FAKULTÄT FÜR !NFORMATIK

VPN Technologie, Vergleich von VPN Protokolle und möglicher Einsatz in der Schule

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur/in

im Rahmen des Studiums

Internet Security/ Software Management

eingereicht von

Banu Meneve

Matrikelnummer 0126041

an der

Fakultät für Informatik der Technischen Universität Wien

Betreuung:

Betreuer/Betreuerin: Dr. Andreas Ulovec

Wien, 28.06.2009

INHALTVERZEICHNIS

ABBILDUNGSVERZEICHNIS

1.Einführung

Die Entwicklung der vernetzten Kommunikation hat in den letzten beiden Jahrzehnten eine überaus rasante Entwicklung erlebt. Mit der Einführung des ersten Personals Computer (PC) Anfang der 1980 er Jahre und der Notwendigkeit PCs miteinander kommunizieren zu lassen, hat sich eine ganz neue Kommunikationscharakteristik herausgebildet.

Die direkte Kommunikation zwischen Menschen war bislang auf das persönliche (beide Gesprächspartner müssen anwesend sein) oder fernmündlich Gespräch (Telefon) beschränkt und beruht auf dem Prinzip einer akustischen Übertragung von Daten. Die Nutzung von PCs und der an diesen Arbeitsplätzen anfallenden Daten verlangte nach einer ebenso direkten Kommunikationsmöglichkeit.[1]

Durch die Informationstechnologie und den sich ändernden Kommunikationsmöglichkeiten sehen sich die Unternehmen mit einer rasanten Entwicklung konfrontiert.

Die Unternehmen müssen inzwischen ihre Marktpositionen in immer kürzeren Produktzyklen behaupten. Dies wirkt sich auf die eingesetzten IT-Anwendungen und Systeme und ihre Vernetzung aus. Neue Applikationen erlauben ein effizienteres Abwickeln bestehenden geschäftlicher Vorgänge oder zwingen zu deren Veränderung. Die traditionellen Verfahren zum Datenaustausch, Z.B. Brief-Post oder Fax- Kommunikation, werden den neuen Anforderungen nicht mehr gerechnet, da sie zeitaufwändig und verwaltungsintensiv sind.[2]

Die ersten LANS (LAN: Local Area Network) entstanden. Netzwerke aus aktiven (Bridges, Switches, Router) und passiven (Kabel, Verteiler) Komponenten wurden in den Unternehmen neben der bislang meist großrechnerbasierten Infrastruktur eingerichtet, um somit innerhalb kürzester Zeit alle relevanten Daten bedarfsorientiert zur Verfügung stellen zu können. Unternehmen mit mehreren Standorten benötigen allerdings neben der lokalen Kommunikation auch Verbindung zu geografisch entfernten Standorten.

---

[1] Gerhard Lienemann, Virtuelle Private Netzwerke Aufbau und Nutzen, 2002, S 13

[2] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005 , S 4

Solche WAN- Strukturen (WAN: Wide Area Network) werden in der Regel über Datenfernverbindungen (Frame Relay, ATM usw.) errichtet, an deren Endpunkten spezielle Rechner, Router oder auch Firewallsystem stehen.[3]

ATM und Frame Relay Netzwerke ermöglichten höhere Datenübertragungsraten im WAN und vereinfachten die Verwaltung durch den Einsatz virtueller Leitungen im Frame Relay bzw. ATM-Netzwerk. Doch aufgrund ihrer begrenzten Übertragungsmöglichkeiten für verschiedene Arten von Datenverkehr machten diese beiden Netzwerk Technologien neueren, auf dem Internet-Protokoll basierenden VPN- Lösungen den Weg frei. Diese VPNs gewährleisten eine höhere Flexibilität beim Versenden unterschiedlicher Arten von Informationen über das Netzwerk.

Es gibt eine Vielzahl von Situationen, die bei unzureichender Planung oder nicht konsequenter Berücksichtigung der Leitungscharakteristik im WAN- Verbund Probleme verursachen können.

Der Datenverkehr jeder Anwendung, die über WAN- Strecken betrieben werden muss, ist exakt zu berechnen. Jeder zusätzliche Datenverkehr, der nicht berücksichtigt wird, führt zu einem späteren Zeitpunkt zu Verzögerungen und Einbußen in der Reaktionsfähigkeit (Performance) der Anwendungen.

- Ausgesprochene LAN- Anwendungen (Anwendungen mit einem hohen Datenaufkommen, das im LAN auf Grund der hohen verfügbaren Bandbreite keinerlei Probleme verursacht, wie Z.B. die Nutzung von Ressourcenfreigaben im Netzwerk) werden auch über WAN- Strecken genutzt, die allerdings für das hohe Datenaufkommen nicht ausgelegt sind.
- Ein WAN- Verbund ist kein statisches Gebilde. Es unterliegt den sich dynamisch entwickelnden Kommunikationsanforderungen des Unternehmens. Die Einführung neuer Anwendungen in allen Standsorten oder Teilen des Konzerns führt zu einer Neugestaltung des Weitverkehrsnetzes und einem zusätzlichen Bedarf an Bandbreite.[4]

---

[3] Gerhard Lienemann, Virtuelle Private Netzwerke Aufbau und Nutzen, 2002, S 13

[4] Gerhard Lienemann, Virtuelle Private Netzwerke Aufbau und Nutzen, 2002 , S 15

Die Vielfalt der Anforderungen ha in den vergangenen Jahren dazu geführt, dass für unterschiedliche Bedürfnisse mitunter sehr spezifische Lösungen gesucht und gefunden wurden.[5]

Eine vernünftige Möglichkeit, diese oder ähnlich gelagerte Probleme vollständig oder nur teilweise zu lösen, stellt die Einführung von „Virtuellen Privaten Netzen“ (VPN) dar.

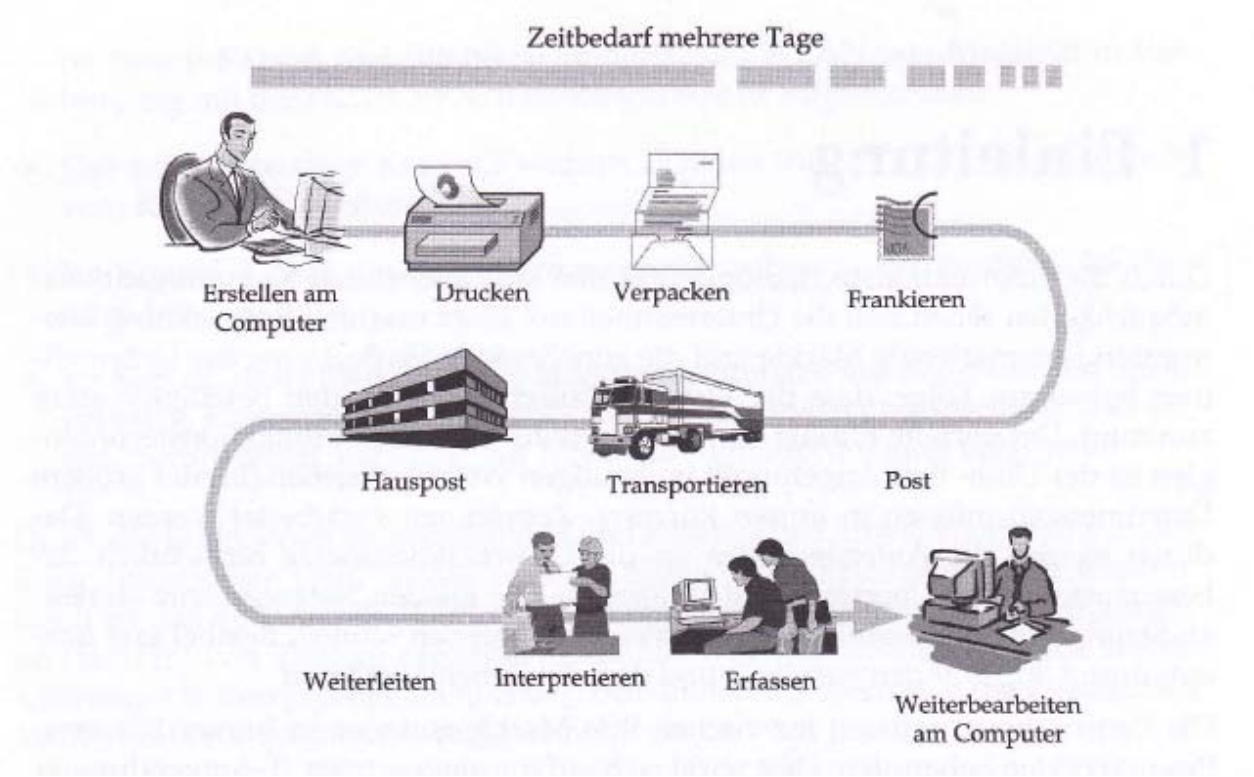

Abb. 1 : Herkömmlicher zeitraubender Informationsaustausch

Quelle: Wolfgang Böhmer VPN Virtual Private Networks, S 2

[5] Jörg Buckbesch, Rolf- Dieter Köhler, VPN Virtuelle Private Netze Sichere Unternehmenskommunikation in IP-Nutzen, 2001, S 9

