschiedliche Kommunikationsebenen, wobei die Daten von der übergeordneten zur nächsttieferen Ebene weitergereicht werden. Jede Kommunikationsebene fügt den Daten eigene Kontrollinformationen hinzu, bis sie über das Netz gesendet werden. Beim Empfänger werden diese Daten dann Ebene für Ebene nach oben weitergeleitet, wobei jede Ebene nur die für sie relevanten Daten auswertet und aus dem Datenpaket entfernt, bevor es an die nächsthöhere Ebene weitergegeben wird.

Abb. C.3: Ebenen der TCP/IP-Protokollarchitektur

- Die Netzzugangsebene ermöglicht einem Rechnersystem, Daten zu einem anderen Rechnersystem innerhalb des direkt angeschlossenen Netzes (zum Beispiel Ethernet) zu übertragen. Dazu sind genaue Kenntnisse des zugrunde liegenden Netzaufbaus nötig. Die Netzzugangsebene umfasst die zwei unteren Ebenen des OSI-Modells und beinhaltet die Kapselung von IP-Paketen in Netzrahmen (Frames) sowie die Zuordnung von IP-Adressen zu physikalischen Netzadressen, beispielsweise MAC-Adressen.
- Die Netzwerkebene definiert den Aufbau von IP-Paketen und bestimmt, auf welchem Weg die Daten durch das Internet übertragen werden (Routing).
- Die Transportebene stellt eine Verbindung zwischen zwei Endpunkten (Rechnersystemen) her. Die wichtigsten Protokolle sind hier TCP und UDP.
- Die Anwendungsebene beinhaltet sämtliche Programme und Dienste, die über die Netzwerkverbindung durchgeführt werden sollen. Dazu gehören Dienste wie Telnet (Login auf einem anderen Rechnersystem), FTP (Datentransfer zwischen zwei Rechnersystemen), SMTP (E-Mail-Funktionen), HTTP (World Wide Web) usw.

C.5 Internet-Adressen

Wie finden die Daten im Internet ihr Ziel? Ganz klar, jedes Rechnersystem im Internet hat eine bestimmte IP-Adresse und einen Namen.

Bei der Entwicklung der Internet-Adressierung legte man nicht nur hohen Wert auf die Identifizierung jedes angeschlossenen Rechnersystems, sondern auch darauf, an welcher Stelle innerhalb eines Netzwerkes es sich befindet und über welche Übertragungswege die Daten ihr Ziel erreichen können. Dazu bekommt jeder Benutzer im weltweiten Netzwerk eine einmalige 32 Bit oder 4 Byte lange Internet-Adresse (IPv4-Adressierung), bestehend aus einer Netzwerk- und einer Rechnersystem-Identifikation, die als 4 Dezimalzahlen dargestellt werden und jeweils durch einen Punkt getrennt sind.

Beispiel: 11000011 . 10010011 . 00111000 . 11101101 entspricht 195 . 147 . 56 . 237

Diese Adressierung wird in 5 Klassen (Klasse A bis E) aufgeteilt. Jede dieser Klassen unterscheidet sich in der Länge der Netzwerk- und der Rechnersystem-Identifikation (Abb. c.4). Diese Aufteilung wurde getroffen, da man in den Anfangstagen des ARPANET davon ausging, dass es in Zukunft nur wenige große (Klasse-A-) Netzwerke (z. B. für Militär und Forschung) geben würde. Doch nach einigen Jahren zeigte sich mit der Einführung von lokalen Netzwerken in vielen Organisationen, dass diese Annahme nicht mehr zutraf. Durch die Vergabe von Klasse-A-Adressen wurden die Möglichkeiten schnell begrenzt. Aus diesem Grund führte man zwei weitere Klassen für mittelgroße (Klasse B) und kleine Netze (Klasse C) ein. Den Klasse-D-Adressen fällt eine besondere Bedeutung zu. Sie werden als so genannte Multicast-Adressen bezeichnet. Das bedeutet, dass bestimmte Datenpakete nicht mehr an jedes Rechnersystem einzeln verschickt werden müssen, sondern gleichzeitig an eine ganze Gruppe von Rechnersystemen gesendet werden können, denen eine Multicast-IP-Adresse zugeordnet wurde. Die IP-Adressen der Klasse E sind für zukünftige Anwendungen reserviert und werden derzeit zu Forschungszwecken verwendet. Sie sollen genutzt werden, um IPv6-Pakete über IPv4-Netze zu routen.

Das starke Wachstum des Internet hat zu einem Mangel an IP-Adressen geführt. Außerdem sind dadurch die Routing-Tabellen der Backbone-Router, die die einzelnen Netze verbinden, zu groß geworden. Aus diesem Grund hat man die starre Aufteilung in nur 5 Netzklassen aufgehoben (vgl. RFC 1517). Die 32 Bit der IP-Adresse können nun beliebig auf Netz-ID und Rechnersystem-ID verteilt werden. Somit ergeben sich 33 mögliche Netzwerk-Klassen. Für die ursprünglichen fünf Klassen, die immer noch am häufigsten vorkommen, werden die alten Bezeichnungen (Klasse A bis E) weiterverwendet.

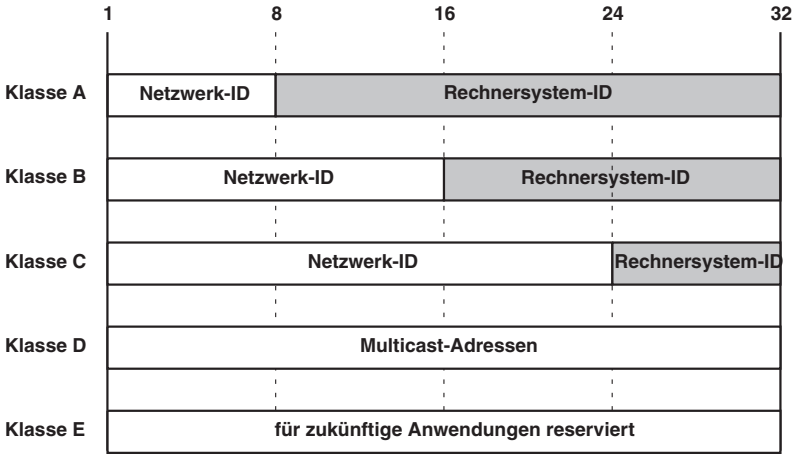


Abb. C.4: Aufbau von Internetadressen und Einteilung in Klassen

Viele Anwender sind nur gelegentlich über einen Provider mit dem Internet verbunden. Für diese Rechnersysteme ist es nicht notwendig, eine permanente IP-Adresse zu vergeben. Hier benutzt man die Möglichkeit, IP-Adressen automatisch zu vergeben. Wenn ein Kunde Zugang zum Internet haben möchte, wählt er zunächst einen Einwahlknoten eines Providers in seiner Nähe an. Das Rechnersystem des Providers hat zu diesem Zweck eine Reihe von IP-Adressen reserviert, die dem jeweiligen Anrufer dann automatisch zugeordnet werden und nur für die aktuelle Sitzung gültig sind. Dieses Verfahren nennt man »dynamische IP-Adressierung«.

Da aufgrund des starken Wachstums des Internet abzusehen war, dass die Anzahl der freien IP-Adressen eines Tages erschöpft sein wird, wird seit 1995 daran gearbeitet, die Adresslänge zukünftig auf 128 Bit oder 16 Byte (IPv6 oder IPnG next generation) zu verlängern. Natürlich sind die alten IP-Adressen weiterhin gültig und können auch nach dem neuen Standard weiterhin verarbeitet werden. Es muss damit gerechnet werden, dass der fließende Übergang zwischen IPv4 und IPv6 noch sehr lange dauern wird.

Unternehmen verwenden heute meistens nur noch wenige offizielle IP-Adressen, sondern arbeiten mit verborgenen, intern reservierten IP-Adressen, was die Adressenproblematik stark reduziert.

Die IP-Adressierung ist für technische Systeme hervorragend geeignet. Im praktischen Umgang hat sich aber gezeigt, dass dieses Verfahren für viele Anwender zu kompliziert und undurchsichtig ist. Wer schon einmal durch das World Wide Web gesurft ist, dem ist sicherlich aufgefallen, dass viele Rechnersysteme nicht über ihre IP-Adressen aufgerufen werden, sondern über einen oder mehrere symbolische Namen.

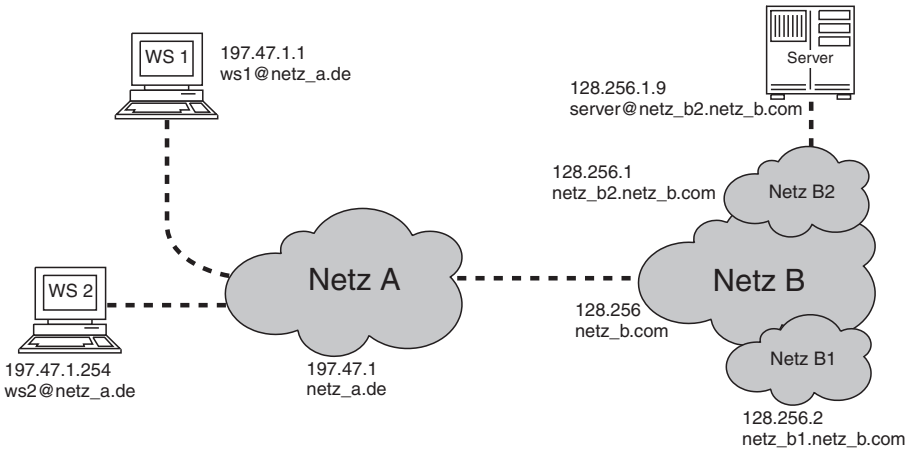


Abb. C.5: IP- und Domainnamenadressierung

Jedes ans Internet angeschlossene Netz kann zu diesem Zweck neben einem IP-Adressbereich zusätzlich einen Domainnamen erhalten. IP-Netze und DNS-Domains müssen nicht deckungsgleich sein, auch wenn dies meistens der Fall ist. Innerhalb der Domain kann der jeweilige Netzbetreiber für untergeordnete Netze weitere Subdomains erstellen, um sein Netz noch tiefer zu strukturieren. Die Domainnamen werden zentral vom Network Information Center (NIC) und seinen Unterorganisationen (zum Beispiel DENIC in Deutschland) vergeben und verwaltet. Wenn eine Organisation einen eigenen Domainnamen verwenden möchte, so muss sie oder ihr Provider bei der verantwortlichen Unterorganisation des NIC die Zuordnung dieses Namens beantragen. Die Top Level Domains sind vom Network Information Center fest vorgegeben und in unterschiedliche Nutzerprofile oder lokale Gruppen eingeteilt:

- .arpa für Einrichtungen des ARPANET
- .com für kommerzielle Organisationen aus Industrie und Handel
- .edu für Universitäten und Schulen
- .gov für Regierungsstellen und staatliche Einrichtungen
- .mil für militärische Einrichtungen der US-Streitkräfte
- .org für nicht kommerzielle Einrichtungen
- .de für Einrichtungen in Deutschland
- .uk für Einrichtungen in Großbritannien

Neue, so genannte generic Top Level Domains (gTLD), sind in Vorbereitung:

- .aero für Unternehmen der Luftfahrtindustrie
- .biz für Unternehmen
- .coop für genossenschaftliche Organisationen
- .info für allgemeine WWW-Angebote

- .museum für Museen
- .name für Privatpersonen
- .profür Ärzte, Anwälte, Steuerberater etc.

Die Vorschläge ».firm«, ».shop« und ».web« wurden verworfen.

Ausführlichere Informationen dazu und eine Sammlung von Links, mit deren Hilfe Sie die Entwicklung verfolgen können, finden Sie unter `http://www.denic.de/doc/gtld/index.html`.

C.6 Die Kommunikationsprotokolle

Die folgenden Beschreibungen der am häufigsten im Internet verwendeten Kommunikationsprotokolle und Dienste sollen als Hinweis dienen, welche Informationen jeweils übertragen werden. Diese Informationen sind äußerst wichtig für den Transport der Daten innerhalb und zwischen den Netzen. Gleichzeitig können die übertragenen Daten aber auch manipuliert werden und bei falschem Umgang enormen Schaden beim Empfänger verursachen.

Grundsätzlich unterscheidet man zwei verschiedene Arten von Kommunikationsprotokollen. Die verbindungslosen Protokolle kann man mit Telegrammen vergleichen. Die Daten werden vom Absender ins Netz geschickt und können während der Übertragung verloren gehen, dupliziert werden oder verspätet eintreffen, ohne den Absender darüber zu informieren. Man nennt derartige Informationseinheiten auch Datagramme. Diese Art der Kommunikation ist wie der Paketdienst einer Post-Gesellschaft. Man gibt das Paket an einer Stelle ab; wie es dann weitergeleitet wird, darauf hat man keinen Einfluss.

Im Gegensatz dazu bauen die verbindungsorientierten Protokolle eine Kommunikation nach einem bestimmten Schema auf. Zuerst wird eine virtuelle Verbindung zwischen Absender und Empfänger aufgebaut. Nach dem gegenseitigen Austausch von festgelegten Informationen erfolgt dann der eigentliche Datentransfer, und erst wenn beide Seiten den ordnungsgemäßen Empfang der Daten bestätigt haben, wird die Verbindung wieder abgebaut. Eine Analogie hierzu ist eine Telefonverbindung: Ein Teilnehmer baut die Verbindung auf, und wenn der andere abgenommen hat, kann das Telefonat beginnen.

C.6.1 IP-Protokoll

Das Internet Protocol (IP) ist ein verbindungsloses Protokoll auf der Netzwerkebene. Ein IP-Header besteht aus mehreren Feldern, die folgende Bedeutungen oder Funktionen haben:

- Version: Versionsnummer des verwendeten IP-Protokolls, mit dem das IP-Paket (Datagramm) erstellt wurde.

- Headerlänge: Dieses Feld bestimmt die Länge des IP-Headers in 32-Bit-Einheiten.
- Servicetyp: Man kann die Wichtigkeit eines IP-Paketes mit diesem Feld festlegen und bestimmen, auf welche Art oder welchem Weg dieses IP-Paket übertragen werden soll, zum Beispiel mit geringer Verzögerung, mit hohem Datendurchsatz oder auf einer sicheren Route.
- Gesamtlänge: Die Länge des gesamten IP-Pakets in Bytes.
- Identifikation: Während der Übertragung kann ein IP-Paket in mehrere Fragmente aufgeteilt werden. Dabei wird jedes IP-Paket mit einer Identifikation versehen. Anhand dieser Identifikation und der Quell-Adresse kann ein fragmentiertes IP-Paket beim Ziel-Rechnersystem wieder zusammengefügt werden.
- Flags: Das erste Bit legt fest, ob ein IP-Paket während der Übertragung fragmentiert werden darf. Das zweite Bit ist bei der Zusammensetzung einer fragmentierten Nachricht von Bedeutung. Es bestimmt, ob die enthaltenen Daten aus der Mitte oder vom Ende der ursprünglichen Nachricht stammen.
- Fragment-Offset: Wenn eine Nachricht in mehrere Fragmente zerlegt wird, werden diese Fragmente der Reihe nach durchnummeriert und dann abgeschickt. Da die einzelnen IP-Pakete innerhalb des Netzwerks unterschiedliche Wege nehmen können, treffen die IP-Pakete beim Ziel-Rechnersystem nicht immer in der richtigen Reihenfolge ein. Dieser kann die Teile einer Nachricht erst dann wieder zu einer vollständigen Nachricht zusammensetzen, wenn er sämtliche Teile erhalten hat.
- Time to Live (TTL): Wenn ein IP-Paket vom Quell-Rechnersystem ins Netz geschickt wird, muss das Ziel-Rechnersystem nicht unbedingt erreichbar sein. In einem derartigen Fall würde das IP-Paket solange im Netz kursieren, bis das Ziel-Rechnersystem irgendwann bereit ist, das IP-Paket zu empfangen. Damit dies nicht passiert, wird vom Quell-Rechnersystem für jedes IP-Paket eine Lebensdauer in Sekunden festgelegt. Jedesmal, wenn das IP-Paket von einer Zwischenstation, zum Beispiel einem Router oder einem Netzknoten, weitergeleitet wird, wird der Wert dieses Feldes herabgesetzt. Hat das Feld den Wert Null erreicht, wird das IP-Paket gelöscht beziehungsweise nicht mehr weitergeleitet.
- Protokoll: In diesem Feld wird protokolliert, welche weiteren Protokolle in das IP-Paket eingebettet sind, beispielsweise TCP, UDP, ICMP, usw.
- Header-Prüfsumme: Um die Unversehrtheit eines Headers zu gewährleisten, wird aus den vorhandenen Feldern eine Prüfsumme errechnet und vom Quell-Rechnersystem in dieses Feld eingetragen. Wenn das IP-Paket weitergeleitet wird oder beim Ziel-Rechnersystem angekommen ist, wird die Prüfsumme neu berechnet und mit dem eingetragenen Wert verglichen.
- Quell-Adresse: Dieses Feld enthält die IP-Adresse des Quell-Rechnersystems (Absender).
- Ziel-Adresse: Dieses Feld enthält die IP-Adresse des Ziel-Rechnersystems (Empfänger).

