Virtual Private Networks (VPN)

Autor:	**Dipl.-Ing. Norbert Pohlmann**
	Geschäftsführer KryptoKom GmbH
☎	0241-963-1380
🖷	0241-963-1390
E-Mail:	norbert.pohlmann@kryptokom.de
Internet:	www.kryptokom.de

KryptoKom

Inhaltsverzeichnis

1 Einleitung

Die moderne Informationstechnik arbeitet zunehmend mit verteilten Anwendungen. Das bedeutet, daß Daten an verschiedenen Orten erstellt oder bearbeitet werden, die man dann über Kommunikationsnetze austauscht. Diese Kommunikationstechniken bieten unübersehbare Vorteile in puncto Schnelligkeit, Performance 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 werden, während sie über öffentliche Netze (Kommunikationsinfrastrukturen) übertragen werden.
- Unbefugte können durch die Ankopplung an ein offenes Netz 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, weil niemand in der Lage ist unbefugt, auf die eigenen Rechnersysteme zugreifen.

Diese Sicherheitsmaßnahmen ermöglichen es, die Vorteile öffentlicher Kommunikationsinfrastrukturen zu nutzen, und bieten zugleich die Vertraulichkeit und Infomationssicherheit eines Privaten Netzwerkes. Man spricht daher von einem sogenannten **Virtual Private Network (VPN)**.

2 Veränderung von Geschäftsprozessen

Die meisten Geschäftsprozesse wurden in der Vergangenheit schriftlich auf Papier mit Hilfe der Post (z.B. Angebotserstellung, Auftragsannahme, Bestellung, Liefereingang usw.) oder durch persönlichen Kontakt abgewickelt.

Solche Abläufe werden heute mit Hilfe von modernen IT-Konzepten (Informationsverarbeitungs- und Telekommunikationsprozesse) wie z.B. Client/Server, Web-Systeme oder E-Mail-Austausch weitaus rationeller gestaltet. Der personelle und materielle Aufwand wird dabei größtenteils durch elektronische Verfahren ersetzt.

Moderne IT-Konzepte und IT-Sicherheit

Der Trend zu Internationalisierung und Globalisierung macht es für Unternehmen und Organisationen unverzichtbar, immer mehr Arbeitsprozesse über Netzwerke zu realisieren, wenn sie nicht auf Zeit- und Wettbewerbsvorteile verzichten wollen.

Dabei werden in der Regel preiswerte Kommunikationsinfrastrukturen, wie das Internet oder andere öffentlich angebotene IP-Backbones, genutzt. Technologische Weiterentwicklungen schaffen drastisch höhere Zugangsgeschwindigkeiten zu den öffentlichen Kommunikationsinfrastrukturen. Während ISDN im Duplexbetrieb schon bis zu 128 KB pro Sekunde ermöglicht, schafft die neue ADSL-Technik (Asymetric Digital Subscriber Line) bis zu 8 MB pro Sekunde und zwar mit dem konventionellen Telefonkabel, wie es “auf der letzten Meile” zwischen Vermittlungsstelle der Telekom und dem Teilnehmeranschluß verlegt ist.

Die neue Organisation von Arbeitsprozessen führt dazu, daß unsere Rechnersysteme und insbesondere der Zugriff auf die Informationen während der Übertragung für potentielle Angreifer immer attraktiver werden, je weiter Wert und Quantität der übertragenen Daten zunehmen. Zugleich kommt keine Organisation heute ohne die Veränderung der Geschäftsprozesse und die Vernetzung von Rechnersystemen aus. Die neuen Informationstechnologien können aber nur dann sinnvoll eingesetzt werden, wenn sie sicher und beherrschbar sind. Die Bedrohungen durch die neuen Arbeitsprozesse können wir kaum beeinflussen, sehr wohl aber unsere Verletzlichkeit. Voraussetzung dafür ist, daß wir angemessene Sicherheitsmechanismen einführen, um die Gefahren zu minimieren.