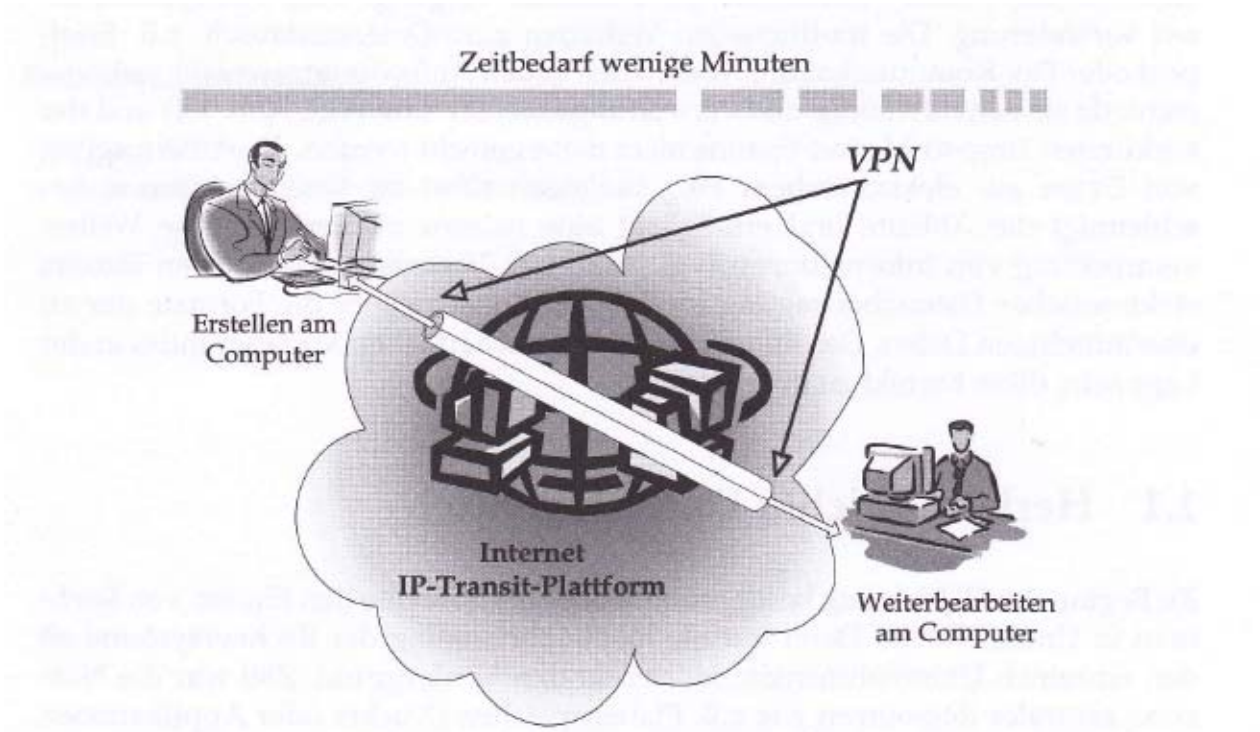

Abb. 2 : Moderner Informationsaustausch mittels VPN zur direkten Kommunikation zwischen zwei Standorten

Quelle: Wolfgang Böhmer VPN Virtual Private Networks, S 2

1.1 Was ist Virtuelles Privates Netzwerk?

Ein Virtuelles Privates Netz (VPN) ist ein logische Netz verbinden, um die privaten Daten und Informationen bzw. Datenverkehr zu senden. Eine logische Verbindung ist eine Netzverbindung zwischen einem Sender und einem Empfänger. Auf diese Weise werden der Information und Bandbreite durch den Weg dynamisch zugewiesen.

Ein Virtuelles Privates Netz ist eine Anzahl von Verbindungen, die über ein öffentliches Netzwerk aufgebaut werden, sich aber für den Nutzer wie private Leitungen darstellen. Der Begriff des Virtuellen Privaten Netzes wurde mit dem Aufkommen und der breiten Verfügbarkeit entsprechender IP- basierter Techniken geprägt. Ein VPN ist ein Netzwerk, das ein anderes, öffentliches Netzwerk benutzt, um private Daten zu transportieren.[6]

[6] Jörg Buckbesch, Rolf- Dieter Köhler, VPN Virtuelle Private Netze Sichere Unternehmenskommunikation in IP-Nutzen, 2001, S 11

Hierbei bedeutet privater Datenaustausch, dass die Übertragenen Daten hinsichtlich ihrer Integrität und Ihre Vertraulichkeit nicht kompromittiert können.

Ein VPN erfordert eine Menge Technologieanpassung und Prozess Veränderungen. Die Unternehmen verfügen über eigene Netze, die die einzelnen Filialen verbinden. Sie lokale Netzsegmente sind über Weitverkehrsnetzte miteinander verbunden. Gerade im Zuge des aufkommenden E-Business wird die Sicherheit der Kommunikation über das Internet immer wichtiger. Eine Schlüsselrolle wird hierbei die VPN- Technologie einnehmen. Neben reinen Sicherheitsfunktionen sind allerdings noch weitere Kenngrößen gefragt, wie Z.B. Interoperabilität, Kosten und Performance.

Neben dem Internet las beliebter Kommunikationsplattform kommen im Weitverkehrsbereich jedoch auch Plattformen wie Z.B. ATM oder Frame Relay zum Einsatz. Die Entscheidung, welche der genannten Plattform gewählt wird, richtet sich nach dem zu transportierenden Verkehrsvolumen und den daraus resultierenden Kosten. Ist das Unternehmen über mehrere Standorte verteilt, die eine gemeinsame Plattform nutzen, erfüllt die Plattform und die darauf aufsetzende Kommunikation die Eigenschaft eines privaten Netzes.[7]

Der Begriff „Virtuelles Privates Netz“ enthält bereits eine sehr genaue Beschreibung seiner Bedeutung durch die Worte „virtuell“ , „private“ und „ netz“ . Er vermittelt zunächst, dass es sich um ein Netzwerk mit privatem, also ausdrücklich nicht öffentlichem Charakter handelt.[8]

„Private“ bedeutet in diesem Kontext, dass einerseits der Zugang nur einem begrenzten und namentlich bekannten Personenkreis möglich ist, andererseits ist die Vertraulichkeit und dies eine Forderung, die erst neuerdings hinzugekommen ist- der elektronisch ausgetauschten Informationen gewährleistet. [9]

Durch die Eigenschaft „virtuell“ wird die Konkretisierung vermutet, dass es sich um verschiedene Betrachtungsweise zwischen dem physikalischen Netzwerk und der funktional verwendbaren Aufbau handelt. Verbindungen werden durch Plattformen zwischen

---

[7] Manfred Lipp VPN- Virtuelle Private Netzwerke Aufbau und Sicherheit, S 23

[8] Gerhard Lienemann, Virtuelle Private Netzwerke Aufbau und Nutzen, 2002, S 16

[9] Manfred Lipp VPN- Virtuelle Private Netzwerke Aufbau und Sicherheit

Unternehmensstandorten ermöglicht, bei denen lediglich der Weg der Daten in der Kommunikationsplattform hinterlegt ist. Wenn die anstehende Daten zur Übertragung auf der erforderliche Bandbreiten zugewiesen werden. Die Informationen werden erweckt, als seien die Standorte physikalisch miteinander verbunden, derartige Verbindungen werden als „virtuell“ bezeichnet.

1.2 Ziele und VPN Grundidee

Heutzutage wird sich VPNs angeschaut und wenn die Eigenschaften von sie mit dem vergleicht werden, was vor sechs, sieben Jahren eingesetzt wurde, wird man sich schnell versteht, wie sich auch in diesem Bereich vieles verändert hat. Wenn man der erste denkt, sieht dies alles nur mit gestiegenem Bandbreitenbedarf und Kostengründen aus, kann jedoch nur ein kleiner Teil wahr annehmen. Denn es ist eine ganze Reihe von Faktoren, sowohl technologisch als auch wirtschaftliche, betriebliche und soziale, die den Wandel zu VPN heutiger Ausprägung beeinflusst haben. Wenn dies Netzwerk für die Zukunft geplant wird, machen sollte man sich vor allem.

Die Frage lautet also: Wie können die komplexen Kommunikationsanforderungen möglichst einfach und transparent mit einer herstellerunabhängigen und bezahlbaren Technologie erfüllt werden, ohne dabei den Datenschutz zu vernachlässigen?
VPN sind aus heutiger Sicht die optimale Lösung dieser Aufgabenstellung:

1. Mit VPN ist es erstmals technisch möglich, alle Kommunikationsdienste auf einem einzigen Trägermedium zu integrieren und damit eine deutliche Reduzierung der Komplexität von Weitverkehrsnetzen zu erreichen.
2. Indem mit VPN öffentliche Netze durch viele Teilnehmer gemeinsam genutzt erden, sind erhebliche Einsparungen bei den Übertragungskosten möglich.
3. Durch die Nutzung virtueller Übertragungswege können in den Netzkomponenten wenige schnelle Interfaces anstelle einer großen Anzahl verhältnismäßig langsamer Anschlüsse verwendet werden.