- IP-Optionen: Dieses Feld dient hauptsächlich dem Testen von Netzwerken und der Fehlersuche. Hier können bestimmte Optionen festgelegt werden, die unter anderem Einschränkungen oder Informationen zur Weiterleitung der Daten enthalten. So können hier etwa Informationen für das Source Routing eingefügt werden, das heißt jede Zwischenstation einer Verbindung wird vor der Übertragung genau festgelegt.

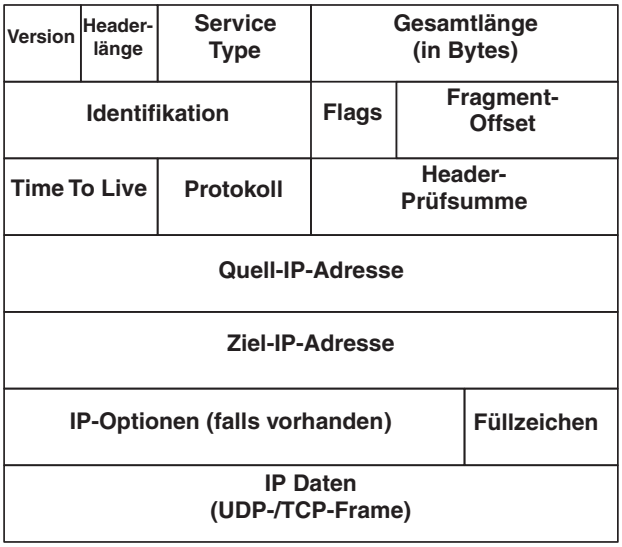


Abb. C.6: Header eines IP-Datenpaketes

C.6.2 Routing Protokolle

In einem komplexen Netzwerk wie dem Internet gibt es viele verschiedene Möglichkeiten, wie Daten von der Quelle an ihr Ziel gelangen. Den Prozess, bei dem die Verbindungswege innerhalb der Netze festgelegt werden, nennt man Routing.

Zu diesem Zweck gibt es an der Verbindungsstelle von zwei oder mehreren Netzen spezielle Rechnersysteme (Router oder Gateways), die nach festgelegten Regeln bestimmen können, welchen Weg die Daten nehmen sollen. Jeder Router benutzt zur Festlegung der Wege eigene Routingtabellen.

Darin sind alle direkt angeschlossenen Rechnersysteme und die Verbindungsstellen zu benachbarten Netzen enthalten. Diese Tabellen können sich in Abhängigkeit von verschiedenen Faktoren wie zum Beispiel der Netzauslastung oder der Verfügbarkeit bestimmter Rechnersysteme oder Netze jederzeit ändern. Dieses Verfahren nennt man dynamisches Routen.

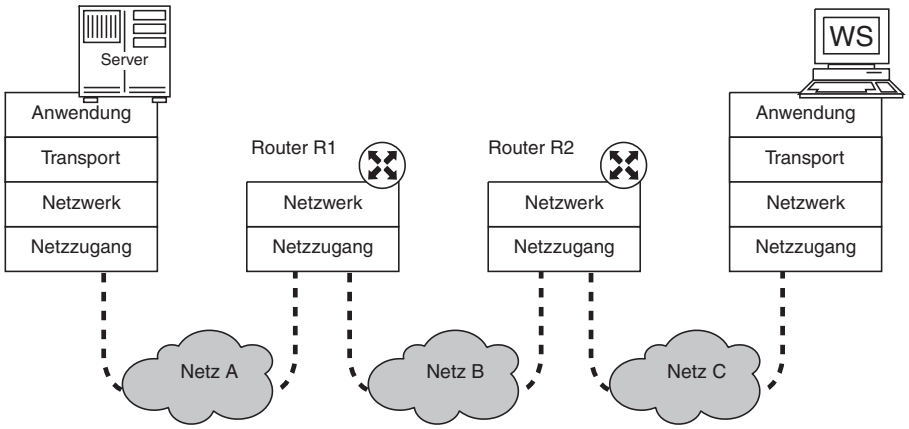


Abb. C.7: Routing über verschiedene Netze

Routing Protokolle wie RIP (Routing Information Protocol) oder OSPF (Open Shortest Path First) dienen dazu, diese Veränderungen der Routen an die beteiligten Systeme weiterzuleiten. Ein Angreifer hat die Möglichkeit, falsche RIP-Informationen zu erzeugen und dadurch unerwünschte Routen beziehungsweise Zwischenstationen einzufügen. Eine dieser Zwischenstationen kann es ihm dann ermöglichen, die Informationen abzuhören oder zu manipulieren. /Boro92/

Als wesentlich sicherer hat sich dagegen die Methode des statischen Routings erwiesen. Bei diesem Verfahren wird nicht jedem einzelnen Router die Entscheidung überlassen, welchen Weg die Daten zu nehmen haben, sondern der Übertragungsweg wird vorher detailliert festgelegt und in die Datenpakete mit eingefügt. Das statische Routing ist wegen der Dynamik im Internet nicht möglich. Im Intranet kann es eine höhere Sicherheit gewährleisten.

Im Gegensatz zu Rechnersystemen, in denen die Daten alle Protokollebenen durchlaufen, werden die Daten bei Routern nur bis zur Netzwerkebene weitergereicht.

C.6.3 ICMP

In einem verbindungslosen Protokoll besteht keine Möglichkeit, den Absender zu informieren, ob das Datenpaket die vorgesehene Lebensdauer (Time To Live) überschritten hat, der Empfänger nicht erreichbar ist oder die Daten unterwegs verloren oder zerstört wurden. Dennoch braucht man eine Möglichkeit, derartige Informationen zwischen Rechnersystemen auszutauschen. Aus diesem Grund wurde das Internet Control Message Protocol (ICMP) in das IP-Protokoll integriert, das ein unverzichtbarer Bestandteil der Internet-Protokolle ist und in keiner Internet-Anwendung fehlen darf.

Router oder Rechnersysteme werten diese Nachrichten meist automatisch aus und veranlassen bestimmte Aktionen oder Umkonfigurationen. Ein Angreifer wird so in die Lage versetzt, durch Absenden falscher ICMP-Informationen Einfluss auf das System zu nehmen und bestimmte Reaktionen zu erzeugen, die es ihm später ermöglichen, die Funktionsfähigkeit zu beeinträchtigen oder ins System einzubrechen.

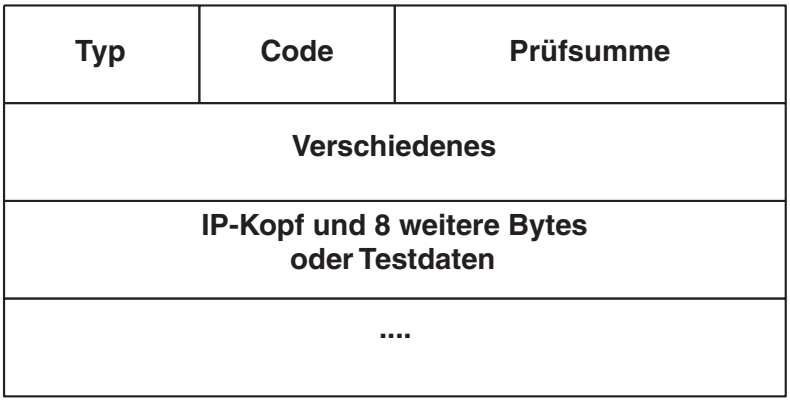


Abb. C.8: Header eines ICMP-Datenpaketes

Das ICMP-Datenpaket enthält Fehler- und Diagnoseinformationen. Es wird intern vom IP angestoßen und verarbeitet. Obwohl die ICMP-Nachrichten in ein IP-Datenpaket gekapselt werden, bilden sie kein höheres Protokoll, wie zum Beispiel TCP oder UDP, sondern sind ein direkter Bestandteil des IP-Protokolls. Das IP-Protokoll kann in der Praxis nicht ohne das ICMP-Protokoll verwendet werden.

ICMP-Nachrichten werden nur von dem Rechnersystem abgesendet, das den Fehler versendet oder ausgelöst hat, und direkt an den ursprünglichen Absender der Daten zurückgeschickt.

Man unterscheidet verschiedene Typen von ICMP-Nachrichten. Diese werden durch eine Ziffer im Header eines ICMP-Paketes (Typ) gekennzeichnet und können je nach ICMP-Datentyp unterschiedliche Daten enthalten. Die wichtigsten sind:

- Echo Reply (0): Diese Nachricht wird ausgelöst, sobald eine EchoRequest-Nachricht von einem anderen Rechnersystem empfangen wurde. Im Datenfeld dieses Paketes werden Testdaten versendet, die unter anderem Aufschluss über Betriebsbereitschaft, Laufzeit usw. geben.
- Destination Unreachable (3): Wenn eine Nachricht nicht an ihr beabsichtigtes Ziel gelangt, wird diese Nachricht an den Absender zurückgesandt. Ein Grund dafür kann sein, dass ein Netzwerk, ein Host, ein Protokoll oder ein Port nicht

erreichbar waren. Möglicherweise wäre auch während der Übertragung eine Fragmentierung des gesendeten Datenpakets nötig gewesen, dies wurde aber durch das Setzen des Fragmentierungsbits im Header des IP-Pakets verboten. Ein weiterer möglicher Grund ist, dass ein bestimmtes Rechnersystem, das vom Absender in der Source-Routing-Option eingetragen wurde, nicht erreichbar war. Die Meldung »Destination Unreachable« kann beispielsweise von einem Angreifer dazu missbraucht werden, alle Verbindungen zwischen den beteiligten Rechnersystemen zu unterbrechen.

- Source Quench (4): Wenn ein Router nicht über die entsprechende Kapazität verfügt, um die empfangenen Daten direkt weiterzuleiten, sendet er an den Absender diese Nachricht. Dieser muss dann die Aussenderate von weiteren Nachrichten verringern.
- Redirect (5): Wenn ein Router erkennt, dass der Absender, anstatt direkt an den nächsten Router zu senden, einen unnötigen Umweg nimmt, sendet er diese Nachricht an den Absender. Das Datenfeld enthält die IP-Adresse des direkt erreichbaren Routers und wird in die Routingtabelle des Absenders eingetragen. Dieses Vorgehen kann von einem Angreifer missbraucht werden, um unerwünschte Routen zu konfigurieren und die Daten unterwegs abzuhören oder zu manipulieren.
- Echo Request (8): Diese Nachricht wird ausgesendet, um zu überprüfen, ob der beabsichtigte Empfänger erreichbar ist. Zusammen mit der Echo-Reply-Antwort auf diese Nachricht lassen sich Rückschlüsse über Betriebsbereitschaft, Laufzeit usw. ziehen.
- Time exceeded (11): Wenn ein IP-Datenpaket seine Lebensdauer (Time to Live) überschreitet, bevor es sein Ziel erreicht hat, wird es verworfen. Der Absender erhält dann von dem Rechnersystem, das diesen Vorgang ausgeführt hat, diese Meldung.
- Parameter Problem (12): Wenn ein IP-Datenpaket aufgrund fehlerhafter Angaben im Header verworfen wurde, erhält der Absender des Paketes diese Nachricht.

Ein Beispiel für die Benutzung von ICMP-Nachrichten ist der Befehl »Ping«, der auf den meisten Rechnersystemen verwendet wird. Dieser Befehl wird auf der Benutzerebene erzeugt und sendet eine oder mehrere ICMP-Nachrichten an den Empfänger. Dabei werden die Befehle »EchoRequest« und »EchoReply« verwendet, und der Absender erhält Informationen über:

- die IP-Adresse des Empfängers und die Erreichbarkeit des Rechnersystems,
- die MAC-Adresse des nächsten Routers beziehungsweise Rechnersystems,
- Routing-Einträge,
- Laufzeit der Daten,
- Datenverluste.

C.6.4 Portnummern

Ein wichtiger Begriff, der im Zusammenhang mit den Kommunikationsprotokollen auf der Transportebene immer wieder auftaucht, sind die so genannten Ports. Ein Rechnersystem, zum Beispiel ein Server, muss in der Lage sein, mit mehr als einem anderen Rechnersystem gleichzeitig zu kommunizieren. Anderenfalls wäre der Server während einer aufgebauten Verbindung für alle anderen Rechnersysteme nicht erreichbar. Bestimmte Anwendungen erfordern auch den gleichzeitigen Aufbau von zwei oder mehr Verbindungen, zum Beispiel jeweils eine für die Übertragung von Kommandos und für die Datenübertragung. Zu diesem Zweck verfügt jedes Rechnersystem über so genannte Portnummern, die zusammen mit der Netzwerk-Identifikation und der Rechnersystem-Identifikation einen Kommunikationsendpunkt (Port) bilden. Dieser Aufbau ist in etwa vergleichbar mit einer Telefonnummer. Die Netzwerk-Identifikation ließe sich mit der Vorwahl vergleichen, die Rechnersystem-Identifikation mit der Rufnummer und die Portnummer mit der Nebenstelle.

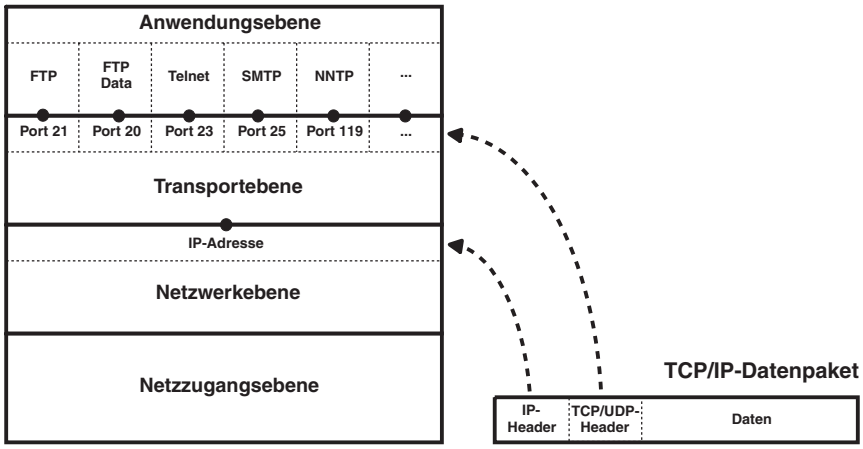


Abb. C.9: Eindeutige Identifizierung des Kommunikationsendpunkts durch IP-Adresse und Portnummer

Da eine Portnummer aus 16 Bit aufgebaut wird, wäre ein Rechnersystem mit einer IP-Adresse rein theoretisch in der Lage, gleichzeitig 65 535 Verbindungen zu anderen Kommunikations-Endpunkten herzustellen. Dies ist in der Praxis jedoch nicht der Fall, da die unterschiedlichen Kommunikationsprotokolle wie TCP oder UDP unterschiedliche Adressräume verwenden, die zwar identische Portnummern haben können, aber physikalisch nicht übereinstimmen.