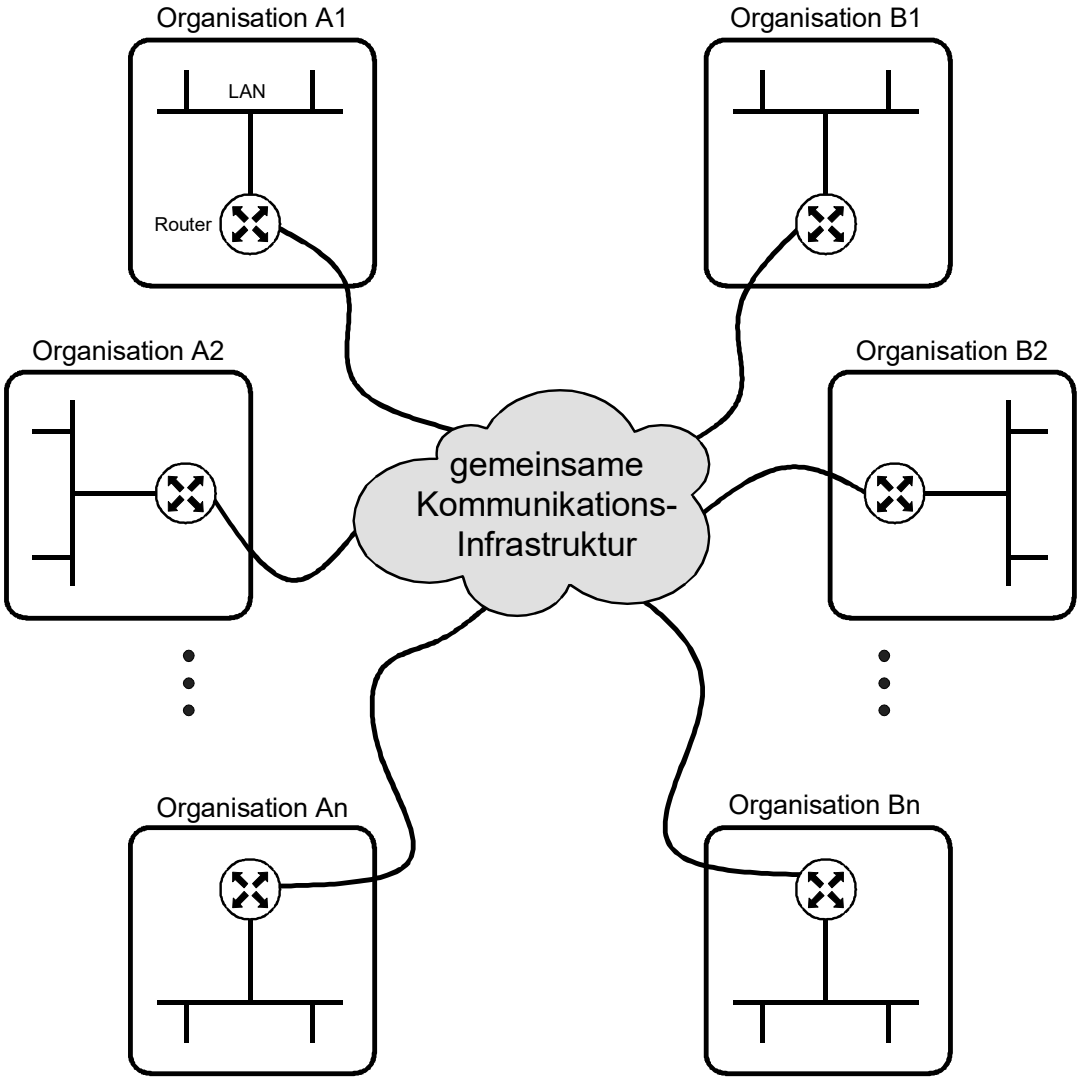

Abbildung 2.1 Kopplung von Organisationseinheiten über öffentliche Kommunikationsinfrastrukturen

3 Corporate Network versus öffentliche Kommunikations-infrastruktur

Es gibt zwei unterschiedliche Wege, um die Kommunikationsnotwendigkeiten einer Organisation zur realisieren:

1. Eine Organisation kann für die interne Kommunikation zwischen den einzelnen Organisationseinheiten ein **Corporate Network mit einer eigenen Kommunikationsinfrastruktur** aufbauen und die Kommunikation nach außen – zu Kunden, Lieferanten und Geschäftspartnern – über eine zentrale Stelle, die an eine öffentliche Kommunikationsinfrastruktur angebunden ist, realisieren.
2. Die gesamte Kommunikation – nach innen wie nach außen – wird über eine **öffentliche Kommunikationsinfrastruktur** realisiert. Dabei müssen jedoch geeignete Sicherheitsmechanismen eingebunden werden, die den zusätzlich entstehenden IT-Gefahren begegnen.

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

3.1 Corporate Network

Vorteile eines Corporate Network**:**

- völlige Freiheit bei der Gestaltung der eigenen Kommunikationsinfrastruktur, mit allen gewünschten (technisch realisierbaren) Features
- höhere Sicherheit und zugleich höhere Verfügbarkeit, denn die Kommunikationsinfrastruktur wird nur von der eigenen Organisation genutzt.
- die eigene Security Policy kann auf allen Ebenen eigenverantwortlich durchgesetzt werden

Nachteile:

- Investitionen, Betrieb und Wartung müssen selbst getragen werden
- neue Innovationen im IT-Bereich zwingen jeweils zu neuen Investitionen.

3.2 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
- flexible Kommunikation mit Kunden, Lieferanten und Geschäftspartnern
- der Anbieter ist verantwortlich für Quality of Service in puncto Verfügbarkeit, Performance und Management

Nachteile:

- der Anwender ist abhängig vom Anbieter und dessen Sicherheitsstrategie
- an die öffentliche Kommunikationsinfrastruktur sind auch andere Benutzer angeschlossen, die einen anderen Schutzbedarf haben
- die Security Policy des Anbieters ist nicht immer klar nachvollziehbar und überprüfbar

4 Risiken bei öffentlichen Kommunikationsinfrastrukturen

Die Nutzung der neuen IT-Konzepte über öffentliche Kommunikationsinfrastrukturen ist also in vieler Hinsicht attraktiv; wichtigster Nachteil aber ist die Sicherheitsfrage. Insbesondere sind folgende Risiken zu berücksichtigen:

4.1 Angriff auf die übertragenen Daten

Werden Informationen im Klartext über öffentliche Netze geschickt, kann ein Angreifer unmittelbar in den Besitz der Kommunikationsdaten gelangen und diese zu eigenen Zwecke nutzen. Der Angreifer setzt sich in den Informationsstand von Sender und Empfänger. Wenn er die abgefangenen Daten manipuliert und weiterschickt, kann er das Verhalten des Senders wie des Empfängers auch gezielt beeinflussen.

Die Angriffe lassen sich wie folgt einteilen:

- **Mitlesen von schützenswerten Informationen:**

  Die Informationen (Kommunikationsdaten) werden im Klartext übertragen, so daß sie von einem Lauscher mitgelesen und mißbräuchlich verwendet werden können (z.B. das Mitlesen von Entwicklungsunterlagen, Wirtschaftsspionage).

- **Manipulation von schützenswerten Informationen:**

  Ein Angreifer kann die Inhalte der Kommunikationsdaten verändern, ohne daß dies bemerkt wird (z.B. die Veränderung der Geldbeträge bei Überweisungen).

- **Löschen von schützenswerten Informationen:**

  Ein Angreifer kann Informationen, die für ein Unternehmen von großer Bedeutung sind, löschen (z.B. Verkäufe und Ankäufe von Aktien).

- **Verkehrsflußanalyse**

  Sogar wenn Daten verschlüsselt sind, ist es einem Abhörer u.U. möglich, durch Analyse des Verkehrsflusses gewisse Informationen zu erhalten, zum Beispiel Größenordnungen, Zeitpunkte, Häufigkeit und Richtung des Datentransfers. Diese Informationen können für bestimmte Zwecke interessant sein.