4. Selbst im Internet können VPN- Verbindungen bei Anwendung entsprechender Maßnahmen sicherer sein als herkömmliche Stand- oder Wählleitungen.[10]

Die Grundlage eines herkömmlichen VPNs bildet der Internetanschluss. Je nach VPN- Typ wird dazu eine Wählverbindung erforderlich. Zur Verbindung von Netzwerken unterschiedlicher Unternehmen sollten ausschließlich Festverbindungen eingesetzt werden, die über eindeutige und veränderbare öffentliche IP- Adressen verfügen, über diese eindeutig spezifizierbaren Kommunikationsendpunkte können VPNs als Punk- zu- Punkt- Verbindung eingerichtet werden.[11]

1.2.1 Veränderung der Geschäftsprozesse

Nicht wenige Unternehmen haben die Art und Weise wie sie ihre Geschäfte betreiben, an die veränderte Kommunikationslandschaft angepasst. Neben dem Offensichtlichen, nämlich der Nutzung des Internets zum Zweck der Werbung und Verbreitung von Informationen, sowie dem starken Wachstum des B2C- Geschäftes (B2C, Business to Consumer), haben sich aber auch andere Dinge in den Unternehmen verändert. So ist heutzutage fast kein Rechner, der irgendwo in einem Unternehmen installiert wird, mehr ohne eine Netzwerkverbindung. Die Netze in den verschiedenen Standorten sind ebenfalls miteinander verbunden und damit auch alle Rechner und deren Benutzer im Unternehmen.

Kommunikation zwischen unterschiedlichen Unternehmen hat sich stark verändert. Während anfangs ein eher unverbindlicher Informationsaustausch erfolgte, sind heutzutage nicht wenige Geschäftsprozesse transparent über mehrere verbundene Unternehmen verteilt. Als Beispiel seien hier die großen Verbundnetze für Banken, Reisebüro oder auch das riesige Super- VPN ANX (Automotive Network Exchange) im Automobilbereich genannt.

---

[10] Jörg Buckbesch, Rolf- Dieter Köhler, VPN Virtuelle Private Netze Sichere Unternehmenskommunikation in IP-Nutzen, 2001, S 11

[11] Gerhard Lienemann, Virtuelle Private Netzwerke Aufbau und Nutzen 2002, S 21

Wenn sich erst einmal ein System wie ANX prinzipiell durchgesetzt hat, dann werden sich immer mehr Unternehmen anschließen, es werden immer mehr Informationen übertragen und dadurch auch die Anforderungen an Bandbreite, Verfügbarkeit und Qualität des Netzwerk immer höher.

Der Verband der Automobilindustrie hat in den späten 90ern ein Branchennetz, das European Automotive Network Exchange (ENX) realisiert. Es stellt ein VPN auf Basis des IP- Protokolls dar und zwar mit folgenden Anforderungen:

- Kopplung unternehmensübergreifender Geschäftsprozesse
- Frei wählbare Kommunikationsbeziehungen unter den Geschäftspartnern
- Höchste Sicherheitsforderungen
- Integration altbewährter Kommunikationsdienste (Z.B. E-Mail)
- Electronic- Business- Dienste aus der Steckdose[12]

1.2.2 Globalisierung und Dezentralisierung

Viele Unternehmen, die großen schon lange, der Mittelstand mittle weile auch mehr und mehr, stehen vor neuen Herausforderungen durch Globalisierung und die damit verbundene unausweichliche Dezentralisierung ihrer Firmen und ihrer Geschäftsabläufe. Es gibt nur noch ganz wenige, im produzierenden Gewerbe fast gar keine Unternehmen mehr, die ausschließlich nur in einem Land tätig sind, nur für den Markt dieses Landes produzieren und nur Geschäftsbeziehungen mit Unternehmen und Kunden in eben diesem Land pflegen.
Egal ob man ausländische Märkte bedient, ob man mit ausländische Zulieferern zusammenarbeitet oder ob man aufgrund exorbitanter heimischer Personalkosten und steuerlicher Vorteile im Ausland produziert, im Ausland Standorte oder Büros oder zumindest Personen zu haben, die einen Zugriff auf das Unternehmensnetz benötigen. Da dieser Zugriff ein komfortables soll, werden bestimmte Anforderungen hinsichtlich Bandbreiten, Übertragungsqualität und vor allem auch Sicherheit gestellt, deren Befriedigung nicht unerhebliche Kosten erzeugen kann.

[12] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005, S 13

1.2.3 Veränderung der Wettbewerbssituation

Eine Folge der Globalisierung und der schnellen, weltweiten Verfügbarkeit von Informationen ist auch die veränderte Wettbewerbssituation, in der sich viele Unternehmen wiederfinden. Denn in vielen Branchen wurde früher auf dem lokalen, nationalen Markt für eben diesen produziert. Der Wettbewerb war damit überschaubar, und die Konkurrenz produzierte vor allem auch unter den gleichen wirtschaftlichen und sozialen Bedingungen, heutzutage sieht das anders aus, kaum eine Firma , die nicht für ausländische, internationale Märkte produziert und damit nicht in einer völlig Wettbewerbssituation steckt.

1.2.4 Mobilität und Flexibilität

Mobilität und Flexibilität sind heutzutage keine bloße schicken Schlagwörter mehr, sondern knallharte Anforderungen in vielen Situationen des modernen Geschäftslebens.

Im Zuge immer höherer Mobilität sind insbesondere drahtlose Kommunikationsformen gefragt, sowohl im Bereich mobiler Sprachkommunikation als auch mehr und mehr drahtlose Datenkommunikation.

Mobilität aber auch gleichzeitig Produktivität gewährleisten kann, muss ein zuverlässiger und vor allem sicherer Zugriff mobiler Mitarbeiter auf die von ihnen benötigten Ressourcen möglich sein, egal ob von zu Hause , auf dem Flughafen oder beim Kunden.

1.2.5 Kostenoptimierung

Die in den letzten Jahren, vor allem in einigen europäischen Industrienationen, immer kritischer werdenden Standortkosten zwingen fast alle Unternehmen zu teilweise drastischen Maßnahmen, um ihre Betriebskosten zu senken.

Wenn man die Personalkosten vorerst einmal außer Acht lässt, bei vielen Unternehmen mit mehreren Standorten, vielleicht sogar nach international verteilt, auf einen stattlichen Posten: die Betriebskosten für das Weitverkehrsnetz, vor allem bestehend aus den laufenden Kosten für Leitungsgebühren, Verbindungszeiten oder übertragenen Datenvolumina. Hier versucht man, Ratiopotenzial freizusetzen.

Die Idee, die Gesamtkosten durch Senkungen im größten Anteil, den Betriebskosten, zu reduzieren, hat auch einige Einfluss auf Weitverkehrsnetze, denn hier fallen nicht unbeträchtliche Kosten an. Hier bieten VPN ein sehr hohes Ratiopotenzial.

1.2.6 Sicherheit

Wenn man verschiedene Standorte verbindet, Fernzugriff auf sein Unternehmensnetz erlaubt oder eine Verbindung zum Internet betreibt, dann verbindet man auf die einen oder andere Weise sein privates Netzwerk mit einem öffentlichen Netzwerk. Der Grand der Öffentlichkeit ist stark unterschiedlich, bei der Benutzung von digitalen Standardfestverbindungen zum Beispiel benutzt man ein öffentliches Telefonnetzwerk bei einem IP- VPN unter Umständen des Internet.
Aber auch weniger dramatische Szenarien sind durch die Hacker Angriff, insbesondere in den letzten Jahren, zunehmend ins Bewusstsein einer breiten Öffentlichkeit und leider manchmal erst dadurch auch in das der Verantwortlichen in unseren Unternehmen gerückt.
Denial- of- Service – Angriffe, also die Sabotage von Kommunikationseinrichtungen , das Eindringen in fremde Netze, Ausspionieren fremder Daten oder das Einschleusen von Viren, sind nur einige Beispiele erfolgreicher Angriffe auf Netzwerke, die in letzter Zeit Schlagzeilen gemacht haben.

1.3 Entscheidungskriterien

Bevor man sich für den Einsatz eines VPN entscheidet, sind die Vorteil und Nachteile für das eigene Netzwerk und die genutzten bzw. geplanten Anwendungen abzuwägen. Dabei sind funktionale Eigenschaften, Sicherheitsfragen und selbstverständlich auch die Kosten von entscheidender Bedeutung.

Bei der Implementierung von VPNs geht es somit im Wesentlichen um die Gewährleistung eines geschützten Datenstroms über öffentliches Netzwerk. Zusammengefasst handelt es sich um folgende Schwerpunkte:

- Geringe Kosten für die Nutzung des Internets als öffentliches Netzwerk
- Datensicherheit durch Datenverschlüsselung [13]

Bei der Bewertung einer VPN- Lösung sollte die Gesamtheit dieser Aspekte berücksichtigt werden. Hinsichtlich ihrer technischen Eigenschaften kann eine VPN- Lösung wesentlich

[13] Gerhard Lienemann, Virtuelle Private Netzwerke Aufbau und Nutzen 2002, S 17

flexibler und vielseitiger als ein herkömmliches WAN sein. Insbesondere sind mit der VPN – Technologie heute Anwendungen möglich, die früher völlig undenkbar waren. Obwohl mit der Nutzung des Internet auch Probleme verbunden sein können, dürften die Vorteile insgesamt überwiegen.