Die Dienste der Anwendungsschicht (beispielsweise Telnet oder FTP) erfordern, wie weiter unten erläutert wird, eine bestehende virtuelle Verbindung zwischen

zwei Rechnersystemen. Um diese Verbindung überhaupt aufbauen zu können, muss dem aktiven, Kontakt aufnehmenden Rechnersystem (Client) aber zumindest ein Port bekannt sein, auf dem der entsprechende Dienst des passiven Rechnersystems (Server) erreichbar ist.

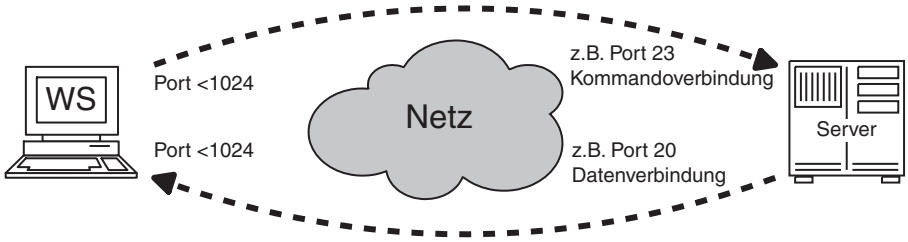


Abb. C.10: Verbindung zwischen zwei Rechnern (z. B. FTP-Verbindung)

Zu diesem Zweck wurden bestimmte Portnummern (well-known ports) definiert, die standardmäßig für die entsprechenden Dienste zur Verfügung stehen. Der Client kann dem Server dann über diesen Port seine eigene verwendete Portnummer mitteilen, und einem Verbindungsaufbau steht damit nichts mehr im Wege.

Dienst	Portnummer	Protokoll
echo	7	UDP oder TCP
ftp-data	20	TCP
ftp	21	TCP
telnet	23	TCP
smtp	25	TCP
dns	53	UDP
tftp	69	UDP
finger	79	TCP
http	80	TCP
nntp	119	TCP

Tabelle 3.1: Auszug aus der Liste mit well-known-ports

C.6.5 UDP

Das User Datagram Protocol (UDP) ist ein verbindungsloses Kommunikationsprotokoll der Transportebene. Es benutzt das untergeordnete IP-Protokoll, um Nachrichten von einem Rechnersystem zum anderen zu transportieren. In Ergänzung zum IP-Protokoll kann es aber zwischen mehreren Anwendungsdiensten (Ports) des Empfängers unterscheiden.

Der entscheidende Vorteil von UDP ist der geringe Overhead. Dadurch eignet es sich beispielsweise zur Übertragung von kleinen Datenmengen. Hier ist es einfacher, die Daten bei einem aufgetretenen Fehler einfach noch einmal zu übertragen, als eine garantiert fehlerfreie Verbindung aufzubauen. Dazu braucht man einen Frage-Antwort-Dialog zwischen zwei Rechnersystemen. Wenn nach einer bestimmten Zeit keine Antwort vom Ziel-Rechnersystem kommt, wird das Datenpaket noch einmal auf den Weg geschickt. Eine weitere Möglichkeit ist, einer übergeordneten Anwendung die Sicherungsfunktionen zu überlassen. In diesem Fall ist es unnötig, die Datenübertragung doppelt zu überwachen.

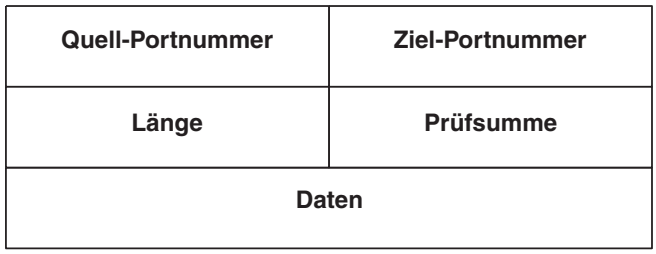


Abb. C.11: Header eines UDP-Datenpaketes

- Das UDP-Protokoll erzeugt keinerlei Transportquittungen oder andere Sicherheitsmaßnahmen, um die Korrektheit der Übertragung zu bestätigen. Es werden keine Informationen an das Quell-Rechnersystem zurückgegeben.
- Wenn die Daten auf dem Weg zum Ziel-Rechnersystem in mehrere Fragmente aufgeteilt wurden, können die Daten unterschiedliche Wege nehmen. So können Daten im Ziel-Rechnersystem in vertauschter Reihenfolge ankommen. Das UDP-Protokoll gibt die Daten unsortiert an die übergeordnete Anwendung weiter.
- Wenn die Daten schneller eintreffen, als das Ziel oder ein Rechnersystem im Netz sie verarbeiten kann, beispielsweise weil es überlastet ist, können die Daten verloren gehen. Es gibt keinerlei Informationen, die den Datenfluss zwischen den Rechnersystemen steuern oder kontrollieren.
- Der Header enthält zwei 16-Bit-Portnummern, die unabhängig von den beim TCP-Protokoll benutzten Portnummern sind.
- Grundsätzlich ist diese Form der Datenübertragung nicht vertrauenswürdig und sehr leicht zu manipulieren. Auf exponierten Rechnersystemen, die öffentlich zugänglich sind, sollte das UDP-Protokoll vermieden werden, es sei denn, eine übergeordnete Ebene (Anwendungsebene) übernimmt die Sicherungsfunktionen.

C.6.6 TCP

Das Transmission Control Protocol (TCP) ist nach dem IP-Protokoll das wichtigste Transportprotokoll. Das TCP-Protokoll ist ein verbindungsorientiertes Kommuni-

kationsprotokoll der Transportebene, das heißt, bevor die Daten von der Quelle zum Ziel geschickt werden, wird eine virtuelle Verbindung hergestellt, die in beide Richtungen (duplex) funktioniert. Die Daten werden in Form von festgelegten Paketen übertragen und die korrekte Übertragung durch unterschiedliche Verfahren sichergestellt.

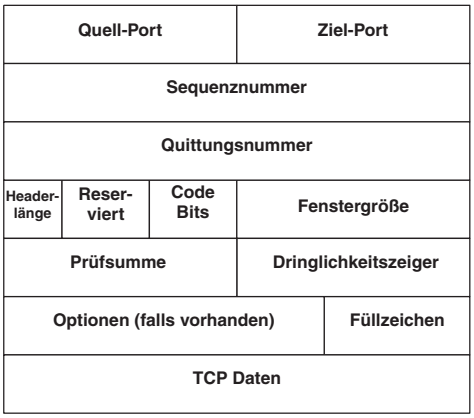


Abb. C.12: Header eines TCP-Datenpaketes

- Der Header eines TCP-Datenpaketes enthält unter anderem zwei 16-Bit-Portnummern, die zur Identifikation der Kommunikationsendpunkte von Quelle und Ziel dienen. Über die standardisierte Zuordnung (well-known ports) können die unterschiedlichen Dienste der Anwendungsschicht Verbindung miteinander aufnehmen.
- Beim Aufbau einer Verbindung generiert jede TCP-Einheit eine Anfangs-Sequenznummer. Diese Nummern werden ausgetauscht und gegenseitig bestätigt. Jedes gesendete Datensegment enthält eine fortlaufende Sequenznummer, wobei Duplikate ausgeschlossen werden. Anhand dieser Sequenznummern können die Daten beim Ziel, unabhängig vom Zeitpunkt des Eintreffens der Segmente, in der korrekten Reihenfolge zusammengesetzt werden.
- Die Quittungsnummer wird vom Ziel-Rechnersystem an das Quell-Rechnersystem übermittelt. Die Quittungsnummer ist immer um eins höher als die letzte Sequenznummer, die korrekt empfangen wurde. Anhand dieser Nummer kann das Quell-Rechnersystem die Pakete, die noch für eine eventuell erforderliche Wiederholung vorhanden sind, aus seinem Datenpuffer löschen.
- Das Feld Headerlänge bestimmt die Länge des Protokollkopfes in 32-Bit-Worten und damit den Anfang der Nutzdaten.
- Die Codebits oder Flags lösen bestimmte Reaktionen im TCP-Protokoll aus. Auf die genaue Bedeutung soll hier aber nicht weiter eingegangen werden.

- Ein Quell-Rechnersystem darf nicht mehr Daten abschicken, als ein Ziel-Rechnersystem verarbeiten oder weiterleiten kann. Dazu gibt das Ziel-Rechnersystem im Feld »Fenstergröße« an, wieviel Daten es zur sofortigen Verarbeitung in seinem Puffer zwischenspeichern kann.
- Jedes Datensegment enthält eine Prüfsumme, die aus dem Header und den Nutzdaten gebildet wird. Das Ziel-Rechnersystem errechnet aus den erhaltenen Daten ebenfalls eine Prüfsumme und vergleicht diese mit dem Datenfeld im Header des Datensegmentes. Stimmen die Werte überein, so schickt das Ziel-Rechnersystem eine positive Bestätigung an das Quell-Rechnersystem. Ein beschädigtes Datensegment wird zunächst ignoriert und nach einer angemessenen Wartezeit erneut angefordert.
- Für einige Dienste wurde ein Mechanismus konzipiert, mit dem der Server dazu veranlasst werden kann, dringende Anweisungen auszuführen, obwohl noch nicht alle Eingabedaten verarbeitet wurden. Diesem Zweck dient der Dringlichkeitszeiger (Urgent Data), der auf das Datenbyte vor der dringenden Meldung verweist (zum Beispiel die Übertragung eines Ctrl-C-Zeichens bei einer Telnet-Session).
- Normalerweise wird in einem TCP-Paket als Option nur die maximale Segmentgröße (Maximum Segment Size) verwendet. Damit teilt das Quell-Rechnersystem dem Ziel-Rechnersystem die maximale Größe der zu sendenden Datensegmente mit. Die weiteren Optionen sind No Operation und End of Option List.
- Das Feld »Füllzeichen« wird dazu benutzt, die Länge des Optionsfelds auszugleichen, damit die Gesamtgöße des Headers immer ein Vielfaches eines 32-Bit-Wortes ergibt.

Jedes Segment enthält eine Zeitüberwachung, das heißt, dass ein Ziel-Rechnersystem nach einer bestimmten Zeit eine Quittung über die enthaltenen Pakete an das Quell-Rechnersystem zurückschicken muß. Wenn ein Quell-Rechnersystem nach Ablauf der Quittungszeit keine Antwort erhalten hat, wird das entsprechende Datensegment erneut gesendet.

Damit haben wir die Protokolle der Transportschicht abgehandelt. In den folgenden Kapiteln werden die Protokolle und Dienste der Anwendungsschicht genauer betrachtet.

C.6.7 DNS

Um Rechnersystem-Namen entsprechende IP-Adressen zuordnen zu können, musste man in den Anfängen des Internet eine Liste der Rechnersystem-Namen von einem zentralen Server regelmäßig per Datenübertragung auf jedem Rechnersystem aktualisieren. Durch die rasante Ausbreitung des Internet ist diese Methode nicht mehr praktikabel. Aus diesem Grund wurde der Domain Name Service (DNS) entwickelt. Damit werden die Rechnersystem-Namen nicht mehr auf

jedem einzelnen Rechnersystem registriert, sondern auf speziell für diesen Dienst bereitgestellten Servern innerhalb jedes Teilnetzwerks. Die einzelnen Rechnersysteme senden bei Bedarf Abfragen (Queries) an diese Namen-Server, die als Antwort die entsprechende IP-Adresse oder den dazugehörigen Rechnersystem-Namen liefern.

Um dieses System benutzen zu können, ist jedes Internet-Teilnetzwerk dazu verpflichtet, einen Domain-Namens-Server zu betreiben oder betreiben zu lassen, auf dem sich so genannte Zonen-Datenbanken befinden. In diesen Datenbanken befinden sich unter anderem zwei Tabellen, mit der einem bestimmten Rechnersystem-Namen die dazugehörige IP-Adresse zugeordnet werden kann und umgekehrt.

Prinzipiell muss beachtet werden, dass alle vom DNS zur Verfügung gestellten Informationen missbraucht werden können, da diese Informationen nicht durch kryptographische Verfahren geschützt werden. Um Zugriff auf ein Rechnersystem eines Netzes zu erhalten, benötigt ein Eindringling zunächst dessen IP-Adresse, die er entweder durch blindes Probieren oder einfacher durch Auswertung der DNS-Informationen erhalten kann. Mittels dieser Informationen kann der Eindringling dann beispielsweise eine Adressfälschung (IP-Spoofing) vornehmen und damit Zugriff auf Rechnersysteme innerhalb des zu schützenden Netzes erhalten.

C.6.8 Telnet

Das Telnet-Protokoll erlaubt einem Benutzer (Client), eine Terminalsitzung auf einem entfernten Rechnersystem (Server) durchzuführen. Dazu wird zuerst eine TCP-Verbindung zwischen Client und dem Port 23 des Servers aufgebaut. Anschließend wird eine Login-Prozedur durchgeführt, in der sich der Benutzer durch die Angabe des Benutzernamens und des Passwortes identifizieren und authentisieren muss.

Abb. C.13: Beispiel einer Telnet-Sitzung

Bei dieser Authentikation über den Telnet-Dienst wird das Passwort im Klartext übertragen. Dabei besteht die Gefahr, dass sich ein Angreifer auf dem Übertragungsweg in eine autorisierte Telnet-Verbindung eingeschaltet hat, um sicherheitsrelevante Informationen (zum Beispiel Passwörter) abzuhören, oder um eigene Befehle in die Telnet-Verbindung einzugeben.

Anschließend kann der Angreifer sich unter Angabe der vorher abgehörten Identität auf dem Server anmelden (Maskerade-Angriff), um für ihn relevante Daten auszuspionieren, zu manipulieren oder zu löschen.

C.6.9 FTP

Das File Transfer Protocol (FTP) ermöglicht den Austausch und die Übertragung von beliebigen Dateien, ähnlich einem Datei-Manager, zwischen entfernten Rechnersystemen ähnlich einem Datei-Manager. Bei der Nutzung von FTP werden zwei unterschiedliche Verbindungen genutzt. Der Client baut als erstes von einem beliebigen Port eine Verbindung zum Port 21 des Servers auf. Über diese Verbindung sendet der Client dem Server die Kommandos. Mit dem Kommando »port« teilt der Client dem Server mit, über welchen Port er die Daten übertragen soll. Der Server baut nun anhand dieser Angaben eine TCP-Verbindung vom Port 20 zum angegebenen Port des Client auf und überträgt die angeforderten Daten.