4.2 Zugriff auf Rechnersysteme über die Kommunikationsinfrastruktur

Die Kopplung an eine Kommunikationsinfrastruktur ist keine Einbahnstraße. Alle, die an die Kommunikationsinfrastruktur angeschlossen sind, können im Prinzip auf alle Rechnersysteme im Netz zugreifen.

Welche Gefahren sind damit verbunden?

- High-Tech-Spione stehlen fremdes Know-how oder Strategiepläne und verkaufen sie lukrativ an die Konkurrenz.
- Cracker dringen in das Netz von Firmen und Behörden ein und fälschen Daten oder schleusen falsche Informationen ein.
- Cracker können die Rechnersysteme einer Organisation lahmlegen und so wirtschaftlichen Schaden in Millionenhöhe verursachen.

Die folgende Abbildung zeigt, daß Angreifer, die Zugriff auf die öffentliche Kommunikationsinfrastruktur haben, auf die Kommunikationsdaten und auf die angeschlossenen Rechnersysteme zugreifen können, wenn keine Sicherheitsmaßnahmen getroffen werden.

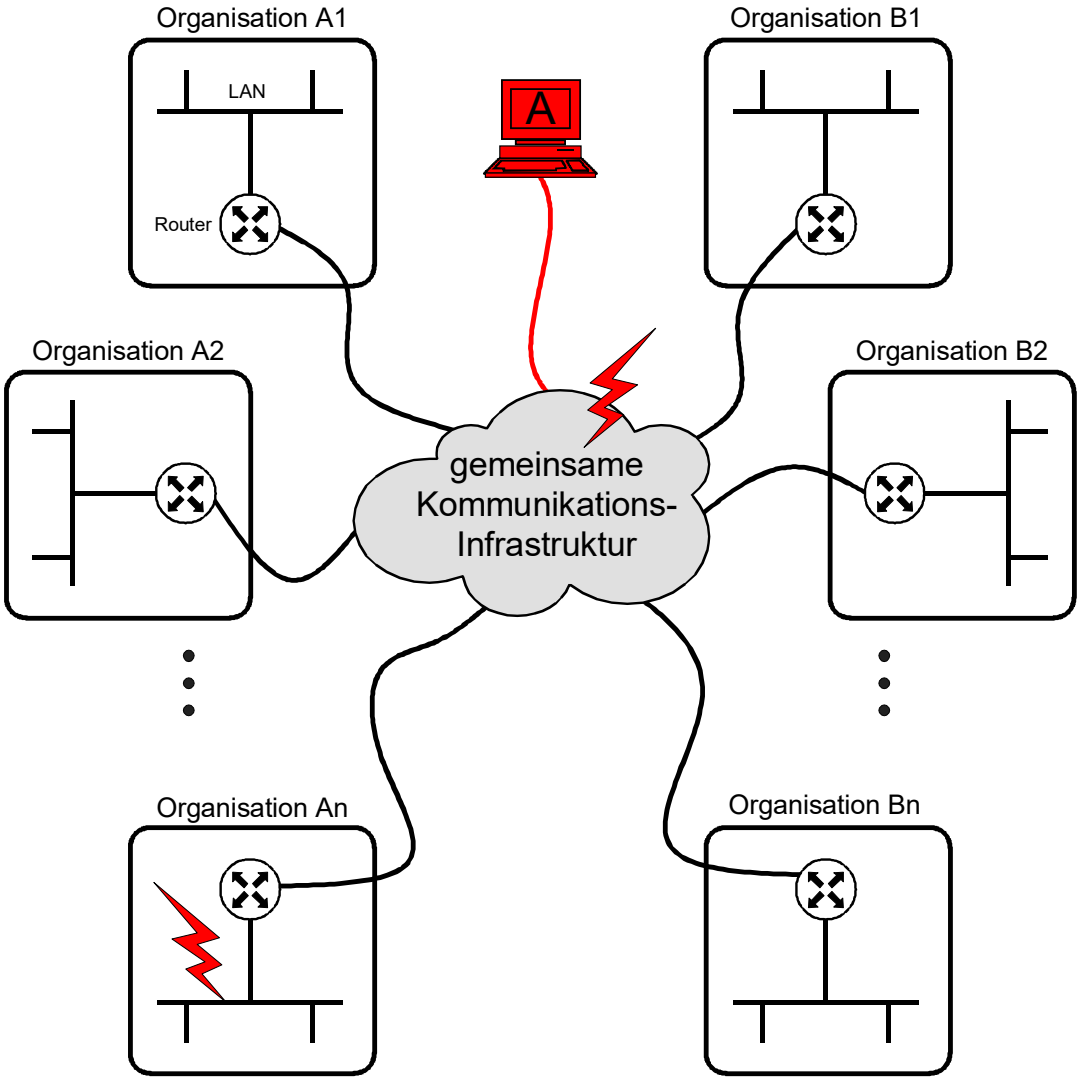

Abbildung 4.1 Risiken

5 Aufbau von Virtual Private Networks

Die grundsätzliche Idee bei Virtual Private Networks (VPNs) ist, die Vorteile einer offenen Kommunikationsinfrastruktur zu nutzen – z.B. die kostengünstige, weltweit verfügbare “shared infrastructure” des Internet – aber dabei allen Gefährdungen der Informationssicherheit sinnvoll entgegenzuwirken.

Ein VPN soll gewährleisten, daß sensible Daten während der Übertragung über Netzwerke (LANs und WANs) vertraulich übertragen werden, so daß nur die dazu berechtigten Personen auf die sensiblen Daten zugreifen können und keine Fremden in der Lage sind, auf die Rechnersysteme des eigenen Netzes unerlaubt zuzugreifen.