1. IP-VPN verwenden das Ebene- 3- Protokoll IP zum Transport. Sie sind daher unabhängig von der Verfügbarkeit einzelner Ebene- 2- Techniken. Eine VPN- Verbindung kann zu jedem Punkt der Welt aufgebaut werden, zu dem eine IP- Kommunikation möglich ist. Dabei ist es Prinzip unerheblich, über welche und wie viel verschiedene physikalische Übertragungsdienste die Verbindung geführt wird.
2. Eine VPN- Verbindung wird als logische Beziehung zweier im Trägernetz erreichbaren Systeme konfiguriert. Diese Konfiguration erfolgt nur an den Endpunkten und liegt in der Verantwortung des Unternehmens oder Dienstanbieters. In jedem Fall kann eine solche Verbindung wesentlich schneller hergestellt, verändert oder abgeschaltet werden, als irgend ein Netzanbieter einen Wählanschluss installieren oder eine Standleitung ändern könnte.
3. Mit VPN- Verbindungen kann eine beliebige Netzstruktur auf der Basis nicht physikalischer Übertragungswege aufgebaut werden.
4. Die im Internet bisher nicht verfügbaren Dienstqualitäten stellen beim Einsatz von VPN ein Problem für bestimmte Anwendungen dar. Dies betriff sowohl die Ende- zu- Ende verfügbare Bandbreite als auch die variierende und mitunter zu hohe Verzögerungszeit.[14]

Kosteneinsparungen können ein weiterer wichtiger Grund für den Einsatz von VPN sein. Ob eine VPN- Lösung tatsächlich kostengünstiger als die möglicherweise schon vorhandene klassische WAN- Lösung ist, hängt stark von den konkreten Anforderungen ab und muss daher in jedem Einzelfall untersucht werden.

VPN alle WAN- Anbindungen eines Unternehmens auf der Basis einer einzigen Technologie realisierbar sind, können Betriebs-, Personal- und Ausbindungskosten gespart werden.

[14] Jörg Buckbesch, Rolf- Dieter Köhler, VPN Virtuelle Private Netze, Sichere Unternehmenskommunikation in IP-Netzen, S 17

Auch bei den Gerätekosten sind Sparpotenziale vorhanden, weil viele langsame WAN-Schnittstellen (Z.B. am Router) ersetzt werden können durch wenige oder eine einzige schnelle Schnittstelle, über die entsprechend viele logische VPN- Verbindungen geführt werden.

Auch Sicherheitsforderungen können ein Grund für den Einsatz von VPN sein. In diesem öffentlichen Netz muss mit erheblichen Sicherheitsrisiken gerechnet werden. Die VPN-Lösungen der meisten Hersteller bieten deshalb Sicherheitsmechanismen, die von der Authentisierung der Kommunikationspartner und übertragenen Daten über Replay- Schutz und Datenverschlüsselung bis zur Netzabschaltung mittels überwiegend als sehr sicher.[15]

1.4 VPN Typen

Bei VPN unterscheidet man, abhängig vom Einsatzgebiet, zwischen verschiedenen Arten, wobei diese durchaus auch miteinander kombiniert werden können. Die unterschiedlichen Arten von VPN lehnen sich dabei stark an ihre korrespondierenden klassischen Netzwerk Strukturen an.[16]

Die VPN – Technologie nahezu standardisiert sind, unterstützen nicht alle Produkte am Markt alle VPN – Typen. Solange nur eine Technologie zum einen folgende Gesichtspunkte zu beachten. Die VPN – Lösung sollte:

- auf die Geschäftsprozesse abgestimmt sein,
- eine hinreichende Kommunikationssicherheit bieten,
- ausreichende Performance liefern und
- interoperabel zu den bestehenden Systemen sein.

Den größten Mehrwert kann ein Unternehmen erreichen, wenn sich eine vorhandene Lösung bei Veränderungen, z. B. Geschäftsprozessen flexibel erweitern bzw. neuen Technologien anpassen lässt. Immer mehr Produkte ermöglichen diese Flexibilität.

---

[15] Jörg Buckbesch, Rolf- Dieter Köhler, VPN Virtuelle Private Netze, Sichere Unternehmenskommunikation in IP-Netzen, S 20

[16] Manfred Lipp VPN- Virtuelle Private Netzwerke Aufbau und Sicherheit , S 37

Ausgehend von den sieben Schichten des OSI Referenzmodells können verschiedene Sicherungsmaßnahmen auf den verschiedenen Ebenen zur Absicherung unterschiedlicher VPN-Typen installiert werden – je nachdem welches Ziel und welches Vertrauensmodell verfolgt wird. General lassen sich und einem VPN – Blickwinkel die sieben Schichten auf drei VPN- Ebenen reduzieren. [17]

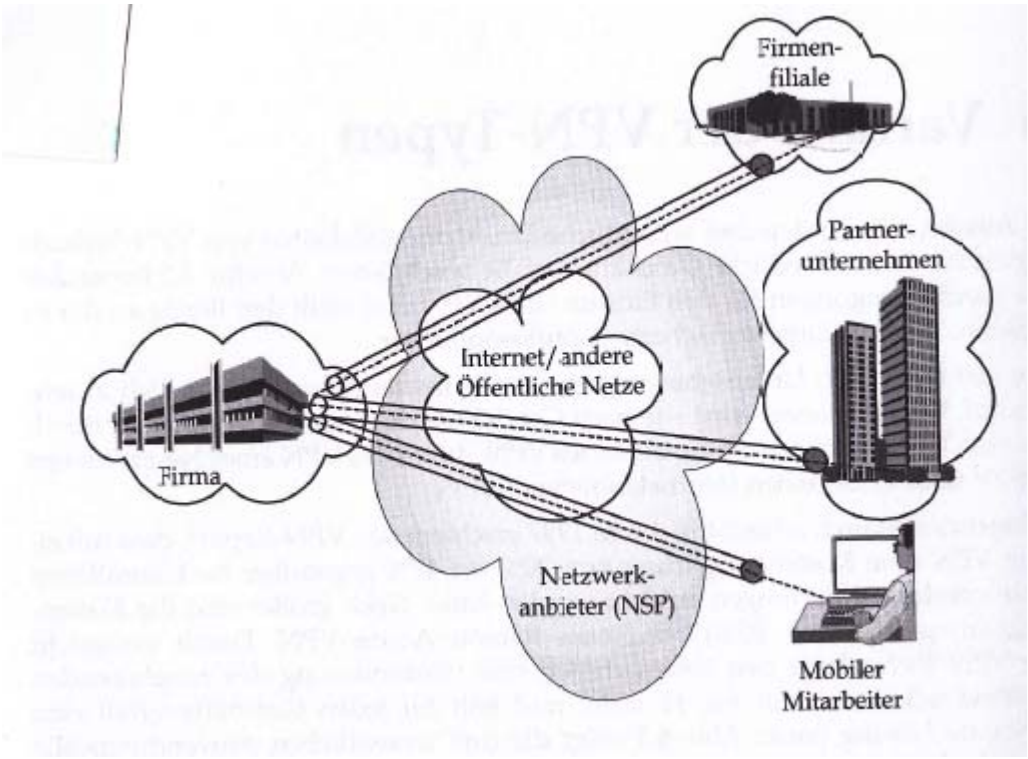

Abb. 3 : Anwendungsspektrum

Quelle: Wolfgang Böhmer VPN Virtual Private Networks, S 182

[17] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005, S 183

- VPN auf der Applikation ebene in den Schichten (5-7)

Ein VPN auf Layer- 5 kann eine sichere Kommunikation auf der Session – Ebene über einen Proxy- Dienst aufbauen, indem TCP verwendet wird. Diese Architektur ist gut geeignet, um mit Partnernetzen zu kommunizieren. Der VPN- Client arbeitet auf der Transportsicht problemlos mit den Computern des Partnernetzes zusammen. Ebenso überwindet auf dieser Ebene der VPN-Client auf einfache Weise die Firewall des Partner- Extra- Netzes, was bei einem VPN auf Layer-3 schwieriger ist.

- VPN auf der Transport / Netzwerkebene in den Schichten (3-4),

Ein Layer 4- VPN dient der sicheren Kommunikation auf der Transportschicht. Diese Art VPN ist gut geeignet für die sichere Kommunikation von zwei oder mehreren Netzwerken, die eine sichere Verbindung für E- Commerce- Anwendungen benötigen.

Ein Layer- 3- VPN bietet die Möglichkeit, neben TCP /IP, auch Protokolle wie RPC und UDP einzusetzen. Derartige VPN – Lösungen werden vornehmlich für ein Remote- Access –VPN eingesetzt und bieten dem Nutzer ein breites Anwendungsspekturm.

- VPN auf der Sicherungs- Bitübertragungsebene in den Schichten (1-2)

VPN auf den unteren Schichten besitzen gegenüber VPN der höheren Schichten den Vorteil, dass wesentlich einfacher Quality of Service Garantieren (QoS) verbindlich erteilt werden können. Vorteile liegen in der Skalierbarkeit und im VPN – Management.