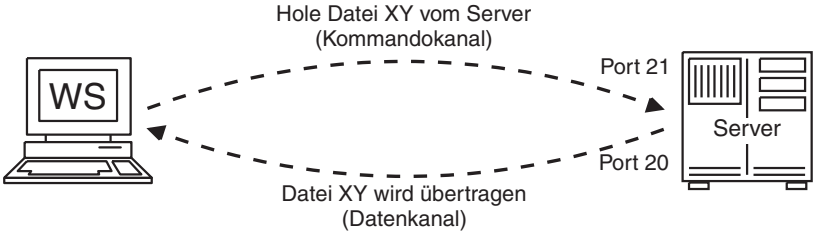


Abb. C.14: Beispiel einer FTP-Verbindung

Während der Client die Kommandoverbindung zum Port 21 des Servers aufbaut, ist der Server für den Aufbau des Datenkanals von seinem Port 20 zu einem beliebigen Port des Clients verantwortlich. Dies stellt eine Sicherheitslücke dar, da sich ein Angreifer selbst als Server ausgeben oder eigene Daten in die Kommunikation mit dem Server einfügen kann. Damit bekommt er die Möglichkeit, gefährliche Programme wie Viren oder Trojanische Pferde in das Rechnersystem einzuschleusen, die anschließend Daten ausspionieren oder zerstören können. Eine Abhilfe bietet die passive Methode des Verbindungsaufbaus.

C.6.10 SMTP

Das Simple Mail Transport Protocol (SMTP) ist ein einfaches Protokoll für die Übertragung von elektronischen Nachrichten (E-Mails) durch das Internet/Intranet. Das E-Mail-System besteht aus zwei Komponenten: dem Message Transfer Agent (MTA) und dem Mail User Agent (UA). Der Message Transfer Agent wird vom jeweiligen Internetprovider oder Intranetbetreiber installiert und hat die Aufgabe, die elektronische Post über die Teilnetzwerke an ihren Bestimmungsort wei-

terzuleiten. Der Mail User Agent ist nichts anderes als die E-Mail-Software, mit der der Benutzer je nach Programm seine elektronische Post verfassen, versenden und empfangen kann. Die elektronische Post wird auf dem Message Transfer Agent so lange gespeichert, bis der Benutzer sie mit Hilfe seiner Software auf das lokale Rechnersystem lädt.

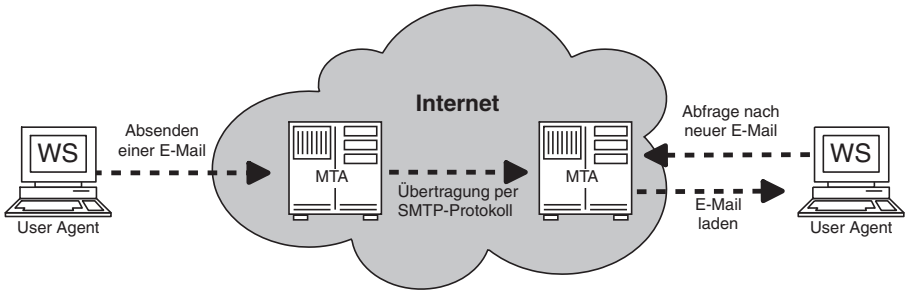


Abb. C.15: Funktionsweise des E-Mail-Dienstes

Der Übertragungsmodus der Nachrichten durch das Internet mit Hilfe des SMTP-Protokolls ist sehr einfach aufgebaut und wird im Klartext durchgeführt. Es ist bisher nicht möglich, die Identität des Absenders zu überprüfen. Dadurch ist es möglich, Nachrichten mit beliebigem oder gefälschtem Absender (Mail-Spoofing) über das Internet zu verbreiten. Einziger Schutz für den Anwender ist die Verwendung von kryptographischen Verfahren wie zum Beispiel der digitalen Signatur mit Verschlüsselung.

Ein weiterer Schwachpunkt des E-Mail-Systems ist das Programm Sendmail als die am weitesten verbreitete Umsetzung eines Message Transfer Agent unter Verwendung des SMTP-Protokolls. Die Komplexität und umfassende Leistungsfähigkeit macht Sendmail gleichzeitig sehr fehleranfällig und schwer zu konfigurieren. Dadurch wurden in den letzten Jahren immer wieder Sicherheitslücken entdeckt, mit denen Daten von Angreifern kopiert, manipuliert oder zerstört werden konnten.

C.6.11 HTTP

Wenn ein Anwender von seinem Rechnersystem aus eine »Reise« ins Internet unternimmt, benötigt er dafür ein spezielles Programm (Browser), das unter anderem die Darstellung von so genannten HTML-Dokumenten ermöglicht. HTML (Hyper Text Markup Language) ist ein Standard, der den Aufbau und das Format der für das World Wide Web charakteristischen Seiten definiert. Dabei muss es sich nicht nur um Textinformationen handeln. Es können gleichzeitig auch Grafiken, Töne oder Animationen und Videos übertragen werden. Um diese Informationen

im Internet übertragen zu können, wurde ein spezielles Kommunikationsprotokoll entwickelt, das Hypertext Transfer Protokoll (HTTP).

Das HTTP-Protokoll arbeitet nicht Session-orientiert, das heißt, die Übertragung eines HTML-Dokuments erfolgt unabhängig von einem zuvor übertragenen HTML-Dokument. Dazu wird, wie bei anderen Kommunikationsprotokollen der Anwendungsschicht (z. B. FTP oder Telnet), zunächst eine virtuelle Verbindung (TCP) zwischen Client und Server aufgebaut. Diese bleibt aber nicht über mehrere Anforderungen des Clients hinweg bestehen, sondern wird sofort nach dem Versenden der Antwort vom Server wieder abgebaut.

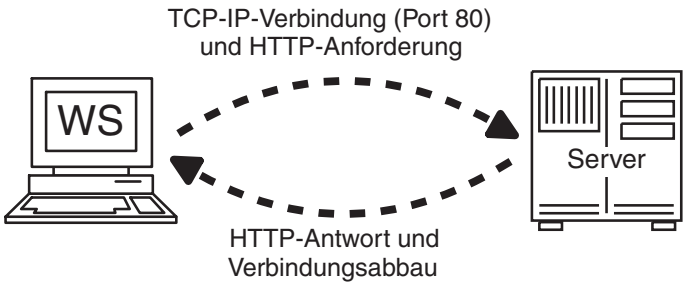


Abb. C.16: Prinzip einer HTTP-Verbindung

Wenn ein Benutzer eine beliebige Seite auf einem Server aufruft, so liest der Browser zunächst das HTML-Dokument und baut den Text entsprechend der angegeben Formatierungen (Größe, Farbe, Schriftart usw.) auf. Wenn eine WWW-Seite zusätzliche Informationen enthält, beispielsweise Grafiken, Töne oder Videos, so ist im HTML-Dokument der genaue Speicherort dieser Datei verzeichnet. Der Browser baut dann über das HTTP-Protokoll eine erneute Verbindung auf und holt sich die Grafik, Klangdatei, Videodatei oder sonstige Information vom Server. Nach dem Abschluss der Übertragung wird diese Information vom Browser auf dem Rechnersystem des Anwenders direkt dargestellt beziehungsweise wiedergegeben. Die meisten Browser kann man so konfigurieren, dass sie nur die gewünschten Informationen darstellen. Wenn zum Beispiel nur eine sehr langsame Verbindung ins Internet vorhanden ist, so kann man auf die Darstellung von großen Dateien wie Grafiken verzichten und nur die Textinformationen darstellen.

C.6.12 NNTP

Das Internet bietet durch seine enorme Größe eine Fülle von unterschiedlichen Informationen. Da die Entwicklung auf fast allen Wissensgebieten schnell fortschreitet, ist man darauf angewiesen, ständig auf dem neuesten Wissensstand zu sein. Eine Möglichkeit dazu bieten die so genannten Newsserver.

Manche Newsserver haben sich wegen der Vielzahl an Informationen auf spezielle Themengebiet spezialisiert.

Um die Newsserver ständig auf dem aktuellen Stand zu halten, tauschen diese untereinander in regelmäßigen Abständen neu eingegangene Beiträge aus. Innerhalb des Internet erfolgt dieser Datenaustausch mittels eines eigenständigen Protokolls. Das Network News Transfer Protocol (NNTP) wird benutzt, um neue Beiträge an den nächsten Newsserver zu versenden. Dieser überträgt die aktuellen Informationen dann weiter zum nächsten usw. Diesen Vorgang bezeichnet man als »News Feed«. Da einige dieser Server die Informationen nicht nur an einen, sondern gleich an mehrere Server weiterleiten, kann sich eine neue Information innerhalb weniger Tage innerhalb des gesamten Internet ausbreiten.

Das heute benutzte NNTP-Protokoll verfügt über einen Mechanismus, mit dem es möglich ist, nur jene Artikel zu übertragen, die auf dem Rechnersystem des Empfängers noch nicht vorhanden sind.

Anhang D

Wichtige Adressen und Web-Links

Im Folgenden sind einige wichtige Adressen und Web-Links angegeben, bei denen Sie Informationen und Hilfestellungen rund um das Thema VPN erhalten können.

D.1 Adressen zur Informationssicherheit

- Bundesamt für Sicherheit in der Informationstechnik (BSI)
  Postfach 20 03 63, 53133 Bonn
  Telefon: (02 28) 95 82-444, Fax -427

  E-mail: cert@bsi.de

  Homepage: `www.bsi.de`

  Universität Siegen

  Homepage: `www.uni-siegen.de`

- Recht im Internet
  Homepage: `www.netlaw.de`

  Utimaco Safeware AG
  Niederlassung Aachen
  Germanusstraße 4, 52080 Aachen

  Tel.: (02 41) 1696-0, Fax -199

  Homepage: `www.utimaco.de`

- Compumatica secure networks GmbH
  Germanusstraße 4, 52080 Aachen

  Tel.: (0241) 1696-400, Fax: -410

  Homepage: `www.compumatica.de`

D.2 CERT

Computer Emergency Response Teams (CERT) sind Organisationen, die über bekannt gewordene Betriebssystemfehler und deren Behebungsmöglichkeiten informieren.

Computer Emergency Response Team/Coordination Center (CERT/CC),
Software Engineering Institute
Carnegie Mellon University, Pittsburgh, PA 15213-3890

Tel. +1 41 22 68-70 90 (24-Stunden-Hotline)

E-mail: `cert@cert.sei.cmu.edu` oder `cert@cert.org`

ftp: cert.sei.cmu.edu (192.88.209.5)

- Die CERT-Mitteilungen werden in Newsgruppen (`comp.security.announce` und `info.nsfnet.cert`) und über Mailinglisten (Aufnahme durch E-mail an: `cert-advisory-request@cert.org`) veröffentlicht.

CERT in Deutschland

- BSI-CERT
  Bundesamt für Sicherheit in der Informationstechnik (BSI)
  Postfach 20 03 63, 53133 Bonn
  Telefon: (02 28) 95 82-444, Fax: -427

  E-mail: `cert@bsi.de`

- DFN-CERT
  Universität Hamburg
  Fachbereich Informatik
  Vogt-Kölln-Straße 30, 22527 Hamburg

  Telefon: (0 40) 5 47 15-262, Fax: -241

  E-mail: `dfncert@cert.dfn.de`

  ftp: `ftp.cert.dfn.de: /pub/security`

  gopher: `gopher.cert.dfn.de`

  Aufnahme in Mailingliste für CERT-Mitteilungen durch E-mail an:
  `dfncert-request@cert.dfn.de`

  Mailinglisten für Diskussionen: `win-sec@cert.dfn.de`

Mailinglisten für sicherheitsrelevante Informationen:
win-sec-ssc@cert.dfn.de
URLs: ftp://ftp.cert.dfn.de/pub.security
www.cert.dfn.de/dfncert.dfncert.html

- Micro-BIT Virus Center/CERT
  Universität Karlsruhe
  Postfach 69 80, 76128 Karlsruhe
  Telefon: (07 21) 37 64 22, Fax: (07 21) 3 25 50

  E-mail: cert@rz.uni-karlsruhe.de

D.3 Informationen zu VPNs im Internet

VPN allgemein

ICSA Labs (zertifizierte Produkte)

www.icsalabs.com/html/communities/cryptography/index.shtml

Linux-VPN

www.linuxdoc.org/HOWTO/mini/VPN.html
www.linuxdoc.org/HOWTO/VPN-Masquerade-HOWTO.html

VPN-Insider (News und Links)

www.vpninsider.com/

VPN-Forum von About (News und Links)

http://intranets.about.com/compute/intranets/cs/vpn/index.htm

Kryptographische Algorithmen

Dokumentation zum AES-Auswahlverfahren und dem Rijndael-Algorithmus

http://csrc.nist.gov/encryption/aes/

Linkseite der Universität von British Columbia

www.cs.ubc.ca/spider/mjmccut/crypto.html

Linkseite der Carnegie Mellon School of Computer Science

www.cs.cmu.edu/afs/cs/project/pscico-guyb/realworld/www/crypto.html

Computer Security and Industrial Cryptography (Universität Leuven)

www.esat.kuleuven.ac.be/cosic/

Electronic Frontier Foundation

www.eff.org/pub/Privacy/Crypto_misc/

Glossar zum Thema Verschlüsselung

www.identification.de/crypto/cryterms.html

Website des Krypto-Experten Bruce Schneier

www.counterpane.com/

Protokolle

Internet Engineering Task Force (IKE)

www.ietf.org/

Microsoft (PPTP)

http://windows.microsoft.com/windows2000/en/server/help/access_PPTP.htm
www.microsoft.com/ntserver/commserv/deployment/moreinfo/PPTPfaq.asp

Ohio State University (online-Zugriff auf RFCs)

www.cis.ohio-state.edu/htbin/rfc/INDEX.rfc.html

PGP

www.pgp.com/

Sun Microsystems (SKIP)

www.sun.com/security/skip/
http://skip.incog.com/

Secure Shell

www.ssh.com/products/ssh/

WAP-Forum

www.wapforum.org/

Anhang E

VPN-Anbieterverzeichnis

Der VPN-Markt ist der am dichtesten besetzte Markt im Bereich »Internet Communication Security«. Vorrangig sind dort große Netzwerk-Anbieter, IT-Sicherheitsfirmen oder Spezialisten für VPN-Systeme tätig.

VPN-Lösungen unterscheiden sich hinsichtlich ihres Preises, der Skalierbarkeit sowie der herstellerspezifischen Mehrwerte.

Im Folgenden wird eine alphabetische Liste von VPN-Herstellern aufgeführt. Weitere Informationen sind auf den entsprechenden Websites (meistens `www.firmenname.com`, `www.firmenname.de` etc.) zu finden.