Damit diese Ziele erreicht werden, setzt man kryptographische Verfahren und andere Sicherheitskomponenten ein. Sicherheitsmechanismen von VPNs sind in der Regel:

- Verschlüsselung,
- Firewalling und
- Tunneling

5.1 Vertraulichkeit durch Verschlüsselung

Mit der Verschlüsselung der Kommunikationsdaten wird ein besonders wichtiger Teil der Sicherheitsanforderungen an ein VPN erbracht. Ohne Kenntnis des Schlüssels ist es Dritten nicht möglich, abgefangene Daten zu lesen oder unbemerkt zu manipulieren.

Die Verschlüsselung kann insbesondere im heterogenen Rechnerumfeld mit Hilfe von Black-Boxen einfach und transparent verwirklicht werden.

Als **Black-Box-Lösungen** bezeichnet man Hardware-Geräte, die auf einfache Weise zwischen Rechnersysteme und Netzanschluß (LAN-Anschluß) geschaltet werden. Das macht sie unabhängig von den jeweiligen Endgeräten und Betriebssystemen und wegen ihrer einfachen Handhabung benutzerfreundlich. In der High-Tech Black-Box geschehen alle sicherheits-relevanten Operationen – unsichtbar für den Benutzer und ohne daß er sie eigens veranlassen muß.

Vor jede Organisationseinheit, die über öffentliche Kommunikations-infrastrukturen gesichert kommunizieren möchte, wird dafür eine Black-Box geschaltet. In Zusammenarbeit mit einer entsprechenden Sicherheitseinrichtung

auf der Gegenseite sorgt sie für die kryptographische Sicherung der Kommunikation über die öffentliche Kommunikationsinfrastruktur hinweg.

Die folgende Abbildung zeigt, daß mit mehreren Black-Boxes gleichzeitig und unabhängig voneinander beliebig viele VPNs über eine öffentliche Kommunikationsinfrastruktur realisiert werden können.

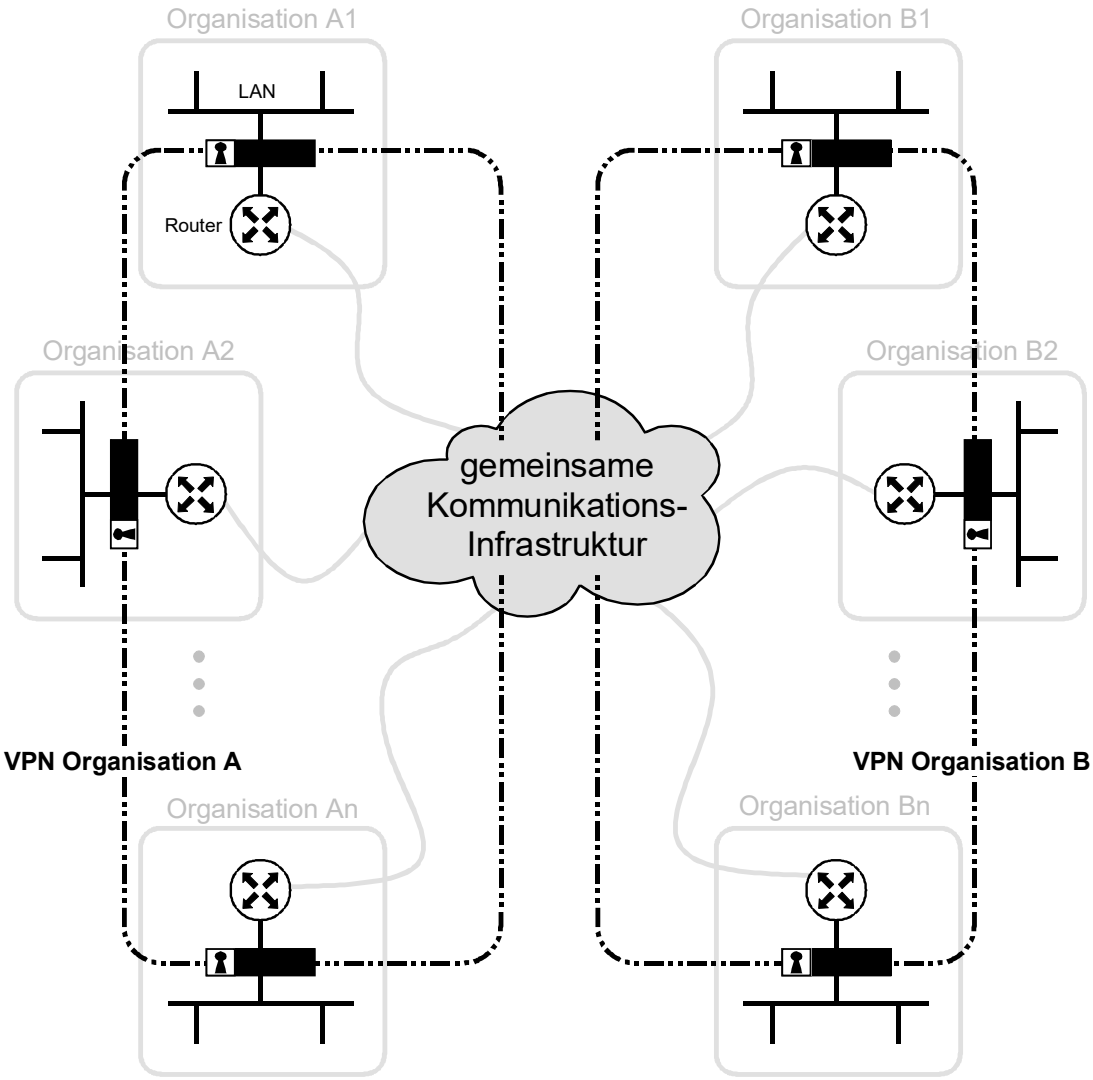

Abbildung 5.1 mehrere VPNs

5.2 Firewall-Systeme

Der Sicherheitsmechanismus Verschlüsselung wirkt nur gegen die unerlaubte Einsicht der Informationen während der Kommunikation. Zusätzlich muß noch mit Hilfe von Firewall-Systemen das zweite Hauptrisiko: der unerlaubte Zugriff auf die eigenen Rechnersysteme verhindert werden

Firewall-Systeme werden als Schranke zwischen ein zu schützendes Netz und ein unsicheres Netz geschaltet, so daß der gesamte Datenverkehr zwischen den beiden Netzen nur über das Firewall-System möglich ist.