In den drei Ebenen (Applikationsschicht, Transport - / Netzwerkschicht und Link bzw. Physikalische Ebene) lassen sich die wesentlichen Protokolle und Sicherungsmechanismen einordnen, mit denen sich sie vollständige Absicherung eines VPN und damit auch des sonstige Datenverkehrs erreichen lässt. Da die VPN –Technologie in direktem Zusammenhang mit der vertraulichen Datenübertragung steht, haben sich im Laufe der Zeit in den drei Ebenen unterschiedliche Absicherungsmechanismen mit Unterschiedlichen Zielsetzungen herauskristallisiert.

- Einige der modernen kryptographischen Sicherungsmechanismen lassen sich in der Anwendungsebene finden. Die gängigen für ein VPN geeigneten Sicherheitstechnologie sind:
- IP Paket Filtertechniken

- Network Adresse Translation (NAT)
- SOCKS
- Secure Socket Layer (SSL)[18]

1.4.1 Intranet – VPN (Site- to- Site)

Das VPN wird hierbei durch Erweiterungen der in lokalen Netzwerken (LAN) eingesetzten Switching – Technologien erzeugt.

Am Aufbau eines Site- to- Site VPN sind zwei VPN – Gateways (Firewall -Systeme) beteiligt. Sie Verschlüsselung der Daten erfolgt nur auf dem Weg zwischen den beiden VPN- Gateways; der Weg durch das lokale Netz vom Gateway zum End- gerät bleibt unverschlüsselt. Das VPN ist somit für Endgerät transparent und sie benötigen keine zusätzliche VPN- Client- Software.
Eine Möglichkeit, ein Site- to- Site- VPN zwischen einer Zentrale und einer Niederlassung einzurichten, besteht darin, lediglich einen Internetanschluss bei einem ISP zu mieten und auf beiden Seiten Firewall- Systeme bzw. Router mit integrierter Firewall- Technologie oder spezielle IPSec – Gateways an der Schnittstelle zum Internetanschluss einzurichten.[19]

Bei der Installation von VPNs im eigenen Unternehmensnetzwerk wird die Kommunikation zwischen einzelnen Abteilungen oder Bereichen des Unternehmens an verschiedenen Standorten verschlüsselt, sofern die Infrastruktur eine solche Installation zulässt. Innerhalb des eigenen Unternehmensnetzwerkes kann es sinnvoll sein, VPNs zur gesicherten Kommunikation einzusetzen. Hier sind mindestens drei Szenarien denkbar:

- Sensible Personendaten, die aus Datenschutzgründen auch für die Mitarbeiter des eigenen Unternehmens nicht eingesehen werden dürfen, müssen verschlüsselt übertragen werden. Bei einem Unternehmen mit mehreren Standorten ist eine sichere Übertragung zwischen den Personalabteilungen zu gewährleisten.

---

[18] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005, S 185

[19] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005 , S 187

- Sensible technische Daten aus Forschung und Entwicklung müssen über nationale Standorte hinaus zu anderen Unternehmensstandorten im Ausland übertragen werden.
- Beim Einsatz von eCommerce- Applikationen im Internet fallen in der Regel umfangreiche Datenmenge an, die zur Weiterverarbeitung in die Backend – Systeme des Unternehmens übernommen werden müssen. Da die Daten auch im Internet übertragen werden müssen, ist auch hier für die Geheimhaltung der Daten zu sorgen.[20]

1.4.2 Extranet- VPNs

Wenn die Netzwerke zweier unterschiedlicher Unternehmen miteinander über VPNs verbunden werden, so bezeichnet man dies als „Extranet-VPNs“. Mehrere Firmen, die unterschiedliche Ansätze haben können, können durch einem Extranet eine virtuelle Verbindungen mit anderen Firmen verknüpft.
Ein VPN bildet ein rein privates Netzwerk ab, auf das nun Angehörige der eigenen Firma oder Organisation Zugriff haben und das nur einige Standorte miteinander verbindet. Ein Extranet-VPN hingegen öffnet das private Netzwerk auch für externe Personen oder Organisationen und gewährt diesen Zugriff auf Ressourcen im Unternehmensnetzwerk.

Die beteiligten Organisationen (Hersteller / Zulieferer) haben unterschiedlich beschränkte Zugriffe auf das Extranet. Es lassen sich weitere Vorteile für ein Extranet- VPN aufzählen.

- Ein weitgefächerte Erreichbarkeit des Unternehmens
- Ein größere zeitliche Effizienz der Geschäftsprozesse
- Ein bessere Zusammenarbeit innerhalb des Unternehmens
- Ein Verbesserung der Zusammenarbeit innerhalb der Wertschöpfungskette im Bereich der Zulieferer
- Ein frühere Investitionsrückgewinnung[21]

---

[20] Gerhard Lienemann, Virtuelle Private Netzwerke Aufbau und Nutzen 2002, S 40

[21] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005

Eine solche Verknüpfung der Kommunikation kann aus verschiedenen Gründen erfolgen:

- Ein mit der Betreuung des Produktionssystems beauftragter Wartungspartner muss zur Administration und Fehleranalyse direkt auf das kritische System zugreifen können.
- Zur Optimierung der Kommunikation zwischen Kunde und Lieferant ist eine unmittelbare Verbindung beider Netzwerke erforderlich. So können wichtige Geschäftsdokumente (Bestellungen, Lieferscheine, Versandpapiere usw.) in elektronische Form direkt und schnell übermittelt werden.
- Für die regelmäßige Durchführung von Übersetzungen werden externe Übertragungsbüro beauftragt. Hier ist eine schnelle und direkte Übermittlung der Originaldokumente sowie der übersetzten Endprodukte relevant. [22]

Ein Extranet kann über das Backbone eines einzigen Netzbetreibers geschalte sein. Es können jedoch auch mehrere Netzbetreiber und sogar autonome Systeme somit existiert ein gravierender Unterschied zum Intranet- VPN, in dem Zugangskontrollmechanismen den beschränkten Zugriff der unterschiedlichen Organisationen regeln.

In einem End- to- End – VPN erfolgt die Verschlüsselung häufig direkt zwischen zwei Endgräten über den gesamten Kommunikationsweg hinweg. Beide Seiten sind mit einer VPN- Client-Software ausgestaltet und müssen die öffentlichen Schlüssel aller Kommunikationspartner kennen. Bei der Kommunikation über das Internet benötigt jeder VPN- Client eine offizielle feste IP- Adresse. Ein VPN dieser Kategorie kann Z.B zwischen dem Arbeitsplatzrechner einer Zuliefererfirma und der Produktionsfirma, die mit dem Zulieferer Zusammenarbeitet, geschaltet sein. Dabei kann eine Kommunikationsverbindung direkt zum Intranet- Server des Herstellers eingerichtet werden. Häufig entsteht eine Ende-zu –Ende- Verbindung. [23]

Extranet- VPN werden also auf der Basis der normalen VPN- Technologie aufgebaut, aber die Datenpakete stammen nicht von eigenen Mitarbeitern und müssen deshalb gesondert behandelt

---

[22] Gerhard Lienemann, Virtuelle Private Netzwerke Aufbau und Nutzen 2002, S 42

[23] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005

werden. Dies kann entweder das VPN- Gateway selbst tun, oder man übergibt die Pakete einem speziell dafür ausgelegten System, meist einer Firewall.

In kleinen Netzen kann man aus Kostengründen auch Firewalls und VPN- Router miteinander auf einer Plattform erstellen Allerdings haben viele gute VPN- Router auf ihrem öffentlichen Interface kann und damit das System sehr gut von Angriffen geschützt wird.

1.4.3 Remote- Access- VPN (End- to- Site)

Ein End- to- Site – VPN ist eine Mischung und den ersten beiden Varianten. Sie dient dem Aufbau von Remote – Access – VPN, wenn ein externer Client eine verschlüsselte Verbindung zum Firmennetz benötigt. Die Verschlüsselung erfolgt vom Client zum VPN – Gateway wobei derzeit noch alle Clients mit einer VPN- Client- Software ausgestaltet werden müssen.[24]

Ein Remote- Access VPN ermöglicht es, von entfernten Systemen auf ein Unternehmensnetz zuzugreifen. Auf herkömmliche Weise erreicht man dies durch den Einsatz von RAC im Unternehmensnetz. Ein RAC I(Remote Access Concentrator) ist ein System, das an öffentliche Telefonnetze angeschlossen wird und die analoge oder digitale Einwahl in diese Netze ermöglicht.[25]

Die klassische Anwendung eines Remote – Access- VPN ist die Anbindung von Außendienstmitarbeitern. Z.B bei Versicherungsunternehmen ergreifen die Versicherungsvertreter die Initiative, um mit dem Firmennetz eine Verbindung herzustellen.

Heutige Remote- Access- Konzentratoren technisch ist sehr komplex und damit auch meist sehr teuer. Weiterhin müssen solche Geräte auch skalierbar sein, da die Anzahl der benötigten Ports in der Regel stetig wächst. Skalierbarkeit bedeutet in diesem Kontext nicht nur, dass eine

---

[24] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005, S 190

[25] Manfred Lipp VPN- Virtuelle Private Netzwerke Aufbau und Sicherheit, S 37

ausreichend große Anzahl von Einwahlports verfügbar sein muss, sondern auch, dass die interne Verarbeitungskapazität und die Anbindung an das Intranet ebenfalls mitwachsen müssen, andernfalls entsteht zunehmend ein Performance- Eng pass. Somit sieht man sich mit einer Reihe von Anforderungen und den damit verbundenen Kosten konfrontiert, die einen Remote- Access- Dienst üblicherweise sehr kosten intensiv machen.