- 3Com
- Alcatel
- Ashley Laurent
- Aventail
- Axent Technologies
- Biodata
- Bull
- Cabletron/Entrasys/Indus River
- Celo Communications
- Check Point/Nokia
- Cisco
- Compumatica secure networks GmbH
- Computer Associates
- Cosine Communciations
- Cylink
- Fischer International Systems
- Fortress Technologies
- F-Secure
- Infoexpress
- Internet Dynamics
- IPlanet
- IRE
- Lucent Technologies
- Microsoft
- Netscreen Technologies
- Network Associates

- Network Telesystems
- Norman
- Nortel
- OneBox Networks
- Radgurad
- Redcreek
- Secure Computing
- Shiva
- Siemens
- SonicWALL
- SSH Communications Security
- Syndata
- Trustworks
- Tut Systems
- Utimaco Safeware AG
- V-One
- VPNet
- Watchguard
- WindRiver

Anhang F

Literaturverzeichnis

/AbO92/	M.D. Abrams, I.D. Olson: »Rule-Based Trusted Access Control«, in: IT-Security, Proceedings of the IFIP/SEC ´92 Singapore, North-Holland 1992
/Acam2001/	Markus a Campo: »Security News Letter«, erscheint alle zwei Wochen im Interest-Verlag, Kissing, 2001-2002
/AHKP91/	M.D. Abrams, J. Heaney, O. King, L.J. LaPadula, I.D. Olson: »Generalized Framework for Access Control«, Proceedings of the 14th National Computer Security Conferenz, Oct. 1991
/Alad99/	Aladdin. »Safe Internet Connectivity for the Home & Small Office«, White Paper, Aladdin Knowledge Systems, USA , Seattle 1999
/Arno2000/	Ingmar Arnold: »Luft-Züge – Die Geschichte der Rohrpost in Berlin und anderswo«, Gesellschaft für Verkehrspolitik und Eisenbahnwesen e. V.; ISBN: 389218061X, Berlin 2000
/BaHoKn/	A. Badach, E. Hoffmann u. O. Knauer: »High Speed Internetworking: Grundlagen und Konzepte für den FDDI und ATM«, Bonn u.a.: Addison-Wesley, 1994
/Bans96/	Banse, Gerhard, IT-Sicherheit im Spiegel der aktuellen Risikodiskussion – die philosophisch-technikgeschichtliche Bündelung, in: BSI (Hrsg.), Wie gehen wir künftig mit den Risiken der Informationsgesellschaft um?, SecuMedia Verlag, Ingelheim 1996
/Birn96/	Birnbacher, Dieter, Sicherheit und Risiken – philosophische Reflexionen, in: BSI (Hrsg.), Wie gehen wir künftig mit den Risiken der Informationsgesellschaft um?, SecuMedia Verlag, Ingelheim 1996
/Black2001/	Edwin Black: »IBM und der Holocaust«, 704 S., Berlin: Propyläen-Verlag
/BLP74/	D.E. Bell, L.J. LaPadula: »Secure Computer System – A Refinement of the Mathematical Model«, NTIS AD-780 528, MTR 2547 Vol. III, MITRE Corp., Bedford, MA, USA, 1974
/BoOl96/	Paul M. Boshoff, Martin S. Olivier: »Increasing Firewall Realiability by Recording Routes«, in: Communication and Multimedia Security, II, Chapman & Hall, Padstow, Cornwall 1996
/Boro92/	Petra Borowka: »Brücken und Router: Wege zum strukturierten Netzwerk«, Bergheim: DATACOM-Verlag Lipinski, 1992
/BoWo97/	Andreas Bonnard, Christian Wolff: »Gesicherte Verbindung von Computernetzen mit Hilfe einer Firewall«, BSI-Studie, Bonn, 1997

/BSI00/	BSI - Bundesamt für Sicherheit in der Informationstechnik: »DDoS Analyse der Angriffe Erkenntnisse, Auswertung, Tendenzen«, BSI-Studie, Bonn 2000
/BSI97/	BSI: »Mit Sicherheit in die Informationsgesellschaft«, Tagungsband, 5. Deutscher IT-Sicherheitskongreß des BSI, Ingelheim: SecuMedia Verlag, 1997
/BSI98/	BSI – Bundesamt für Sicherheit in der Informationstechnik: »Object Code and Optimizing Compiler Analyzing Tool – Analyse der Risiken ausführbarer Web-Contents, Teil 1; BSI Studie, Bonn, 1998
/BSI99/	BSI: »IT-Grundschutzhandbuch«, BSI 7152, Köln: Bundesanzeiger-Verlag, 1999
/Cart95/	Carter,G., Clark, A., Dawson, E., and Nielsen, L., »Analysis of DES Double Key Mode« Information Security – the Next Decade, Conference Proceedings of IFIP/Sec'95, Chapman & Hall, 1995, pp.113-127
/CCITT/	CCITT: »The Directory – Authentication Framework«, Draft Recommendation X.509, Gloucester: 11/1987
/CERT95/	CERT im DFN: »Sicherheit in vernetzten Systemen«, Hamburg: Workshop, 1995
/CESG3/	UK Systems Security Confidence Levels: CESG Memorandum No. 3, Communications-Electronics Security Group: 01/1989
/Chau87/	D. Chaum: »Security without Identification: Transaction Systems to Make Big Brother Obsolete«, Comm. ACM 28, 10/1985, S. 1030–1044, Deutsche Übersetzung in: »Sicherheit ohne Identifizierung«, Informatik-Spektrum 10, 1987, S. 262–277
/CheBe/	W. R. Cheswick, St. M. Bellowin: »Firewalls und Sicherheit im Internet« – Schutz vernetzter Systeme vor cleveren Hackern, Deutsche Übersetzung von Thomas Maus, Mit einem Beitrag über das deutsche Recht von Prof. Dr. U. Sieber, Bonn: Addison-Wesley Publishing Company, 1996
/ChZw96/	D. B. Chapman & E. D. Zwicky: »Einrichten von Internet Firewalls – Sicherheit im Internet gewährleisten«, Bonn: O´Reilly, Internat. Thomson-Publishing, 1996
/Cole99a/	Tim Cole: »Erfolgsfaktor Internet – Warum kein Unternehmen ohne Vernetzung überleben wird«, ECON, 1999
/Cole99b/	Tim Cole, Michael Matzer: »Managementaufgabe Sicherheit«, Hanser, 1999

/Comm98/	ISO/IEC SC27 N2161: »Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and gerneral model« 1998
/DTIEC/	DTI Commercial Security Centre Evaluation Levels Manual, V22 Department of Trade and Security, 02/1989
/Fluh01/	S. Fluhrer, I. Mantin, A. Shamir: Weakness in the Key Scheduling Algorithm of RC4, Eighth Annual Workshop on Selected Areas in Cryptography, 2001
/Fuhr98/	Kai Fuhrberg: »Internet-Sicherheit: Browser, Firewalls und Verschlüsselung«, Hanser-Verlag, Munich, Vienna, 1998
/Gord84/	J. Gordon: »Strong RSA keys«, Electronic letters, 7.th June 1984, Vol. 20, No. 12
/Görtz99/	Horst Görtz, Jutta Stolp: »Informationssicherheit in Unternehmen, Sicherheitskonzepte und -lösungen in der Praxis« Bonn, Addison-Wesley, 1999
/Hamp96/	J. F. Hampe: »Intranet: Einordnung und Entwicklungstrends«, Beitrag zum Kongreß zur Einführung und Anwendung von Intranets in Unternehmen, München: ComMunic, 09/1996
/Harl2000/	Magnus Harlander: »Hochverfügbarkeit und Loadbalancing«, IT-Sicherheit – Praxis der Daten- und Netzsicherheit, DATAKONTEXT-Fachverlag, Köln, 5/2000
/Hugh95/	L.J. Hughes, Jr.: »Actually Useful Internet Security Techniques«, Indianapolis: New Riders Publishing, 1995
/IEEE1/	IEEE Standard 802.3 und 802.2: »Aufbau des Ethernet MAC Frames«, USA, 1996
/ISO9798/	Information Processing Systems – Open Systems Interconnection, Electronic Data Ingerchange for Administration, Commerce and Transport (EDIFACT) – Application Level Syntax Rules
/ITSEC91a/	Commission of the European Communities: »Information Technology Security Evaluation Criteria (ITSEC)«, Brussels, Luxembourg: 1991
/ITSEC91b/	Office for Official Publications of the European Communities: »Information Technology Security Evaluation Criteria«, Luxembourg: 06/1991 (=Amt für amtliche Veröffentlichungen der Europäischen Gemeinschaften): »Kriterien für die Bewertung der Sicherheit von Systemen in der Informationstechnik«, Luxemburg: 06/1991)
/ITSEM94/	Commission of the European Communities, Directorate-General XIII »Information Technology Security Evaluation Manual (ITSEM)« ECSC-EEC-EAEC, Brüssel/Luxembourg, 1994
/Kahn97/	David Kahn, The Codebreakers, Revised Edition (1997), Simon & Schuster; ISBN: 0684831309

/Koke97/	Andreas Koke: »Java und ActiveX – Gefahr aus dem Internet?«, in: Mit Sicherheit in die Informationsgestellschaft, Tagungsband 5. Deutscher IT-Sicherheitskongress des BSI, SecuMedia Verlag, Ingelheim 1997
/Kupp99/	Martin Kuppinger: »Sicher ist Sicher«, PC Professionell, 06/1999
/Kyas96a/	O. Kyas: »Internet professionell«, Technologische Grundlagen & praktische Nutzung, Bonn: International Thomson Publishing, 1996
/Kyas96b/	O. Kyas: »Sicherheit im Internet – Risikoanalyse, Strategien, Firewalls«, Bergheim: DATACOM-Verlag, 1996
/Leu01/	Matthias Leu, Checkpoint Firewall-1/VPN-1, Computer & Literatur, 2001
/McKe95/	McKenney, Copeland, Mason: »Waves of Change: Buisiness Evolution Through Information Technologie«, Havard Buisiness School Press, USA, 1995
/NCSA/	NCSA: »Firewall Policy Guide«, NCSA Security White Paper Series, Carlisle: NCSA Publication, 1994
/Pohl90/	Norbert Pohlmann: »Das RSA-Verfahren und dessen Anwendung«, DuD, Vieweg, 1990
/Pohl92/	Norbert Pohlmann: »Vernetze Systeme: Alptraum oder Chance zur Lösung der Sicherheitsproblematik?«, Bergheim: DATACOM-Verlag, 1992
/Pohl96/	Norbert Pohlmann: »Datenschutz – Sicherheit in öffentlichen Netzen«, Heidelberg: Hüthig Verlag, 1996
/Pohl97a/	Norbert Pohlmann: »Sinn und Zweck von IT-Sicherheitsstudien, Teil 1 – Feststellung des Schutzbedarfes und Bedrohungsanalyse«, in: W&S – Wirtschaftsschutz & Sicherheitstechnik, Heidelberg: Hüthig Verlag, 3/97
/Pohl97b/	Norbert Pohlmann: »Sinn und Zweck von IT-Sicherheitsstudien, Teil 2 – Vom Anforderungskatalog bis zu den Ergebnissen einer IT-Sicherheitsstudie«, in: W&S – Wirtschaftsschutz & Sicherheitstechnik, Heidelberg: Hüthig Verlag, 04/1997
/Pohl 99a/	»Mailtrust macht europäische E-Mail sicher« LANline – Das magazin für Netze, Daten- und Telekommunikation Awi LANline Verlagsgesellschaft, Grasbrumm 10/99

/Pohl 99b/	»Die Zukunft von Firewall-Systemen« DATACOM – Fachzeitschrift für die elektronische Datenkommunikation CMP-WEKA-Verlag, Poing 1/99
/Pohl99c/	»Virtual Private Networks (VPN)«, IT-Sicherheit - Praxis der Daten- und Netzsicherheit, DATAKONTEXT-Fachverlag, Köln 4/99
/Pohl99d/	»Virtuelle Private Netze«, Funkschau – 23/99, WEKA Fachzeitschriften-Verlag, Poing, 1999
/Pohl2000a/	Norbert Pohlmann: »Dezentrale Firewalls schließen Lücken«, KES – Kommunikations- und EDV-Sicherheit, SecMedia Verlag, Ingelheim 4/2000
/Pohl2000b/	Norbert Pohlmann: »Personal Firewall-Systeme«, IT-Sicherheit - Praxis der Daten- und Netzsicherheit, DATAKONTEXT-Fachverlag, Köln, 5/2000
/Pohl2001a/	Norbert Pohlmann: »Firewall-Systeme«, 600 S., Bonn: mitp-Verlag
/Pohl2001b/	Norbert Pohlmann: »Organisationshandbuch Netzwerksicherheit«, Loseblatterk mit CD, wird 5 x jährlich aktualisiert, Augsburg: INTEREST-VERLAG, siehe auch: *www.interest.de*
/Pohl 2002/	Norbert Pohlmann: »Nutzen und Chancen von Public-Key-Infrastrukturen«, in: »Sicherheitsinfrastrukturen in Wirtschaft und Verwaltung«, hrsg. v. Patrick Horster, IT Verlag, 2002
/PoRi95/	Norbert Pohlmann und Wolfgang Ring: »Faxmanipulation am Beispiel einer Rangbescheinigung«, in: »Elektronischer Rechtsverkehr – Digitale Signaturverfahren und Rahmenbedingungen«, hrsg. v.: Bundesnotarkammer, Köln: Verlag Dr. Otto Schmidt, 1995
/RFC1700/	Request for Comment: »SOCKS«,IETF, Network Working Group; USA; September 1981
/RFC759/	Request for Comment: »File Transfer Protocol«; IETF, Network Working Group; USA, October 1985
/RFC768/	Request for Comment: »User Datagram Protocol«; IETF, Network Working Group; USA, August 1980
/RFC791/	Request for Comment: »Internet Protocol«; IETF, Network Working Group; USA, September 1981
/RFC792/	Request for Comment: »Internet Control Message Protocol«; IETF, Network Working Group; USA, September 1981
/RFC793/	Request for Comment: »Transmission Control Protokol«; IETF, Network Working Group; USA, September 1981
/Rula94/	Christoph Ruland: »Informationssicherheit in Datennetzen«, Bergheim: DATACOM-Verlag, 1993
/Sand00/	Sandbox: »Protection against Malicious Mibile Code«, White Paper, Sandbox Security AG, Germany, Puchheim, 2000

/Santifaller/	M. Santifaller: »TCP/IP und ONC/NFS in Theorie und Praxis – UNIX in lokalen Netzen«, 2. Auflage, Bonn: Addison-Wesley Publishing Company, 1993
/Schmi02/	M. Schmidt: Consistent M-Commerce Security on Top of GSM-based Data Protocols – A Security Analysis, Institut für Datenkommunikation der Universität Siegen, 2002
/Schn96 /	Bruce Schneier: »Angewandte Kryptographie«, Bonn: Addison-Wesley-Publishing Company, 1996
/SCSSI/	Catalogue de Critères Destinés à évaluer le Degré de Confiance des Systèmes d'Information, Service Central de la Sécurité des Systèmes d'Information, 07/1989
/Sieber/	Ulrich Sieber: »Computerkriminalität und Informationsstrafrecht – Entwicklungen in der internaltionalen Informations- und Risikogesellschaft«, in: Computer und Recht 02/1995
/SiHa95/	Karanjit Siyan, Chris Hare: »Internet Firewall and Network Security«, New Rider Publishing, USA, Indianapolis, 1995
/Sobi99/	M. Sobirey: »Datenschutzorientiertes Intrusion Detection«, Vieweg-Verlag, 1999
/STOA/	Scientific and Technological Options Assessment (STOA) of the European Parliament: Report: »An Appraisal of the Technologies to Political Control«, Download und aktuelle Ergänzungen des Reports unter: `www.europarl.eu.int/dg4/stoa/en` oder `http://cryptome.org/stoa-atpc.htm`
/Stol98/	Bernd Stoltefuss: »Auswahl von Firewall-Systemen – Eine strukturierte Vorgehensweise«, KES, SecuMedia, Ingelheim, 04/98
/Strömer/	Tobias H. Strömer: »Online-Recht – Rechtsfragen im Internet und in Mailboxnetzen«, Heidelberg: dpunkt-Verlag, 1997
/Stubb01/	A. Stubblefield, J. Ioannidis, A. Rubin: Using the Fluhrer, Mantin, and Shamir Attack to Break WEP, AT&T Labs, 2001
/Tann98/	A.S. Tannenbaum: »Computer Networks« PrenticeHall, New Jersey, 1998
/Tann98/	A.S. Tannenbaum: »Computer Networks«, Prentice Hall, USA, New Jersey, 1998
/TCSEC/	Department of Defence (USA): Trusted Computer Systems Evaluation Criteria, DOD 5200.28-STD, 12/1985
/uti98/	Utimaco Safeware: »Circuit Level Proxy«, White Paper, Utimaco Safeware AG, Aachen 1998

/uti99/	Utimaco Safeware: »Globale Authentikation«, White Paper, Utimaco Safeware AG, Aachen 1998
/WashEv/	K. Washburn, J. Evans: »TCP/IP: Aufbau und Betrieb eines TCP/IP-Netzes«, Bonn u.a.: Addison-Wesley Publishing Company, 1994
/Weck/	G. Weck: »Datensicherheit: Methoden, Maßnahmen und Auswirkungen des Schutzes von Informationen«, Stuttgart: Teubner, 1984
/Woel99/	Woelke von der Brüggen: »Schutz gegen Malicious Mobile Code«, White Paper, Soft Research Linited, Irland 1999
/ZSIEC/	BSI: Criteria for the Evaluation of Trustworthiness of Information Technology (IT) Systems, German Information Security Agency (Bundesamt für Sicherheit in der Informationstechnik) 9, 01/1989
/Zurf99/	E. Zurfluh: »Erfolg im Electronic Business durch Management der Risiken«, Tagungsband des Seminar IT- und Informations-Sicherheit, Zürich 1999

Anhang G

Glossar, Abkürzungen

Als Nachschlagewerk für den Bereich Informationstechnologie empfiehlt sich das über 3000 Seiten umfassende, regelmäßig aktualisierte Loseblattwerk: »Informationstechnologie von A–Z« aus dem INTEREST-Verlag, siehe: `www.interest.de`

ActiveX

Von Microsoft entwickelte Programmiersprache als Antwort auf →Java und →JavaScript. Der Programmcode (ActiveX Control) wird mit einem ActiveX-fähigen →Browser von einem →Web-Server geladen und auf dem lokalen Rechnersystem ausgeführt.