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 wird und mit welchen Rechnersystemen kommuniziert werden darf.

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.

Ein Angreifer darf nicht in der Lage sein, die Firewall zu überwinden.

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 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 über das Firewall-System eine Kommunikation 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 Security Management 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 geheimzuhalten. Das Firewall-System schirmt die Struktur des zu schützenden Netzes nach außen hin ab. Es soll aus dem unsicheren Netz nicht sichtbar sein, ob im zu schützenden Netz 10, 100, 1.000 oder 10.000 Rechnersysteme vorhanden sind.

5.2.1 Aktive Firewall-Elemente

Bei Firewall-Elementen wird unterschieden zwischen Elementen, die aktiv in die Kommunikation zwischen dem zu schützenden und dem unsicheren Netz eingreifen, und dem Security Management, das für die Verwaltung des aktiven Firewall-Elementes verantwortlich ist, indem die Sicherheitspolitik einer Organisation in Form eines Regelwerkes definiert wird.
In der Praxis haben sich die aktiven Firewall-Elemente **Packet Filter** und **Application Gateway** herauskristallisiert, die einen unterschiedlichen Ansatz bei der Einbindung in das Kommunikationssystem und bei den Möglichkeiten der Analyse und Protokollierung haben *(siehe auch: Norbert Pohlmann, Firewall-Systeme, 2. Auflage 1998, 440 S., DATACOM, ISBN 3-8266-4040-6).*

Packet Filter

Das aktive Firewall-Element “Packet Filter” analysiert und kontrolliert die ein- und ausgehenden Pakete

- auf Netzzugangsebene,
- Netzwerkebene und
- Transportebene.

Ein Packet Filter interpretiert den Inhalt der Pakete und verifiziert, ob die Daten in den entsprechenden Headern der Kommunikationsebenen den definierten Regeln entsprechen. Die Regeln werden so definiert, daß nur die notwendige Kommunikation erlaubt ist und bekannte sicherheitskritische Einstellungen vermieden werden, zum Beispiel die IP-Fragmentierung. Die Packet Filter werden transparent in die Leitung eingefügt.

Application Gateway

Ein Application Gateway zeichnet sich dadurch aus, daß es die Netze sowohl logisch als auch physikalisch entkoppeln kann.
Ein Benutzer, der über das Application Gateway mit dem privaten Netz kommunizieren möchte, muß sich zunächst identifizieren und authentisieren.
Ein Application Gateway empfängt 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.
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 – tatsächlich aber ist es der Proxy, der nach beiden Seiten als Vermittler auftritt, so daß niemals eine direkte Verbindung zwischen Zielrechner und Besucher zustandekommt. Jeder Proxy auf dem Application Gateway kann speziell für den Dienst, für den er zuständig ist, weitere Sicherheitsdienste (z.B. die Kontrolle der Kommandos get, put, ... bei FTP) anbieten. Bedingt durch den jeweiligen speziellen Proxy und das Wissen um den Kontext eines speziellen Dienstes ergeben sich im Application Gateway umfangreichere Sicherungs- und Protokollierungsmöglichkeiten.

5.2.2 High-level Security Firewall-System

In der Praxis gibt es eine Vielzahl von Kombinationsmöglichkeiten von Firewall-Systemen (nur Packet Filter, nur Application Gateway, Packet Filter und Application Gateway, usw.). Ein High-level Security Firewall-System faßt mehrere aktive Firewall-Elemente intelligent zusammen – nämlich zwei Packet Filter als Screened Subnet und ein dual-homed Application Gateway – und garantiert so ein Höchstmaß an Sicherheit.

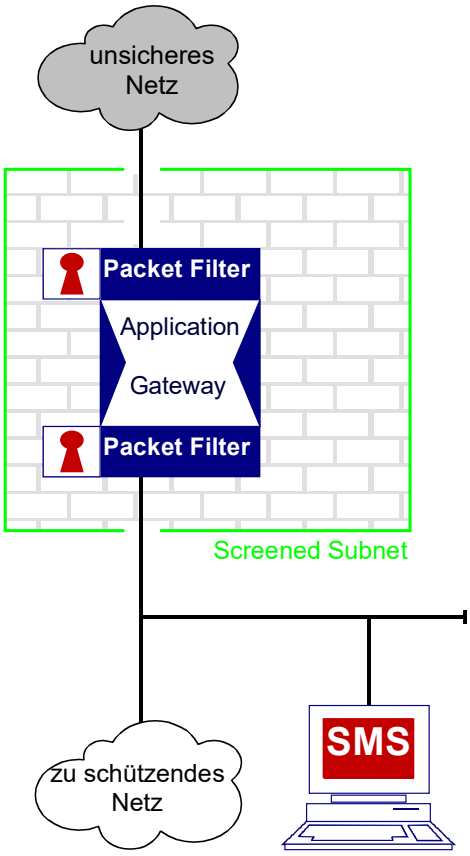

Abbildung 5.2 High-level Security Firewall-System

Grundgedanke und Zielsetzung eines High-level Security Firewall-Systems:

- **Einfache Regeln:** Die Anordnung der Elemente ermöglicht eine einfache Definition der Regeln für die einzelnen aktiven Firewall-Elemente.
- **Gegenseitiger Schutz:** Die Packet Filter sorgen dafür, daß nicht jeder auf das dual-homed Application Gateway zugreifen darf, und schützen damit das dual-homed Application Gateway selbst.
- **Geschachtelte Sicherheit:** Wer auf ein zu schützendes Netz zugreifen will, das durch ein High-level Security Firewall-System abgeschottet wird, muß verschiedene Barrieren überwinden: zuerst ein Packet Filter, dann ein dual-homed Application Gateway und zum Schluß wieder ein Packet Filter.
- **Verschiedene Betriebssysteme:** Aus Sicherheitsgründen verwenden High-level Security Firewall-Lösungen für die verschiedenen aktiven Firewall-Elemente verschiedene sichere Betriebssysteme: z.B. ein UNIX-Betriebssystem für das dual-homed Application Gateway und ein Real-Time-Betriebssystem für die Packet Filter. Eventuell auftretende Betriebssystemfehler oder Lücken wirken sich dadurch nur jeweils auf ein aktives Firewall-Element aus.
- **Unterschiedliche Einbindungs- und Analysemöglichkeiten:** Zudem arbeiten die verschiedenen aktiven Firewall-Elemente mit unterschiedlichen Strategien (Sicherheitsansätzen). Die Packet Filter interpretieren die übertragenen Pakete von unten nach oben auf der Netzzugangs-, der Netzwerk- und der Transportebene. Das dual-homed Application Gateway interpretiert die Kommunikation auf der Anwendungsebene. Auch hier können sich mögliche Schwächen der Einbindungs- und Analysemöglichkeiten nur jeweils auf eines der aktiven Firewall-Elemente auswirken.
- **Separates Security Management:** Das separate Security Management stellt viele eigene Sicherheitsmechanismen wie Zugangskontrolle, Rechteverwaltung, Verschlüsselung und Protokollierung zur Verfügung und sorgt auf diese Weise ebenfalls für High-level Security.

Alle diese Sicherheitsmechanismen zusammen garantieren ein höheres Maß an Sicherheit als jeder Sicherheitsmechanismus für sich alleine, so wie bei einem Auto der Sicherheitsgurt, der Airbag, der Seitenaufprallschutz und die Knautschzone zusammen ein Höchstmaß an Sicherheit bieten.

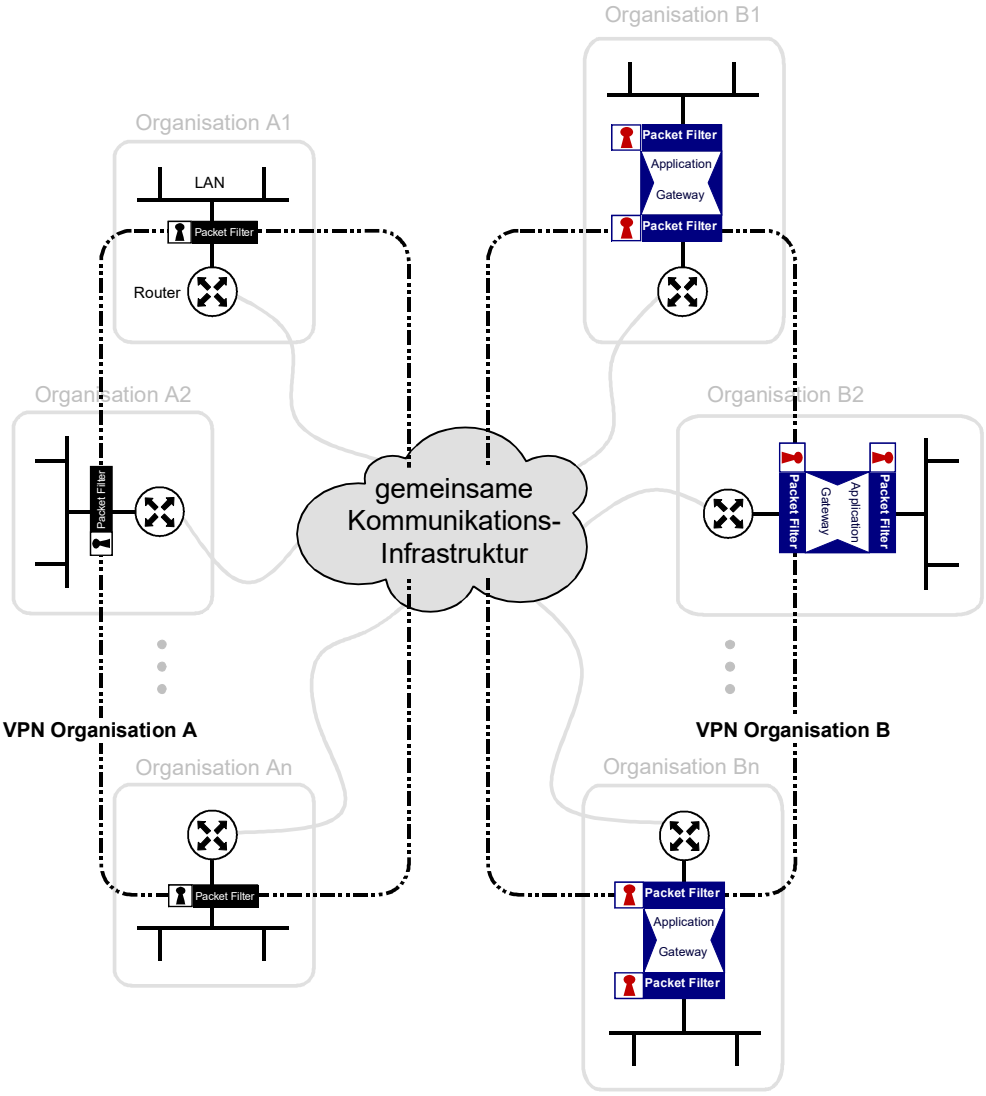

Abbildung 5.3 Integration von Firewall-Systemen in VPNs

5.2.3 Unterschiedliche Firewall-Konzepte:

Packet Filter, Application Gateway oder aber 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 Kommunikationinfrastruktur selber ab. Wenn die Kommunikationsinfrastruktur an sich schon ein Höchstmaß an Sicherheit und Vertrauenswürdigkeit bietet, d.h. alle angeschlossenen Teilnehmer haben ungefähr die gleichen Sicherheitsbedürfnisse, kann auch mit einer einfachen Firewall-Lösung (z.B. einem Packet-Filter) eine ausreichende Sicherheit erreicht werden.
Wird aber z.B. 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 auf jeden Fall einen hohen Widerstand (mit einem High-level Security Firewall-System) bei der Ankoppelung realisieren.