Seit geraumer Zeit können sich Firmenmitarbeiter via Modem ins Firmennetz einwählen allerdings mit einer inzwischen überhalten Übertragungsleistung. Diese Möglichkeit fordert die Unternehmen die Installation von Modempools, entsprechende Räumlichkeiten und geschultes Personal ab. Mit einem Remote- Access- VPN fallen diese häufig aufwändigen Randbedingungen weg und ermöglichen eine Kostenreduktion bei gleichzeitigem Übertragung und Informationsgewinn für die Außendienstarbeiter des Unternehmens.[26]

Man muss eine relativ teure Technologie zum Terminieren der verschiedenartigen Verbindungen aus dem öffentlichen Telefonnetz beschaffen und warten.
Die Technologie muss ständig an neue technische Gegenheiten und wachsende Kapazitäten angepasst werden.
Ein Remote- Access- VPN befasst sich mit genau diesen kritischen Faktoren, die einen Remote – Access- Dienst sehr teuer und aufwändig machen können. Sein Ziel ist es, die Hardware zum Terminieren der Verbindungen kostengünstig und einfach zu halten und die Verbindungsgebühren zu minieren. [27]

Ein Remote- Access- VPN besteht aus einem VPN- Gateway oder VPN- Router , der die virtuellen Remote- Access- Verbindungen terminiert, und Software Clients, die auf den entfernten Rechnern installiert werden, um die Verbindungen aufzubauen.

---

[26] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005, S 190

[27] Manfred Lipp VPN- Virtuelle Private Netzwerke Aufbau und Sicherheit, S 38

Im Prinzip gibt es für solch ein Szenario zwei Möglichkeiten, um ein Remote- Access – VPN aufzubauen.
Client- initiiert: Über die Einwahl Software auf dem Laptop des Außendienstmitarbeiters wird eine sichere IP- Verbindung zum Internet Service Provider aufgebaut und zum Unternehmensnetz weitergeleitet.
Server – initiiert: Vom Client – Rechner (Laptop) wird einen nichtsichere Verbindung zum ISP aufgebaut und erst der Network Access Server (NAS) stillt anschließend eine sichere Verbindung über das öffentliche Netz zwischen Client- Rechner her.[28]

Bei Kostenvergleichen, die aus Anschlussgebühren, zeitabhängigen Tarifen, Entfernungszonen und Verbindungszeiten bestehen, kann man Einsparungen im Bereich von mehr 50 % erzielen. Die viele Unternehmen ausgeben bei den Gesamtsummen pro Jahr für normales Remote Access.

1.4.4 Branch Office VPN

Branch Office- VPNs ersetzen die herkömmlichen WAN- Verbindungen, mit denen man verschiedene Standorte oder Netzwerke in diesen Standorten miteinander verbindet. Der Begriff Branch- Office- VPN hat sich mittlerweile weitgehend für diesen VPN – Typ durchgesetzt, gelegentlich spricht man auch von Site- to – Site VPN. Warum besteht überhaupt eine Notwendigkeit, bisherige Weitverkehrsnetze, die mit verbreiteten Technologien wie Standortfestverbindungen, Frame Relay oder ATM eingerichtet werden, durch ein VPN zu ersetzen? Auch hier gibt es einen Hauptgrund, nämlich die hohen Kosten durch die relativ hohen Verbindungsgebühren- ganz besonderes dramatisch sind die Kosten, wenn die zu verbindenden Standorte sehr weit voneinander entfernt oder gar im Ausland liegen. Je nach Anzahl, Entfernung, benötigter Bandbreite und zu übertragender Datenmenge kommen da schnell sehr hohe Kosten zusammen.[29]

---

[28] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005, S 191

[29] Manfred Lipp VPN- Virtuelle Private Netzwerke Aufbau und Sicherheit, S 41

2. Grundsätzliche Anforderungen

2.1. Sicherheit

Der Bergriff der Computer bzw. Datensicherheit umfasst all jene Maßnahmen, die die Daten und Programme einzelner Benutzer und Systeme vor zufälligen oder beabsichtigten Zugriffen schützt. Konnte IBM im Jahre 1975 als größter und einflussreichster Hersteller von Datenverarbeitungssystemen noch folgende Definition „Security := Rpevetion of access to or use of data or programs without authorization“ liefern.

Zu den Absicherungsmaßnahmen zählen sowohl technische als auch organisatorische Vorkehrungen, um Vertraulichkeit, Verfügbarkeit, Integrität und Beherrschbarkeit zu gewährleisten. Nur langsam setzt sich in den Unternehmen die Auffassung durch, eine eigene Sicherheitsstrategie für die Informations- und Kommunikationsverarbeitung entwerfen zu müssen.[30]

IT – Sicherheit werden stets von mehreren Seiten, aus Sicht verschiedener Gruppen verteilt. Auf diese Weise werden die Systemanforderungen aller Beteiligten- Systembetreiber, Hersteller und Benutzer- berücksichtigt. Sichere Systeme müssen beherrschbar sein. Wenn die Rechte oder persönlichen Belange weder direkt noch indirekt durch das Vorhanden sein bzw. durch die Nutzung von Informations- Kommunikation Systeme unzulässig beeinträchtigt werden dürfen, wird IT- Sicher System herstellt.

Das Sicherheitsmodell ermöglicht nicht nur die optimale Einbettung eine VPN, sondern bietet auch die Grundlage für eine umfassende Kommunikationsstrategie mit Geschäftspartnern, Zulieferfirmen und Endverbrauchern.

Gebildete VPN bedürfen also unbedingt zusätzlicher Maßnahmen, um die notwendige Sicherheit insbesondere für Tunnel über das Internet zu erreichen. Die Annahme, dass Einpacken allein schon ein gewisses Maß an Sicherheit gewährleistet, ist eindeutig als falsch zu bezeichnen. Dies gilt umso mehr, als es bezüglich der Sicherheitsansprüche und Unterschiede gibt. Um Gefahren

[30] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005,S 60

kennen, denen es zu begegnen gilt. Bei der Übertragung von Daten ist allgemein mit den folgenden Sicherheitsrisiken zu rechnen:

- Die Daten werden während der Übertragung durch Unbefügte mitgelesen.
- Die Daten werden während der Übertragung verändert oder gezielt manipuliert.
- Die Daten werden während der Übertragung aufgezeichnet und dem Empfänger unbemerkt wiederholt zugesendet.
- Ohne dass der Empfänger es merkt, werden Daten von einer nicht autorisierten Quelle empfangen.
- Ohne dass der Empfänger es merkt, werden von einer autorisierten Quelle veränderte oder gezielt manipulierte Daten empfangen.[31]

Der Aufbau der neuen Informationssysteme bringt nicht nur Vorteil mit sich, da Aufwand und Zeit eingespart werden können, sondern es entstehen auch neue Risiken und Gefahren quellen. Durch technisches oder menschliches Versagen, durch höhere Gewalt, durch vorsätzliche oder fahrlässige Handlungen oder auch organisatorische Mängel können Schäden unterschiedlicher Art und Höhe verursacht werden.

Die Anforderungen lassen sich in wenigen Stichworten zusammenfassen.

1. Vertraulichkeit: weder unbefugte Einsichtnahme von Daten, unbefugtes Erschließen von Informationen noch unbefugtes Interpretieren von Daten.
2. Integrität: keine unbefugte , unbemerkte Veränderung der Daten oder Funktionen des Systems.
3. Authentizität : Sicherheit der Echtheit von Daten und Quelle

Bei der Auswahl der geeigneten Technologie muss man sehr genau untersuchen, welche Anforderungen an das VPN gestellt werden. In der Regel resultieren diese aus

[31] Jörg Buckbesch, Rolf- Dieter Köhler, VPN Virtuelle Private Netze, Sichere Unternehmenskommunikation in IP-Netzen, S 35

Sicherheitsbedürfnissen, gefolgt von Kostenaspekten, der Verfügbarkeit und abhängig von den eingesetzten Applikationen den benötigten Bandbreiten und tolerierbaren Verzögerung zeigten.[32]

2.1.1 Verschlüsselung

Eine der Aufgabe eines Secure VPN in Bezug auf die VPN- Overlay- Techniken – besteht darin, die zu übertragenen Daten für unbefugte Dritte unleserlich und unsichtbar zu machen. Man will aber nun die Leistungsfähigkeit von Verschlüsselung und den daraus generierten VPNs fachlich beurteilten, so reicht diese Basisinformation natürlich nicht aus und man muss die Detail-Charakteristika genau kennen. Vertraulichkeit wird bei der Datenübertragung sichergestellt.[33]

Datenpakete bzw. IP- Pakete werden auf ihrem Wege über unsichere und öffentliche Netze bzw. Netzknoten in einer besonderen Art und wie die Möglichkeit der Reversibilität genutzt wird.

Die Grundgedanke der Verschlüsselung ist leicht vermittelbar: Als Prinzipien werden der geschickten Buchstabenvertauschung und der Buchstabenersetzungen eingestellt.