AES

= Advanced Encryption Standard, neuer Standard für →symmetrische Verschlüsselungsverfahren, →Rijndael-Algorithmus

AOL

= America Online; Onlinedienst und Internet-Provider

AP

= Authentication Process

Applet

In →Java geschriebener Programmcode, der auf dem lokalen Rechnersystem innerhalb einer eigenen Umgebung ausgeführt wird.

Application Gateway

Das Rechnersystem, auf dem ein oder mehrere →Proxies realisiert sind.

ARPA

= Advanced Research Projects Agency

ARPANET

= Advanced Research Projects Agency Network; weltweit erstes Datennetz, basierend auf paketorientierter Datenübertragung. Aus dem ARPANET entstand das heutige →Internet.

ASP

= Application Service Provider, stellt outgesourcte IT-Infrastruktur (Hardware, Software, Litenzen) zur Verfügung

Asymmetrische Verschlüsselung

auch Public-Key-Verfahren genannt; Verschlüsselungsverfahren, bei dem zwei verschiedene Schlüssel eingesetzt werden. Mit dem einen der beiden Schlüssel werden die Daten oder das Dokument verschlüsselt und/oder signiert, und die Entschlüsselung/Prüfung kann nur mit dem entsprechenden anderen Teilschlüssel erfolgen. Hierzu werden Algorithmen aus der Komplexitätstheorie verwendet.

Asynchroner Transfermodus

Der Asynchrone Transfermodus (ATM) ist ein Datenübertragungsverfahren, das die →Bandbreite erheblich steigern kann. Es ermöglicht das gleichzeitige Übertragen von Daten aus verschiedenen Quellen und kann so die Übertragungskapazitäten optimal ausnutzen. Damit kann eine Bandbreite von bis zu 2,3 GBit erzielt werden.

ATM

= →Asynchroner Transfermodus

Authenticode

Kontrollverfahren für die Anwendung von →ActiveX controls. Ein Programmierer von ActiveX controls hat den Zugriff auf sämtliche Systemressourcen und besitzt damit die gleichen Rechte wie der gerade angemeldete Anwender. Um einen Mißbrauch zu verhindern, kann mit der Authenticode-Technologie die Herkunft der verwendeten ActiveX controls durch digitale Signatur nachgewiesen werden.

Authentikation

Authentikation bedeutet die Verifizierung (Überprüfung) der Echtheit bzw. der Identität einer Person oder Sache. Eine Authentikation kann benutzerorientiert (→Benutzerauthentikation) oder rechnerorientiert (anhand der Rechneradresse) durchgeführt werden.

B2B

= Business-to-Business, Applikation, bei der Rechnersysteme unterschiedlicher Firmen untereinander automatisch Geschäftsabläufe abwickeln

Backdoor

= Hintertür; eine versteckte bzw. undokumentierte Programmfunktion, mit deren Hilfe vom Benutzer nicht autorisierte Personen auf dessen Rechnersystem bzw. die darauf gespeicherten Daten zugreifen können (vgl. →Trojanisches Pferd)

Bandbreite

Mit Bandbreite bezeichnet man die Datenmenge, die ein bestimmter Leitungstyp pro Zeiteinheit transportieren kann. Eine analoge Telefonleitung etwa hat eine Bandbreite von ca. 56 KBit, eine ISDN-Leitung schafft 64 KBit, bzw. im Duplex-Betrieb 128 Kbit das Ethernet 10 MBit, das Fast Ethernet 100 MBit. Ein →ATM schließlich erreicht eine Bandbreite von bis zu 2,3 GBit.

Bastion

→Application Gateway, der als einziges Rechnersystem aus dem unsicheren Netz angesprochen werden kann.

BDSG

= Bundesdatenschutzgesetz

Benutzerauthentikation

Die →Authentikation ist an den Benutzer gebunden. Dazu exisitieren bei Firewall-Systemen verschiedene Authentikationsmechanismen, z. B.:

- Eingabe von User-ID und Paßwort
- S/Key
- Token (Challenge/Response)
- Chipkarten.

Biometrie

Biometrische Authentikationsverfahren benutzen unverwechselbare physikalische Besonderheiten des Anwenders wie Fingerabdruck oder Gesichtscharakteristika zu seiner Authentifizierung.

Blowfish

→symmetrisches Verschlüsselungsverfahren, unterlag dem →Rijndael-Algorithmus beim Wettstreit um den neuen Advanced Encryption Standard (→AES)

Browser

Browser nennt man die Software, mit der Internet-Seiten gelesen werden können. Der Browser greift über das HyperText Transfer Protocol (→HTTP) auf Web-Server zu. Dokumente werden im HTML-Format vom Browser interpretiert und dem Benutzer inklusive der Bilddaten dargestellt. Geläufige Browser sind z. B. Netscape Navigator, MS Internet Explorer und Lynx.

Brute-Force-Attack

Beim →Hacking von kryptographischen Schlüsseln oder Passworten kann man unterschiedlich raffiniert vorgehen. Man kann beispielsweise versuchen, Anhaltspunkte zu finden und auszuwerten. Brute-Force (rohe Gewalt) bezeichnet dagegen die primitivste Art des Angriffs: man probiert einfach blindlings alle denkbaren Möglichkeiten durch. Ein solcher Angriff ist heute nicht mehr vielversprechend: Wer per Brute-Force-Attack einen 128-Bit-Schlüssel ermitteln will, braucht voraussichtlich ein Vielfaches der Lebenszeit unseres Sonnensystems.

BSI

= Bundesamt für Sicherheit in der Informationstechnik, siehe auch: `www.bsi.de`

CA

= Certification Authority; Zertifizierungsstelle, die Benutzerschlüssel als Zertifikat (elektronischer Ausweis) ausgibt. Die Zertifikate dienen zum einen der authentischen Übermittlung von Daten und zum anderen der Identitätsprüfung des Urhebers.

CCITT

= Comité Consultatif International Télégraphique et Téléphonique

CERT

= Computer Emergency Response Team; Aufgabe des CERT ist es unter anderem, als Internet-Feuerwehr schnell und effizient auf kritische Vorfälle (z. B. Hacker-Angriffe, Sicherheitslücken, Viren etc.) zu reagieren und Hilfe zu leisten und Informationen aufzubereiten und bereitzustellen. In Deutschland wird das CERT vom →DFN unterstützt.

CGI

= Common Gateway Interface; Programmschnittstelle zwischen beim Web-Server eingehenden Benutzerdaten (z. B. ausgefüllte Formulare) und angeschlossenen Programmen wie z. B. Datenbanken. Mit Hilfe von CGI-Skripten kann man Web-Seiten dynamisch gestalten und mit interaktiven Elementen versehen.

Chiffrierfehler

Wenn bei der Anwendung oder Konzeptionierung eines Verschlüsselungsverfahrens Pannen oder Nachlässigkeiten passieren, spricht man von Chiffrierfehlern. Sie haben in der Regel zur Folge, daß die erzeugten Schlüssel weniger komplex sind bzw. aus einer kleineren Menge von Kombinationen hervorgehen, als technisch möglich wäre.

Common Point of Trust

Einziger Übergang zwischen unterschiedlichen Netzen, der als vertrauenswürdig angesehen und mit Hilfe eines Firewall-Systems realisiert wird.

Content Security

Internet-Dokumente (HTML-Seiten, E-Mails) sind durch Schadensprogramme →Malware gefährdet

Cookies

Informationen, die der →Web-Server im →Browser des Clients ablegt, beispielsweise eine Kundennummer, über die der Benutzer bei einem Folgebesuch der Website identifiziert werden kann.

Corporate Network

Unternehmen und Behörden bauen mit Knoten, Routern und Multiplexern ihre eigenen Kommunikationsnetze, sogenannte »Corporate Networks«, auf.

Cracker

→Hacker, der unbefugt in fremde Computersysteme eindringt und gespeicherte Daten und Programme in böser Absicht manipuliert oder inspiziert: also mit krimineller Energie bzw. für persönlichen Vorteil.

CRL

= Certification Revocation Lists; Schwarze Liste von Zertifikaten (Benutzern), die in einem →TrustCenter geführt wird.

Daemon

Ein UNIX-Prozess, der im Hintergrund abläuft und nur bei Bedarf aktiviert wird. Typische Daemons sind z. B. ftpd (→ftp-Daemon) und httpd (→http-Daemon).

DECNET

Von Digital Equipment Corporation (DEC) entwickelte und verwendete Kommunikationsarchitektur für Rechnersysteme.

Denial of Service

Denial of Service bedeutet soviel wie Funktionsausfall oder Funktionsverweigerung. Dahinter verbirgt sich eine Vielzahl verschiedener Angriffsmöglichkeiten, die alle das Ziel haben, Internetrechner zum Absturz zu bringen oder in bestimmten Funktionen lahmzulegen. Klassische Beispiele sind das Mail-Bombing – das geplante Überlasten eines Mail-Empfängers mit einer Unzahl von E-Mails – oder das Versenden von »Nukes«, das sind IP-Pakete, die ungesicherte Betriebssysteme kurzerhand zum Absturz bringen.

DENIC

= Deutsches Network Information Center; Sitz in Karlsruhe; unter anderem für die Vergabe von →Domain-Namen mit der Endung ».de« zuständig, siehe auch: www.denic.de

DES

= Data Encryption Standard; eines der bekanntesten und am meisten verbreiteten und untersuchten symmetrischen Verschlüsselungsverfahren. Der DES wurde 1976 in den USA normiert (ANSI X3.92). Der DES-Algorithmus hat ursprünglich eine Länge von 64 Bit, wovon 56 signifikant sind. Der DES-Algorithmus wird heute meist als Triple-DES mit 128-Bit →effektiver Schlüssellänge verwendet.

DFN

= Deutsches Forschungsnetz; Der DFN-Verein war am Aufbau des deutschen Wissenschaftsnetzes →WIN beteiligt und unterstützt das →CERT in Deutschland (DFN-CERT).

Diffie-Hellman

Verfahren zum Austausch eines geheimen Schlüssels über öffentliche Netzwerke

Digitale Signatur

Die Digitale Signatur garantiert den Ursprung einer Software, einer Nachricht oder sonstiger Daten. Die Digitale Signatur entspricht also einer eigenhändigen Unterschrift, die den Absender eindeutig identifiziert sowie sicherstellt, daß die empfangenen Daten nicht verfälscht wurden. Technisch basiert die Digitale Signatur auf der →asymmetrischen Verschlüsselung, d. h. dem Public-Key-Verfahren.

Digitales Zertifikat

Wer remote seine Identität nachweisen möchte – etwa durch eine Chipkarte und Eingabe einer PIN –, beruft sich damit auf eine Instanz, die dokumentiert, daß mit dieser Chipkarte und PIN auch genau diese Person verbunden ist. Diese Instanz –

Zertifizierungsinstanz bzw. →Certification Authority (CA) – bürgt für die Authentizität des Kartenbesitzers und dokumentiert diese durch ein Zertifikat. Dieses Zertifikat – in digitaler Form – dient Organisationen, die remote access zulassen, als 'Ausweis' für den User.

DMZ

= De-Militarised Zone; ein entkoppeltes, isoliertes Teilnetzwerk, das zwischen das zu schützende Netz und das unsichere Netz geschaltet wird.

DNS

= Domain Name Service; Internet-Dienst, mit dessen Hilfe die→IP-Adressen der Hosts den entsprechenden →Domainnamen und umgekehrt zugeordnet werden können. Sogenannte DNS-Server verwalten die Datenbanken mit den Adressen.

Domainnamen

Untergliederungseinheit der hierarchisch aufgebauten und weltweit eindeutigen Namen von Rechnersystemen im Internet. Die Domainnamen müssen bei den zugehörigen Verwaltungsstellen (→NIC, →DENIC) beantragt werden.

DSA

= Digital Signatur Algorithm, staatlichen Signaturverfahren in den USA, arbeitet u. a. mit dem Algorithmus →ElGamal

E-Business

= Electronic Business, Abwicklung von Geschäftsvorgängen über elektronische Medien wie das Internet

E-Commerce

= Electronic Commerce; umfaßt im Prinzip alle Schritte von Geschäftsprozessen, die auf elektronischem Wege vollzogen werden. Im Mittelpunkt stehen dabei zunächst die Möglichkeiten, sich online über Produktangebote zu informieren und Bestellungen vorzunehmen. Aber auch die Zahlung vom heimischen PC aus – Online Banking – wird bald zum E-Commerce-Alltag gehören. Und bei Zahlungen gilt noch mehr als bei Bestellungen: es muß sichergestellt sein, daß der Auftraggeber eindeutig identifizierbar ist und daß kein Unbefugter in die Transaktionen Einblick erhält.

Effektive Schlüssellänge

Werden Verschlüsselungsverfahren mehrfach durchlaufen, kann man nicht einfach die Schlüssellänge multiplizieren. Die Kryptologen haben deshalb den Begriff »effektive Schlüssellänge« eingeführt. Beispiel Triple-DES: Bei dreimaligem

Durchlauf mit je 56-Bit Schlüssellänge entspricht die Sicherheit des Verfahrens nicht etwa einer einmaligen Verschlüsselung mit der Schlüssellänge von 3 * 56-Bit = 168 Bit, sondern ist mit 128 effektiver Schlüssellänge geringer.

ElGamal

→asymmetrisches Verschlüsselungsverfahren

E-Mail

Elektronische Post; Austausch von Textnachrichten und Computerdateien über ein Kommunikations-Netzwerk, z. B. lokales Netzwerk oder das →Internet.

Ethernet

Das Ethernet wurde ursprünglich von Xerox für die Verknüpfung von Minicomputern im Palo Alto Research Center entwickelt. Inzwischen ist Ethernet eine weit verbreitete Technik zum Vernetzen von Rechnern in einem →LAN.

Extranet

Extranet heißt der Informationsaustausch zwischen →Intranets von Geschäftspartnern via →Internet (→TCP/IP basierend).

Finger

Internet-Dienst zur Ermittlung und zur Verwaltung der Benutzerinformationen eines Rechnersystems. Die dazugehörige Software ist standardmäßig Bestandteil jedes UNIX-Betriebssystems.

FTP

= File Transfer Protocol; Internet-Dienst zur Übertragung von Dateien

Gateway

Mit Gateway bezeichnet man die Verbindung zwischen zwei Netzen oder Teilnetzen, z. B. das »Tor«, durch das Daten aus dem →Internet in ein lokales Netz gelangen. Gateways arbeiten auf Schicht 7 des ISO/OSI-Modells und können zwei oder mehr Netze mit völlig verschiedenen Protokollen verbinden. Für die Informationssicherheit ist das Gateway der neuralgische Punkt – hier installiert man eine →Firewall, um aus dem Gateway ein →»Secure Gateway« zu machen.