Ein besonderer Aspekt bei Firewall-Systemen ist, daß sie lokal verwaltet werden können, das heißt, bezogen auf die Kommunikationsmöglichkeiten und Protokollierung kann die eigene lokale Sicherheitspolitik realisiert werden, und dies unabhängig von Anderen.

Vorbehalte gegen Softwarelösungen

Vielfach wird angenommen, auch mit einer reinen Softwarelösung, die z.B. auf Windows-NT läuft, sei bereits ein genügend sicheres VPN realisierbar. Das ist auf gar keinen Fall möglich, denn NT zum Beispiel ist kein sicheres Betriebs-system.

5.3 Tunneling

Beim Tunneling wird jedes zu sendende Paket in ein neues Paket verpackt (Black Boxes). Dazu wird ein zusätzlicher neuer Header vorgeschaltet. So wird z.B. für IP-basierende Netze ein IP-Header vorangestellt. Weiter kommen zusätzliche Informationen oder Kennzeichen im Body-Teil des Pakets dazu.

Die vorgeschalteten Header charakterisieren die Endpunkte des Tunnels und 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 (z.B. IP oder IPX) verpackt übertragen und am Ziel wieder entpackt werden. Die dazwischenliegenden Router “wissen” nichts von diesen Mechanismen.

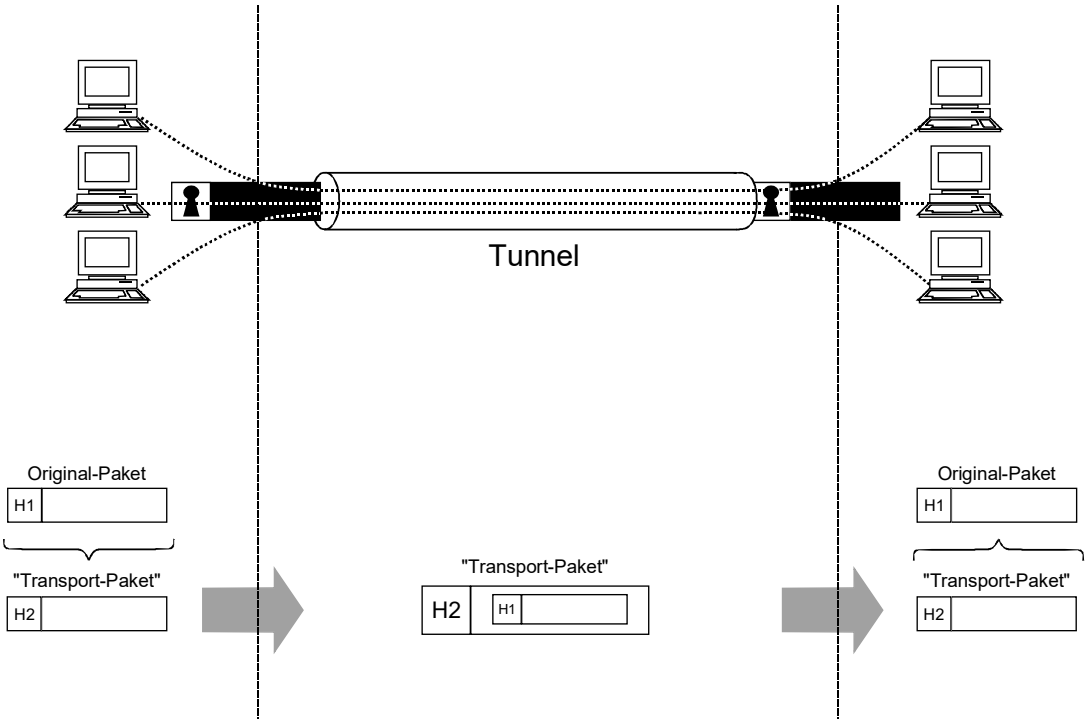

Abbildung 5.4 Tunneling

Vorteil von Tunneling ist, daß, wenn z.B. zwei Organisationen über eine öffentliche Kommunikationsinfrastruktur eine Kommunikation durchführen, immer nur zwei IP-Adressen verwendet werden, unabhängig davon, wie die Kommunikation tatsächlich stattfindet.

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 Quell- und Ziel-Adressen der Komponenten, die das Tunneling realisieren, sichtbar werden. Auf der anderen Seite können dann Features wie Prioritätensteuerung nicht mehr verwendet werden.

6 VPN-Realisierungen

Hinsichtlich der Realisierung von VPNs existieren unterschiedliche Lösungsansätze. Einige Hersteller haben spezielle Security-Protokolle 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 und Terminal-Anwendungen von besonderer Bedeutung.

IPSec

Im Bereich der Standardisierung hat die Internet Engineering Task Force (IETF) einen Internet-Sicherheitsstandard definiert, der IPSec heißt.
IPSec definiert Mechanismen, um sichere VPNs aufzubauen. IPSec bietet im wesentlichen zwei Mechanismen:

1. den sogenannten Authentication Header und
2. den Encapsulated Security Payload.

Beide Mechanismen können mit dem Tunneling kombiniert werden. Diese Kombinationen sind die grundsätzlichen Mechanismen, um VPNs aufzubauen.