Eine Nachricht wird unter Verwendung eines speziellen Mechanismus verschlüsselt und, dann in eine verschlüsselte Nachricht übertraget. Auf Basis des speziellen Mechanismus der Verschlüsselung wird rückgängig gemacht und Originalnachricht zurückgeholt.

Die wissenschaftliche Entwicklung, die sich mit der Ver- und Entschlüsselung von Daten beschäftigt wird „Kryptographie“ genannt. Die grundlegende Aufgabe der Kryptographie besteht in der Geheimhaltung von übertragenen oder gespeicherten Informationen vor Unbefugten.

---

[32] Manfred Lipp VPN- Virtuelle Private Netzwerke Aufbau und Sicherheit, S 53

[33] Gerhard Lienemann, Virtuelle Private Netzwerke Aufbau und Nutzen 2002

2.1.1.1 Symmetrische Kryptosysteme

Kennzeichnend für symmetrische Kryptosysteme ist, dass für die Chiffrierung und Dechiffrierung dieselben geheimen Schlüssel benötigt werden. Oft wird diese Eigenschaft in der Literatur mit dem Begriff Secret- Key – Verfahren genannt. Heutzutage werden vornehmlich symmetrische Kryptosysteme verwendet, wenn Sender und Empfänger erreichen wollen, dass die zwischen ihnen ausgetauschten Nachrichten geheim bleiben sollen.

Der praktische Einsatz von symmetrischen Kryptosystemen wird heute gerne in Kombination mit speziellen Verfahren, die einen sicheren Schlüsselaustausch garantieren, ergänzt.

Ein Vorteil der symmetrischen Kryptosysteme gegenüber asymmetrischen Verfahren liegt in der hohen Geschwindigkeit beim Verschlüsselungsvorgang. Heutzutage weit verbreitete symmetrische Verfahren sind DES, AES, Triple DES, IDEA und Blowfisch, die im Internet und auch bei IPSEC, dem wohl derzeit bedeutendsten Verschlüsselungsverfahren für VPN, zur Anwendung kommen. [34]

Im Detail betrachtet werden folgende Komponenten bei einer Verschlüsselung zusammengefügt.

- Das Verschlüsselungsverfahren (mathematischer Algorithmus)
- Der geheime Schlüssel (Passwort)

Während das Verschlüsselungsverfahren den mathematischen Algorithmus repräsentiert und im allgemeinen öffentlich zugänglich ist, stellt der Schlüssel das Passwort dar, das beim Verschlüsselungsvorgang benutzt wird, um die Originalnachricht unkenntlich zu machen. Ein Schlüssel ist nicht mit einem einfachen Passwort zu vergleichen, sondern umfasst in der Regel eine nur schwer Bitfolge.[35]

---

[34] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005,S 99

[35] Gerhard Lienemann, Virtuelle Private Netzwerke Aufbau und Nutzen 2002, S 44

Ein weiteres Anwendungsgebiet der symmetrischen Verfahren ist die Authentifizierung, die in der Regel auf dem Besitz eines Geheimnisses beruht. Auf diese Weise kann ein Passwort mit der Identität festgestellt werden.

2.1.1.2 Asymmetrische Kryptosysteme

Die asymmetrische Verschlüsselung, auch als Public- Key – Kryptographie bekannt, bedeutet, dass zum Ver- und Entschlüsseln zwei unterschiedliche Schlüssel benutzt werden müssen. Dabei kann der Schlüssel, der zur Verschlüsselung genutzt wird, öffentlich bekannt sein

Die moderne Kryptographie liefert die Schlüssel und Schlösser des Informationszeitalters und bildet somit einen Eckpfeiler des Interneterfolges. Der Austausch digitaler Informationen ist zu einem wichtigen Bestandteil unserer .Gesellschaft geworden. Anwendungsgebiete der modernen Kryptographie sind unter anderem die digitale Signatur, die Public-. Key – Infrastruktur und die VPN- Technologie. [36]

Das Asymmetrische Verschlüsselungsverfahren RSA wurde 1978 von seinen Entwicklern Rivest, Shamir und Adleman veröffentlicht. Es ist heute das meist verbreitete asymmetrische Verfahren. RSA basiert auf der Nutzung eines Schlüsselpaars, bestehend aus öffentlichem und privatem Schlüssel.

2.1.2 Authentifizierung

Die Authentifizierung spielt wichtige Rolle im allen Bereichen des privaten und geschäftlichen Lebens. Durch die Charakteristik einer Beziehung zwischen Privatperson oder Geschäftspartnern wird bestimmt, ob der Partner dieser Beziehung kennengelernt oder vertrauet wird.

[36] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005,S 119

Erst wenn sich die Beziehung auf einer höheren Vertrauensbasis befindet, können die eigentlich Kommunikations- und Geschäftsprozesse in der angestrebten Qualität abgewickelt werden.[37]

Diese Problematik wird auf einen einfachen Nenner gebracht, so entstehen drei Verfahren, die zur Authentifizierung herangezogen werden können.

- Auf die Echtheit einer Person oder eines Rechnersystems, einer Software, eines Dokumentes usw.

Es gibt viele verschiedene Verfahren zur Überprüfung dieser Authentizität. Angewendete Verfahren zur Authentifizierung per Augenschein ist einfachste und sicher. Eine Authentifizierung durch Augenschein ist hier natürlich nicht ohne weiters möglich. Technische Verfahren, wie Beispielweise „biometrische Authentifizierung", erzielten in den letzten Jahren beachtliche Erfolge. Obwohl Systeme zur Identifikation von Fingerabdrücken oder zur Analyse unverwechselbarer Körpereigenschaften schon bereits verfügbar sind, werden allerdings infolge geringer Akzeptanz und noch bestehender Unverlässigkeit nur selten eingesetzt.

- Zur Authentifizierung der eigenen Identität recht einfach

Hierbei handelt es sich in der Regel um Benutzername und Passwort. Letzteres ist zumindest nur dem individuellen Benutzer A bekannt und bleibt allen anderen Benutzern, die nicht der Identität von Benutzer A entsprechen, verborgen. Da ein Passwort allerdings nicht untrennbar mit der Identität von Benutzer A verbunden ist und weitergegeben werden kann, ist mit diesem Verfahren eine eindeutige und unverwechselbare Authentifizierung nicht möglich.[38]

- Zur Bestimmung der eigenen Identität

Die Ausweise werden in unterschiedlichster Form zur Authentifizierung herangezogen. Ausweise sind für unterschiedliche Authentifizierungsprozesse (Personalausweis, Führerschein, Kreditkarte usw.) Ausweise helfen zwar über das Gedächtnis der Person, ist aber Verwaltung schwer. Weil sie alle jederzeit verfügbar sein müssen und damit bei sich getragen werden.

---

[37] Gerhard Lienemann, Virtuelle Private Netzwerke Aufbau und Nutzen 2002, S 57

[38] Gerhard Lienemann, Virtuelle Private Netzwerke Aufbau und Nutzen 2002, S 58

2.1.2.1 Biometrik

Die Biometrik beschäftigt sich mit der Frage nach der Identität einer Person durch die Analyse biologischer Merkmale. Aber zunehmende diesen Techniken werden in Wissenschaft, Industrie oder Behörde versucht, verlässliche Authentifizierungsverfahren zu entwickeln.

Allerdings sind einige dieser Verfahren allein auch noch sehr schwach. Es stellt beispielsweise kein großes Problem dar, sich von einer Person Fingerabdrücke zu beschaffen- man hinterlässt ja genug. Auch hier ist die Kombination von biometrischen Verfahren mit anderen erforderlich.[39]

Biometrische Merkmale sollten folgende Voraussetzungen erfüllen.

- Eindeutige Zuordnung zu einer einzigen Person.
- Keine wesentliche Veränderung im Laufe der Alterungsprozesses
- Messbarkeit- Messmethoden und Geräte müssen bekannt und hinreichend getestet sein.
- Messkosten- die anfallenden Kosten für die Messung müssen vertretbar sein.[40]

2.1.2.2 Passworte

Die Sicherheit hängt bei der Authentifizierung über Passworte von zahlreichen Faktoren ab:

- Passwortqualität – Die beliebte Verwendung von Vornamen oder Modeworten werden leicht abgeschätzt, deshalb diese Passworte in höchstem Maße unsicher ist.
- Passwortkomplexität – Kurze Passworte können leicht ermittelt werden. Bei kurzen Passworten werden Rechnergestützte „Brute – Force- Verfahren“ in weniger Sekunden gefunden können.

[39] Manfred Lipp VPN- Virtuelle Private Netzwerke Aufbau und Sicherheit, S 148

[40] Gerhard Lienemann, Virtuelle Private Netzwerke Aufbau und Nutzen 2002, S 59

2.1.2.3 Signaturen und Zertifikate

Digital Signatur wird zur Erreichung eines hohen Sicherheitsstandards bei der Datenkommunikation verwendet. Digitale Zertifikate lösen das Problem der nicht zweifelsfrei feststellbaren Herkunft des öffentlichen Schlüssels einer Person, der zur Entschlüsselung von Digests, aber auch von verschlüsselten Nachrichten, verwendet wird.