GDD

= Gesellschaft für Datenschutz und Datensicherheit

Gopher

Internet-Dienst, der Textinformationen in Form von hierarchisch verschachtelten Auswahlmenüs strukturiert.

GSM

= Global System for Mobile Communications; Standard für digitale Mobilfunknetze.

Hacker

Als Hacker werden allgemein Anwender bezeichnet, die sehr vielfältige Kenntnisse im Umgang mit der Computertechnologie und Computerprogrammierung besitzen und sich oft damit beschäftigen. Der Begriff wird auch häufig für Personen verwendet, die sich unbefugten Zugang zu fremden Computersystemen verschaffen. Das Hacking sollte man aber keinesfalls mit Computersabotage, Computerspionage oder Computerbetrug gleichsetzen. Viele Hacker arbeiten aus sportlichen oder wissenschaftlichen Motiven und machen ihre Erkenntnisse der Öffentlichkeit zugänglich, was der Entwicklung von Sicherheitsmechanismen zugute kommen kann. Im Gegensatz zum →Cracker »arbeiten« Hacker also ohne kriminelle Energie bzw. nicht für persönlichen Vorteil.

Hacking

→Hacker

HMAC

Algorithmus, der eine →One-Way-Hashfunktion mit Verschlüsselung kombiniert und so eine digitale Signatur eines Dokumentes erzeugt

HTML

= HyperText Markup Language; Seitenbeschreibungssprache, mit der Elemente (Texte, Grafiken, →Hyperlinks, etc.) der Web-Seiten einfach formatiert werden können. HTML ist das derzeit wichtigste im WWW verwendete Dateiformat.

HTTP

= HyperText Transfer Protocol; Internet-Dienst, mit dem Daten zwischen →Web-Server und →Web-Browser ausgetauscht werden.

Hyperlink

Ein mit Hilfe von →HTML markierter Querverweis in einer Web-Seite auf eine Informationsquelle (→URL) im World Wide Web. Durch Aktivierung eines Hyperlinks z. B. per Mausklick wird der Benutzer zu dieser Quelle geführt, wobei er von →Web-Server zu Web-Server geleitet werden kann.

ICMP

= Internet Control Message Protocol; Ein Internet-Protokoll der Netzwerkschicht, welches eine Fehlerkorrektur und andere Informationen liefert, die für die IP-Paketverarbeitung von Bedeutung sind.

IDEA

= International Data Encryption Algorithm; 1990 von Lai und Massey als Alternative zum →DES vorgestelltes →symmetrisches Verschlüsselungsverfahren mit 128 Bit Schlüssellänge.

IKE

= Internet-Key-Exchange, Verfahren zum Austausch von Schlüsseln, Standardverfahren für →IPSec

Internet

Das Internet ist ein weltweites, dezentrales Rechnernetz, das auf dem →TCP/IP-Protokoll basiert. Das Internet ist inzwischen das populärste Netz der Welt mit über 350 Millionen Anwendern (Stand: 2/2001). Es bietet seinen Benutzern zahlreiche Dienste an, wie z. B. →FTP, →E-Mail, →World Wide Web, →Gopher.

Intranet

Internes Netz einer Organisation oder eines Unternehmens, das auf der Internet-Technologie und dem →TCP/IP-Protokoll basiert.

IP

= Internet Protocol; Dieses Netzwerkprotokoll definiert den Aufbau und die Adressierung von Datenpaketen in TCP/IP-Netzwerken.

IP Spoofing

Das Einfügen einer falschen IP-Absenderadresse in eine Internet-Übertragung. Das Ziel dieser Aktion ist der unberechtigte Zugriff auf ein Computersystem.

IP-Adresse

Weltweit eindeutige Adresse eines am Internet angeschlossenen Rechnersystems. Die IP-Adresse besteht aus einem Zahlencode von vier Zahlen von 0 bis 255 (z. B. 192.168.1.2). Die Vergabe erfolgt international vom →NIC bzw. in Deutschland vom →DENIC.

IPRA

= Internet Policy Registration Authority

IPSec

Verfahren zur Erweiterung der normalen →IP-Pakete um →Authentikation und Verschlüsselung, zukünftiger Standard

IPv6

= Internet Protocol Version 6; erweiterte Version des Internet-Protokolls mit vergrößertem Adressraum sowie Funktionen für Sicherheit.

IPX

= Internetwork Packet Exchange; von Novell verwendetes Netzwerkprotokoll. Im Schichtenmodell (→OSI-Modell) ist IPX auf der gleichen Ebene wie das IP einzuordnen.

ISDN

= Integrated Services Digital Network; weltweites digitales Kommunikationsnetzwerk zur integrierten Übertragung von Sprache und Daten.

ISO

= International Organization for Standardization; internationale Vereinigung, in der jedes Mitgliedsland durch die führende Standardisierungsorganisation vertreten ist. Die ISO arbeitet an der weltweiten Vereinheitlichung technischer Standards, u. a. auf den Gebieten der Kommunikation und des Informationsaustausches. Hier ist an erster Stelle das weithin akzeptierte →OSI-Modell zu nennen.

ISS

= Internet Security Systems; amerikanischer Hersteller des Firewall-, Intranet- und Web-Security-Scanners. Die Scanner testen Rechnersysteme auf Schwachstellen, indem sie bekanntgewordene Internet-Angriffe ausführen.

IT

= Information Technology

ITSEC

= Information Technology Security Evaluation Criteria; von Frankreich, Deutschland, Großbritannien und den Niederlanden festgelegte Kriterien für die Zertifizierung von IT-Systemen.

Java

Von Sun Microsystems entwickelte plattformunabhängige Programmiersprache für das Internet. Java-Programme (→Applets) werden von einem →Web-Server auf das lokale Rechnersystem übertragen und dort von einem Java-Interpreter ausgeführt.

Java-Applet

→Applet

JavaScript

Von Netscape definierte und in die HTML-Syntax integrierte Skriptsprache. JavaScript-fähige →Web-Browser interpretieren den in einer Web-Seite enthaltenen Programmcode und führen ihn aus.

Kompromittierung

Kompromittierung ist ein allgemeiner Oberbegriff für alle Formen der Vertraulichkeitsverletzung.

Kryptoanalyse

Ziel der Kryptoanalyse ist die Entschlüsselung von Geheimschriften und Codes. Im Bereich des elektronischen Datenverkehrs kann man Kryptoanalyse als eine Form von →Hacking bezeichnen.

Kryptogesetz

Das sogenannte Kryptogesetz definiert, unter welchen Bedingungen ein kryptographisches Verfahren zur →Verschlüsselung und Signatur von →E-Mails als so sicher gilt, daß der so übermittelte Inhalt rechtsverbindlichen Charakter hat wie ein Dokument auf Papier. Das deutsche Gesetz hierzu hat Pioniercharakter.

Kryptographie

Kryptographie ist der Zweig der →Kryptologie, der sich gezielt mit der Entwicklung von Verschlüsselungs- und Codierungsverfahren befaßt. Diese Wissenschaft ist sehr alt – schon im alten Ägypten beschäftigte man sich mit Geheimschriften. Heute geht es dagegen vorwiegend um mathematische Verschlüsselungsverfahren für den elektronischen Datenverkehr. Auch die →digitale Signatur beruht auf kryptographischen Verfahren.

Kryptographischer Algorithmus

Jedes kryptographische Verfahren beruht darauf, einen verständlichen Text nach bestimmten Regeln in unverständlichen Zeichensalat zu verwandeln. Bei elektro-

nischer Verschlüsselung geschieht dies nach einem bestimmten Algorithmus, wobei die Länge des Algorithmus beeinflußt, wie schwer →Hacker den Text entschlüsseln können. Zur Zeit gelten Schlüssellängen von 128 Bit als sicher.

Kryptographisches Protokoll

Die auf Algorithmen basierenden Verschlüsselungsverfahren müssen in die technologischen Gegebenheiten der Datenkommunikationsstrukturen eingebunden werden – dafür sorgt ein kryptographisches Protokoll.

Kryptologie

Oberbegriff für →Kryptographie und →Kryptoanalyse

Kryptoregulierung

Kryptoregulierung ist der staatliche Versuch, die Verbreitung und Verwendung leistungsfähiger Verschlüsselungsverfahren einzuschränken. Grund: Die Behörden fürchten, daß zu raffinierte Verfahren die Möglichkeiten zur Verbrechensbekämpfung beschneiden könnten. Die USA leiden unter sehr strikter Kryptoregulierung; in Deutschland konnte ein solches Gesetz verhindert werden.

LAN

= Local Area Network – auf deutsch auch: lokales Netz. Darunter fallen Netzwerke, die einen relativ kleinen, abgegrenzten Bereich umfassen – im Gegensatz zum →WAN.

LDAP

= Lightweight Directory Access Protocol, Protokoll zum Zugriff auf →Verzeichnis-Dienste

MAC

= Media Access Control; Protokoll der Netzzugangsebene

oder

= Message Authentication Code; →One-Way-Hashfunktion

Mailbombe

die unerwünschte Zusendung einer großen Menge von E-Mails (oder einer einzelnen sehr großen E-Mail) an einen bestimmten Empfänger oder eine Gruppe von Empfängern mit dem Ziel, den empfangenden Mailserver (bzw. ein Postfach) zu blockieren

Mailbox

elektronischer Briefkasten; Rechnersystem, das per →Modem angewählt wird und auf dem ein Programm läuft, das dem Benutzer erlaubt, Nachrichten anderer Benutzer zu lesen oder ihnen zu schreiben. Meist besteht zusätzlich die Möglichkeit, Dateien herunter- oder heraufzuladen. (siehe auch →E-Mail)

MailTrusT

Ein →TeleTrusT Projekt, in dem die Interoperabilität vielfältiger technologischer Komponenten und Produkte, die die Anwendung der →digitalen Signatur ermöglichen, durch kompatible Ausführung von Verschlüsselung und gemeinsamer Schnittstelle erreicht wurde.

Malware

Eine besondere Gefahr beim Austausch von Dateien als Anhänge von Mails oder WWW-Dokumenten, ist die Gefahr, daß neben der eigentlichen Information (Daten, Programme) sogenannte Malware (Viren, Würmer, Trojanische Pferde, ...) mitgesendet wird, die im Prinzip immer den Empfänger Schaden soll.

MAZ

Größter deutscher Internet-Provider, Sitz in Hamburg.

M-Business

= Mobile Business, Abwicklung geschäftlicher Vorgänge über Mobiltelefone

M-Commerce

= Mobile Commerce, Handel über elektronische Medien (Internet) unter Einbeziehung von Mobiltetefonen

MD4

→One-Way-Hashfunktion, wird häufig im Microsoft-Umfeld eingesetzt

MD5

Von Rivest entwickelte →One-Way-Hashfunktion zur Unterstützung von Authentikationsverfahren.

Mime

= Multipurpose Internet Mail Standard. Standard zum Verschicken von Multimediadateien bei E-Mails.

Modem

= Modulator/Demodulator; Ein Gerät, das den Austausch von Daten über Drahtleitungen ermöglicht. Die klassische Verwendung nutzt die konventionelle Telefonleitung, um sich ans →Internet anzuschließen und →E-Mails zu verschicken. Es gibt aber auch Modems für ISDN-Leitungen, Fernsehkabel, Stromleitungen, Standleitungen usw.

Modulation

Manche Datenleitungen, etwa die analoge Telefonleitung, werden durch einen ständigen Stromfluß aufrechterhalten – das sogenannte Trägersignal. Die eigentliche Informationsübermittlung geschieht durch geringfügige Schwankungen oder sonstige Veränderungen, also durch Modulation des Trägersignals.

MTA

= Message Transport Agent; Programm, das für die Annahme und Weiterleitung von →E-Mails verantwortlich ist.

Multiplexverfahren

Technik, die es ermöglicht, mehrere separate Signale über eine einzelne Leitung zu übertragen.

Nameserver

→DNS

NCSA

= National Computer Security Association; Verein von Anwendern und Hard- und Softwareherstellern mit dem Ziel, Benutzern bei der Erhöhung der Sicherheit, der Wahrung der Integrität ihrer Informationen und der Reduzierung der Bedrohungen durch Computer-Viren zu unterstützen. NCSA entwickelte Kriterien für die Zertifizierung von Firewall-Systemen.

Netz

Netz oder Netzwerk nennt man eine Gruppe von Computern und angeschlossenen Geräten, die durch Kommunikationseinrichtungen miteinander verbunden sind. Die Netzwerkverbindungen können permanent (zum Beispiel über ein Kabel) oder zeitweilig (etwa über das Telefon oder andere Kommunikationsverbindungen) eingerichtet werden und verschiedene Größenordnungen und Ausdehnungen haben.

NMS

= Network Management System

NNTP

= Network News Transport Protocol; Internet-Dienst, mit dem die News-Artikel transportiert werden.

One-Way-Hashfunktion

Auf eine Nachricht, deren Länge variabel ist, wird eine sogenannte One-Way-Hashfunktion angewendet, die eine kryptographische Prüfsumme fester Länge als Ergebnis erzeugt (z. B. →MD5).

OSI

= Open Systems Interconnection

OSI-Schichtenmodell

auch OSI-Referenzmodell genannt; ein von der →ISO entwickeltes Kommunikationsprotokoll, das allgemeine Regeln für die Kommunikation in Netzwerken enthält.

OTP

= One-Time-Password (Einmal-Passwort); das Konzept »Einmal-Passwort« legt fest, daß ein Passwort nur einmal für eine Authentikation verwendet werden darf.

Passwort

Das einfachste Authentikationsverfahren ist das Passwort-Verfahren. Die Stärke dieses Verfahrens beruht allerdings lediglich auf der Geheimhaltung und der Qualität (Länge/Nichttrivialität) des Passwortes.

PEM

= Privacy Enhanced Mail; in den →RFCs 1421-1424 festgelegter Standard für die Verschlüsselung und Authentizität von →E-Mails.

PGP

= Pretty Good Privacy; ein von Phil Zimmerman entwickeltes Verschlüsselungsverfahren, welches auf →RSA und →IDEA basiert.

Phreaker

Personen, die in Telefonleitungen, Anrufbeantwortern und →Voiceboxen ihr Unwesen treiben.

PIN

= Personal Identification Number; eine Codenummer, die einem berechtigtem Benutzer zugewiesen ist.

PKI

= Public Key Infrastructure, Infrastruktur zur Erstellung und Verwaltung von Schlüsselpaaren und →Zertifikaten

POP3

= Post Office Protocol; Standard zur Übermittlung von →E-Mails.

PPP

= Point to Point Protocol; wird zum Austausch von Datenpaketen per →Modem im →Internet verwendet. Das PPP liegt eine Ebene unter →TCP/IP und kümmert sich nur um die serielle Datenübertragung und ihren Aufbau.

PPTP

Point-to-Point Tunneling Protocol, VPN-Protokoll im Microsoft-Umfeld

Private-Key-Verfahren

→Symmetrisches Verschlüsselungsverfahren

Proxy

Ein Proxy ist ein Stellvertreter des →Servers gegenüber dem Client und ein Stellvertreter des Client gegenüber dem Server. Nach der →Authentikation des Clients bzw. des Servers gegenüber dem Proxy arbeitet dieser für beide Seiten transparent. Proxies existieren für die Dienste →HTTP, →SMTP, →FTP, →Telnet u. a.