Als das notwendige Key Management ist bei IPsec das sogenannte ISAKMP-Oakley definiert. Bei dieser Standardisierung sind jedoch noch viele Fragen der Implementierung nicht beantwortet. Auch sind bisher erst wenige Algorithmen zur Authentisierung und Verschlüsselung integriert. Deshalb ist bei vielen heutigen IPSec-Produkten fraglich, ob sie wirklich auf einer gemeinsamen Basis arbeiten und mit Produkten anderer Hersteller zusammenarbeiten können. Dafür ist nicht IPSec verantwortlich, sondern die noch nicht vollständige Umsetzung des Standards.
Auch die bei jeder Verschlüsselung oder Authentikations-Phase entscheidende Frage des Key Management ist noch nicht ausreichend diskutiert. Besonders wichtig beim Key Management ist die Frage einer gemeinsamen Public-Key-Infrastruktur, d.h. einer gemeinsamen Security-Infrastruktur, der die Anwender, die über eine öffentliche Kommunikations-Infrastruktur kommunizieren möchten, wirklich vertrauen können.

Es wird also eine Sicherheitsinfrastruktur benötigt, wo die Generierung eindeutiger Identifikationen, Hinterlegung von Schlüsseln etc. so realisiert ist, daß sich alle Beteiligten auf die Sicherheitsmechanismen absolut verlassen können.
Im Rahmen des Signaturgesetzes wird in Deutschland eine solche kontrollierte Sicherheitsinfrastruktur aufgebaut und eine gemeinsame Security Policy definiert; das ist ein vielversprechender Ansatz.
Im Rahmen des Sicherheitsmanagement wird immer wieder die Aushandlung von Verfahrensweisen, Algorithmen, Parametern und Schlüssellängen usw. diskutiert. In der Praxis wird es sich als Sicherheitsrisiko erweisen, daß die Komponenten, in die IPSec integriert werden soll, nicht sinnvoll entscheiden können, ob eine Kommunikation nun verschlüsselt werden soll oder nicht.
Außerdem gibt es bei IPSec noch weitere Aspekte, die noch einer eingehenderen Untersuchung bedürfen. Dazu gehören z.B. Flow-Control-Funktionen, die bezogen auf Ports bestimmte Prioritäten gewährleisten können. Diese würden bei einer IPSec-Relisierung nicht mehr zur Verfügung gestellt werden können.
Auch wirkt sich die Realisierung von IPSec negativ auf die Routing Performance aus. Die zusätzlichen Bytes belasten die Kommunikation, was zur Folge hat, daß die Nettodatenrate in einem IP-Paket sinkt, so daß die IP-Pakete weniger Nutzdaten transportieren. Im schlimmsten Fall bedeutet das, daß die Router gezwungen sind zu fragmentieren. Das ist ein zusätzlicher Aufwand, der den Datendurchsatz deutlich schrumpfen läßt.

Anderseits bietet IPSec in Zukunft die Chance für einen allgemeinen Sicherheitsstandard, sofern die entsprechenden vertrauenswürdigen Sicherheitsinfrastrukturen geschaffen werden.
Zwei wichtige Aufgaben, die eine gemeinsame sichere Infrastruktur dabei realisieren müßte, sind Identifikationsfestlegung und Generierung von verbindlichen Zertifikaten.

7 Kriterien für die Auswahl von VPN-Lösungen

Die wichtigsten Sicherheitskriterien für die Auswahl einer VPN-Lösung sind:

- die Offenheit und Transparenz der Sicherheit,
- der Nachweis, daß es sich um geprüfte Sicherheit handelt und
- die Gewißheit, daß die Sicherheitsleistung nicht durch staatliche Restriktionen beeinträchtigt wird.

7.1 Offenheit und Transparenz der Sicherheit

Eine VPN-Lösung soll nicht nur die Sicherheitsdienste erfüllen, für die sie angeschafft wurde, sondern in der Praxis “verhindern, was nicht gewollt ist”.
Aus diesem Grund ist die **Vertrauenswürdigkeit in eine VPN-Lösung** von besonderer Bedeutung. Dies ist äquivalent zu einem Pförtner, dem eine Organisation vertrauen können muß, damit die Sicherheitspolitik einer Organisation umgesetzt werden kann.

Offene und transparente Sicherheit

Die Art und Weise der eingesetzten Sicherheitsmechanismen müssen offengelegt werden, damit für den Betreiber eine Virtual Private Networks das erreichbare Sicherheitsniveau überschaubar ist.
Die in einem VPN verwendeten Algorithmen für die Verschlüsselung sollen standardisierte Sicherheitsmechanismen sein, die allgemein bekannt und grundlegend durch Fachleute erforscht sind, damit die Sicherheitsleistung nachweisbar und transparent ist.
Außerdem sollten die Designkriterien für die VPN-Elemente dargestellt werden.

7.2 Geprüfte, nachweisbare Sicherheit

Analog zu den Sicherheitsmechanismen in anderen Bereichen (z.B. Airbag in einem Auto) müssen die VPN-Sicherheitsmechanismen überprüft sein, aber nicht von jedem einzelnen Benutzer (Autofahrer), sondern von unabhängigen Fachleuten (dem TÜV).
Evaluierungen, z.B. durch IT-SEC, dienen dazu, die Qualität von IT-Sicherheitsprodukten zu bestätigen,.

7.3 Sicherheit ohne staatliche Restriktionen

Die Wirksamkeit der Sicherheitsmechanismen darf keinerlei staatlichen Beschränkungen unterliegen, damit ein VPN-System wirklich sicher realisiert werden kann. Mit geeigneter Schlüssellänge für kryptographische Sicherheitsmechanismen wie Verschlüsselung und Authentikation und ohne den Einbau irgendwelcher Sicherheitslücken für Geheimdienste oder andere staatliche Stellen, wie:

- reduzierte Schlüssellängen
- Key Recovery (Möglichkeit zur Rückgewinnung von Schlüsseln)
- Key Escrow-Mechanismen (zwangsweise Schlüsselhinterlegung bei staatlichen Treuhandstellen)
- oder sogar Trapdoors (eingebaute Einstiegsmöglichkeiten).

Bei einer möglichen Bedrohung durch internationale Wirtschaftsspionage muß daher überlegt werden, ausschließlich Sicherheitsprodukte zu verwenden, die diesen Restriktionen nicht unterliegen.