Public-Key-Verfahren

→Asymmetrisches Verschlüsselungsverfahren

RC4 / RC5

→Symmetrisches Verschlüsselungsverfahren

Registration Authority

Bestandteil einer →PKI, untergeordnete Institution, die einer →Certification Authority einen Teil der Routineaufgaben abnimmt

Remote access

Mit Remote access wird die Möglichkeit bezeichnet, aus räumlicher Distanz über ein öffentliches Netz Zugang zu einem Rechnersystem oder lokalem Netz zu erhalten und dort agieren zu können. Da Remote access-Verbindungen von Natur aus ein besonders großes Risiko bedeuten, müssen Sicherheitsvorkehrungen getroffen werden, um Authentizität und Vertraulichkeit zu garantieren. Mit Verschlüsselungs- und Zugangskontrollsystemen kann Remote Access gesichert werden.

RFC

= Request for Comment; Textdokumente, die Vorschläge für neue Internet-Standards zusammenfassen.

Rijndael

→symmetrisches Verschlüsselungsverfahren mit einer für die nächsten Jahrzehnte ausreichenden Schlüssellänge, soll das weit verbreitete →DES ablösen

RIP

= Routing Information Protocol; →Router

Router

Router sind Geräte zur Kopplung verschiedener Netze. Sie leiten Datenpakete auf der günstigsten Route »durch das Gewirr der Netzwerke« zu ihrem Ziel. Dabei arbeiten sie meistens auf Schicht 3 des ISO/OSI-Referenzmodells.

RSA

→Asymmetrisches Verschlüsselungsverfahren, benannt nach den Entwicklern Rivest, Shamir und Adleman. Das bekannteste, bewährteste und am besten untersuchte asymmetrische Verfahren.

S/MIME

= Secure Multipurpose Internet Mail Standard.

Um Mechanismen zur Authetication, Verschlüsselung und Signatur erweiterter →MIME Standard

SATAN

= System Administrator Tool for Analyzing Networks; ein Programm zur Überprüfung von IP-Netzwerken. Getestet werden dabei Schwachstellen, die ein Angreifer über das Internet ausnutzen kann, um sich unbefugt Zugang zu einem Rechnersystem zu verschaffen.

Secure Gateway

→Gateway nennt man den Zugang, der ein lokales Netz mit einem öffentlichen Netz verbindet. Wenn der Betreiber des lokalen Netzes kontrollieren will, wer wann unter welchen Bedingungen Zugang zu welchen Diensten erhalten soll, richtet er durch Sicherheitsmaßnahmen einen Secure Gateway ein. Ein Secure Gateway muß v.a. in der Lage sein, die Authentizität von Besuchern zu überprüfen und entsprechende Zugangsrechte zu differenzieren. Größtmögliche Sicherheit bietet hier ein High-level-Firewall-System.

Secure Shell

Telnet-ähnliches Protokoll, das innerhalb von Unix-VPNs Anwendung findet

Security Policy

Eine wohldurchdachte Security Policy bildet die Grundlage für die Sicherheit in Organisationen. Dazu zählen die Definition von Sicherheitszielen, die Bestimmung des Schutzbedarfs der Daten, die Analyse der Kommunikationsstrukturen und anderes mehr. Erst auf dieser Basis können konkrete Sicherheitsmaßnahmen geplant und durchgeführt werden.

Security Token

Ein Security Token ist ein Datenträger (z. B. Chipkarte oder Diskette), mit dem der User seine Zugangsberechtigung nachweisen kann, wenn er die richtige →PIN kennt. Die →Authentikation funktioniert nach dem Challenge-Response-Prinzip: Das Firewall-System, das den Zugriff gewähren kann, stellt eine Challenge, auf die der Security Token eine Response schickt und damit den User authentifiziert.

Server

Ein Server ist ein Rechner innerhalb eines lokalen Netzes, der den anderen Rechnern seines Netzes Informationen zur Verfügung stellt.

SET

= Secure Electronic Transaction, Protkoll aus dem Bereich des →E-Commerce, erlaubt das Bezahlen von Waren und Dienstleistungen über das Internet

SHA

= Secure Hash Algorithm, oft auch SHA-1 genannt, →One-Way-Hashfunktion

S-HTTP

= Secure HTTP; um Kryptographiefunktionen erweiterte Version des Protokolls →HTTP.

SKIP

= Simple Key Management for Internet Protocols, Protokoll zum Schlüsselaustausch, wird beim Einsatz von →IPSec wahlweise anstelle des üblichen →IKE verwendet

SMIB

= Security Management Information Base

SMTP

= Simple Mail Transport Protocol; Internet-Dienst zur Übertragung von →EMails.

SNA

= Systems Network Architecture; von IBM entwickelte und verwendete Kommunikationsarchitektur für Rechnersysteme.

SSL

= Secure Socket Layer; Protokollschicht zum sicheren Transport von höheren Internetprotokollen wie →HTTP.

Symmetrische Verschlüsselung

auch Private-Key-Verfahren genannt; Verschlüsselungsverfahren, bei dem für die Verschlüsselung der Daten der gleiche Schlüssel verwendet wird wie für ihre Entschlüsselung. Die bekanntesten symmetrischen Verschlüsselungsverfahren sind →DES, →AES und →IDEA.

TCP

= Transmission Control Protocol; das Protokoll innerhalb des →TCP/IP, das die Trennung der Datennachrichten in Pakete steuert und die empfangsseitige Zusammensetzung und Überprüfung auf Vollständigkeit der Datenpakete überwacht.

TCP/IP

= Transmission Control Protocol/Internet Protocol; Kommunikations-Architektur im Internet/Intranet. →TCP, →IP

TeleTrusT e.V.

TeleTrusT e.V. – siehe: www.teletrust.de – wurde 1989 gegründet, und hat sich die Förderung von Wissenschaft, Normung und Bildung im Bereich der Entwicklung einer verläßlichen Informations- und Kommunikationstechnik zum Ziel gesetzt.

Im TeleTrusT arbeiten Forschung, Anbieter, Organisationen und Behörden zusammen. Der TeleTrusT war an der Formulierung des deutschen Signaturgesetzes beratend mitbeteiligt.

Trojanisches Pferd

ein unverdächtig erscheinendes Programm, das im Hintergrund vor dem Benutzer verborgene und von diesem unerwünschte Funktionen ausführt, z. B. eine →Backdoor öffnet, gespeicherte Daten verändert oder vertrauliche Informationen sammelt und an einen Server schickt.
Die Bezeichnung »Trojanisches Pferd« geht auf Homers Odyssee zurück: Nachdem die Griechen Troja lange erfolglos belagert hatten, ließen sie ein hölzernes Pferd vor den Stadtmauern zurück, in dem sich ihre tapfersten Soldaten versteckten. Die Trojaner holten das Pferd in die Stadt, in der Nacht öffneten die versteckten Krieger ihren Mitstreitern die Tore und Troja wurde verwüstet.

TrustCenter

→CA

UDP

= User Datagram Protocol; ein verbindungsloses Übertragungsprotokoll für das Internet. Im Gegensatz zum →TCP/IP findet bei diesem Protokoll keine Überprüfung der ordnungsgemäßen Zustellung von Datennachrichten statt.

URL

= Uniform Resource Locator; ein URL bezeichnet die eindeutige Adresse eines Internet-Servers bzw. einer bestimmten Information darauf. Er beinhaltet Angaben wie Typ der Ressource, mit der verbunden werden soll (z. B. →WWW, →FTP, →Gopher), Serveradresse, Portnummer, etc. Ein URL wird im →Browser eingegeben oder durch einen →Hyperlink aktiviert.

USV

= Unterbrechungsfreie Stromversorgung; wird an hochverfügbaren Rechnersystemen eingesetzt, um den Ausfall der Stromversorgung zu überbrücken oder die Stromversorgung solange zu gewährleisten, bis die Rechnersysteme kontrolliert heruntergefahren worden sind.

Verschlüsselung

Informationen werden verschlüsselt, um sie gegen unberechtigte Einblicke oder Verwendung zu schützen. Verschlüsselungsverfahren beruhen auf komplexen mathematischen Berechnungen (Algorithmen), wobei die Länge der Schlüssel und die Qualität des Algorithmus maßgeblich für die Sicherheit sind.

Verzeichnis-Dienst

Bestandteil einer →PKI, enthält frei definierbare Datenstrukturen und ein Protokoll zum Zugriff auf diese

Viren

Programme, die sich selbst unbemerkt in andere Programme kopieren und zu einem definierten Zeitpunkt meist zerstörerische Aktivitäten ausführen.

Voicebox

Rechnersystem für Teilnehmer in Mobilfunknetzen, das wie ein Anrufbeantworter Nachrichten aufzeichnet.

VPN

= Virtual Private Network; logisches Netz innerhalb eines konventionellen Netzes, in dem nur verschlüsselte Verbindungen zwischen einzelnen Rechnersystemen oder Teilnetzen zugelassen werden. Durch die Verschlüsselung geschieht die Kommunikation über das öffentliche Netz vertraulich, so daß die Verbindung quasi privat (virtual private) stattfindet.

W3C

= World Wide Web Consortium; Organisation zur Koordinierung der weiteren Entwicklung des →WWW durch Erarbeitung von Spezifikationen und Referenzsoftware.

WAN

= Wide Area Network. Darunter versteht man offene, weiträumige Netze – z. B. ISDN, X.25.

WAP

= Wireless Application Protocol, »Netzwerkstack« für Mobiltelefone

Web-Server

Rechnersystem, das den auf →HTTP basierenden Internet-Dienst →WWW zur Verfügung stellt.

WIN

= Wissenschaftsnetz; mit Hilfe des →DFN aufgebautes Datennetz, das alle wichtigen Universitäten und Forschungseinrichtungen Deutschlands miteinander verbindet.

WTLS

= Wireless Transport Layer Security, Ebene innerhalb des →WAP-Stacks, nimmt Sicherungsfunktionen wahr, an das Netzwerkprotokoll →SSL angelehnt

Würmer

Programmcodes, die sich – ähnlich wie Viren – selbsttätig in Netzwerken verbreiten; im Unterschied zu Viren integrieren Würmer sich jedoch nicht in andere Programme oder Dateien

WWW

= World Wide Web; die komplette Sammlung von Hypertext-Dokumenten, die auf HTTP-Servern weltweit abgelegt sind.

X.400

OSI-Standard für E-Mail-Systeme.

X.500

OSI-Standard für Benutzerverzeichnisse.

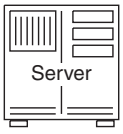
X.509

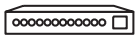
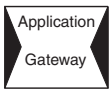
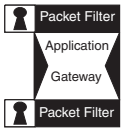
Weit verbreiteter Standard für →Zertifikate

Zertifikat

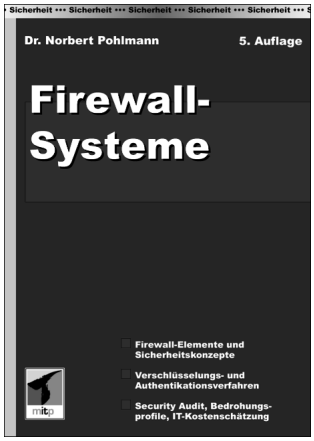
Datenstruktur, die eine Identifikation des Besitzers, seinen öffentlichen Schlüssel, ein Ablaufdatum und die digitale Signatur einer →Certification Authority enthält

Legende

Symbol	Bedeutung
	zu schützendes Netz mit hohem Schutzbedarf
	unsicheres Netz mit nicht abschätzbarem bzw. niedrigem Schutzbedarf
	Workstation, auf der TCP/IP-Applikationen laufen (Browser, Telnet-Client etc.)
	Workstation, auf der das Security Management realisiert ist
	Workstation mit VPN-Client
	Workstation, mit der ein Angriff durchgeführt wird
	Notebook, auf dem TCP-Anwendungen laufen
	Notebook mit VPN-Client
	Server-System, auf dem TCP-Anwendungen laufen (WWW-Server, FTP-Server, News-Server etc.)

Symbol	Bedeutung
	Modem
	Router
	allgemeines Symbol für Firewall-System
	Packet Filter
	VPN-Gateway
	Application Gateway
	High-level Security Firewall-System
	Virenscanner
	Intrusion Detection/Response-System
	Chipkartenleser mit Pin-Pad
	Security Token, der den Benutzern Sicherheitsfunktionen zur Verfügung stellt

Symbol	Bedeutung
	Benutzer
	Chipkarte, die den Benutzern Sicherheitsdienstleistungen zur Verfügung stellt (SmartCard)
	Mobiltelefon



ISBN 3-8266-0988-3
www.mitp.de

Dr. Norbert Pohlmann

Firewall-Systeme

Immer mehr Unternehmen und Behörden nutzen das Internet geschäftlich und koppeln ihre eigenen TCP/IP-basierten Intranets daran an. Die Sicherheit der internen und externen Kommunikation zu gewährleisten ist dabei eine unverzichtbare Aufgabe. Das nach wie vor wichtigste Instrument zum Schutz der Verbindung von Intranet und Internet sind Firewall-Systeme.

Dr. Norbert Pohlmann, international gefragter Experte für IT-Sicherheit, Vorstand der Utimaco Safeware AG und Vorsitzender des TeleTrusT e.V., beschreibt die verschiedenen Ansätze von Firewall-Systemen und zeigt ihre jeweiligen Einsatzmöglichkeiten auf. Damit gibt er den interessierten Lesern – Laien wie technisch versierten Spezialisten – praktische Hilfestellungen an die Hand, das richtige Firewall-System für ihren Anwendungszweck auszusuchen und zu betreiben.

Das Buch liegt jetzt in der fünften, aktualisierten und erweiterten Auflage vor und ist ein unverzichtbares Standardwerk für jeden geworden, der Verantwortung für IT-Sicherheit trägt oder an diesem Themenkomplex interessiert ist. Besonders bewährt haben sich der durchdachte Aufbau, die klare Sprache, die verständnisfördernden Analogien und die didaktisch wertvollen Illustrationen.

Aus dem Inhalt:

- Bedrohungsprofile
- Firewall-Elemente und -Konzepte
- E-Mail-Sicherheit
- Verschlüsselungs- und Authentikationsverfahren
- Public-Key-Infrastrukturen
- Anwendungsmöglichkeiten von Virtual Private Networks
- Intrusion Detection Systems und Personal Firewalls
- Das Security-Gateway-Konzept
- Security Audits
- Kostenschätzungen für die Anschaffung und den Betrieb von Firewall-Systemen
- Technische und rechtliche Grundlagen
- Fakten und Zahlen zur Computerkriminalität
- Themenrelevante Adressen und Web-Links
- Firewall-Produktübersicht, Sicherheitsstandards

Stichwortverzeichnis

ISBN 3-8266-0935-2
www.mitp.de

Franz-Joachim Kauffels

Durchblick im Netz, 5. Auflage

Kauffels wendet sich mit diesem jetzt in der fünften Auflage vorliegenden Buch an alle, die wissen wollen, wie Netze und Kommunikationstechnik funktionieren, und was man damit anfangen kann. Dem neugierigen Leser sollen die Spannbreite und Funktionsweise der heutigen Datenkommunikation vor Augen geführt werden, ohne dass er dabei allzusehr mit technischen Einzelheiten belastet wird.

Aus dem Inhalt:

- Vom Draht zum Downsizing
- Bauplan/Systemarchitektur von Netzen
- Wie Bits reisen
- PC-Netze, der große Erfolg
- Serverbetriebssysteme: NetWare, Windows , UNIX/Linux
- Integration der Netze und Dienste: ISDN, xDSL, ATM
- Internetworking: Bridging, Routing, Switching
- Entwicklung optischer Netze
- Wireless LANs / Drahtlose Netze
- TCP/IP, Internet, WWW
- GroupWare, Intranet
- Netzwerksicherheit, E-Commerce