Wie kann bei der Übermittlung einer Nachricht sichergestellt werden, dass sie authentisch ist, d.h. eine Manipulation der Nachricht während der Übertragung ausgeschlossen werden kann?

Man bedient sich dabei eines sehr einfachen Mechanismus: Die Nachricht wird mit einem Fingerabdruck des Erstellens, einem Digest versehen. Dieser wird ermittelt, indem die Originalnachricht mit einem „Hash- Algorithmus „ bearbeitet wird. [41]

2.2 Verfügbarkeit

Ein virtuelles privates Netzwerk soll traditionelle Weitverkehrs, oder Remote- Access- Lösungen ergänzen oder ganz ersetzen. Dies bedeutet aber auch, dass ein VPN eine Verfügbarkeit bieten muss, die nicht unter der von herkömmlichen WAN- Infrastrukturen liegt. Denn üblicherweise investiert man nicht in eine Technologie, die qualitativ schlechter ist als die aktuelle. Es sei denn, die neue Technologie bietet enorme Kostenvorteile. [42]

Der Remote Access wird über entsprechende PC- Karten oder externe Geräte mittels Wählverbindungen über das analoge oder digitale Fernsprechnetz, bei Bedarf auch über das Mobilfunknetz, aufgebaut und in einem Remote- Access –Konzentrator terminiert.

Für viele Remote- Access – Infrastrukturen ist die so genannte << Niemals besetzt >> Eigenschaft eines Telefonnetzwerks ebenso wichtig. Haben Sie schon jemals am soeben

[41] Gerhard Lienemann, Virtuelle Private Netzwerke Aufbau und Nutzen 2002, S 65

[42] Manfred Lipp VPN- Virtuelle Private Netzwerke Aufbau und Sicherheit, S 59

abgehobenen Hörer eines am öffentlichen Fernsprechnetz angeschlossenen, funktionsfähigen Telefonapparates kein Freizeichen gehört? Vermutlich nicht. Wenn nun mehr Zugangskanäle in ein Unternehmensnetzwerk gelegt werden , als es potenzielle Benutzer gibt, kann man sich damit eine Remote- Access- Lösung mit tatsächlich garantiertem Zugriff aufbauen, da man selbst Einfluss auf die Auslegung seiner Systeme hat. Dies ist in vielen Fällen ein entscheidendes Kriterium, zum Beispiel beim Einsatz von Applikationen für Buchungs- oder Reservierungssysteme.

Verfügbarkeit bietet folgende Eigenschaft,

- Gewährleistung einer hohen Verfügbarkeit des VPNs auf hohem Niveau in Prozent
- Prozentuale Verringerung der Zeitintervalle zwischen zwei Wartungsfenstern
- Bereitstellung fester Bandbreiten für individuelle Anwendungen insbesondere für Geschäftskriterium Applikationen [43]

2.3 Skalierbarkeit

Bei der Planung eines VPN ist die Skalierbarkeit im Bereich der Systemleistung einer ganz wichtigen und kritischen Anforderung. Meist sind Standorte verschiedener Größe, Heimbüros und mobile Mitarbeiter mit der notwendigen Technologie auszustatten. Je nach Einsatzgebiet sind unterschiedliche Datendurchsätze und Anschlusstechnologie notwendig, vom redundanten VPN- Konzentrator bis hinunter zur VPN- Client- Software für PCs. Idealerweise sollen diese verschiedenen VPN- und Managementoberfläche bieten.

[43] Gerhard Lienemann, Virtuelle Private Netzwerke Aufbau und Nutzen 2002, S 29

2.4 Interoperabilität

Interoperabilität ist ein wesentliches Entscheidungskriterium an heutige VPN- Konzetrator und VPN- Gateways. Dies hat gleich mehrere Gründe. Je nach Auswahl eines geeigneten Tunneling-Modells können mehrere Partner an einem VPN beteiligt sein, die unter Umstände Equipment verschiedener Hersteller einsetzen.[44]

Interoperabilität zwischen Produkten verschiedener Hersteller ist bei virtuellen privaten Netzwerken in den heutigen Netzwerkumgebungen unverzichtbar. Zum Beispiel, die mögliche Übernahme von Unternehmen, die Notwendigkeit, Unternehmensnetzwerke auf Lieferanten und Partner auszudehnen, und die unterschiedlichen Geräte innerhalb von Unternehmensnetzwerken.[45]

[44] Manfred Lipp VPN- Virtuelle Private Netzwerke Aufbau und Sicherheit, S 85

[45] Joseph Davies, Elliot Lewis, Virtuelle Private Netzwerke mit Winndows Server 2003 Sichere Netzwerkanbindung mit VPNs, 2004, S 49

3. VPN Tunneling

3.1 Prinzip und Grundlage Tunneling Modelle

Viele VPN- Produkte setzen Tunneling zum Aufbau eines privaten Netzes ein. VPNs ermöglichen, sich über das Internet, das ein IP- Netz darstellt, mit einem fernen Netz zu verbinden.

Das Grundprinzip aller Tunnel- Protokolle ist das Verpacken (Encapsulation) der Anwendungsdatenpakete in die Datenpakete des Transportprotokolls. Bei Verwendung von IP als Transportprotokoll werden die ursprünglichen Pakete der Anwendung unverändert in das Datenfeld der IP- Pakete eingetragen. [46]

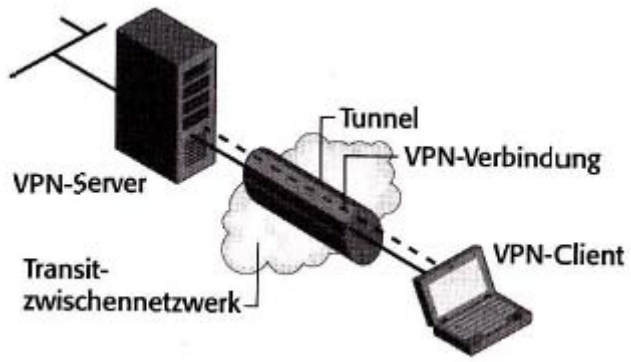

Abb. 4 : Die VPN Verbindung

Quelle: Scott Charlie, Virtuelle private Netzwerk

[46] Jörg Buckbesch, Rolf- Dieter Köhler, VPN Virtuelle Private Netze, Sichere Unternehmenskommunikation in IP-Netzen, S 21

Mit Hilfe dieser Technologie kann man Pakete eines Netzwerkprotokolls in Pakete eines anderen Netzwerkprotokolls kapseln und über dieses Netzwerk übertragen. Die gekapselten Pakete werden zwischen Tunnelendpunkten über das Zwischennetzwerk geroutet. Der logische Pfad, durch den die gekapselten Pakete durch das Zwischennetzwerk reisen, wird als Tunnel bezeichnet. Es gibt viele Beispiele für Tunnel, die über das Zwischennetzwerk eines Unternehmens geleitet werden. Beispielweise, zum Transport von IP- Paketen über anderen Netze ist IP- over- ATM, IP- over – Frame- Relay. Es wird auch verwendet, wenn IPv6 Pakete über ein IPv4 ausgelegtes Teilnetz geführt werden sollen. Das Internet ist zwar eines der allgegenwärtigsten und kostengünstigsten Zwischennetzwerke.[47]

Tunneling gibt die Möglichkeit, ein Paket in ein anderes Paket zu kapseln und damit inkompatible Protokolle zusammenzubringen. Das gekapselte Paket kann demselben, aber auch einem völlig anderen Protokoll angehören. Dies bietet die Möglichkeit, Pakete mit beliebigen Ziel- und Quelladressen im Internet zu verschicken.[48]

Erst am entfernte Tunnel- Ende, dem Zielpunkt des transportierenden IP- Pakets, muss der Inhalt des Datenfelds wieder als ein anderes, eingepacktes Protokoll erkannt, entpackt und bearbeiten werden. In der Art des Verpackens und der Kommunikation der Tunnel – Endpunkte untereinander liegen die Unterschiede der VPN- Protokolle.[49]

Durch Tunneling kann man zum Beispiel IPX- Pakete durch ein IP- Netzwerk transportieren. Ein andere, speziell für IP- Netze interessante Anwendung ist das Verstecken von privaten, nicht

---

[47] Joseph Davies, Elliot Lewis, Virtuelle Private Netzwerke mit Windows Server 2003 Sichere Netzwerkanbindung mit VPNs, 2004, S 17

[48] Gerhard Lienemann, Virtuelle Private Netzwerke Aufbau und Nutzen 2002

[49] Jörg Buckbesch, Rolf- Dieter Köhler, VPN Virtuelle Private Netze, Sichere Unternehmenskommunikation in IP-Netzen, S 32

registrierten Netzwerk- und Host- Adressen, indem man IP in IP tunnelt. Auf diese Weise kann man seine privaten Netze über das Internet miteinander verbinden.[50]

Beim Tunnelmodus wird auch der IP- Header verschlüsselt, so dass die Generierung eines neuen IP- Headers erforderlich wird, der das Routing des Paketes vornehmen muss. Dieses Verfahren gewährleistet eine sehr hohe Datensicherheit, da das gesamte Originalpaket unkenntlich gemacht wird und somit für Dritte nicht mehr ausgelesen werden kann. Der Tunnelmodus kommt meist dann zum Einsatz, wenn aus den jeweiligen Zielnetzen ein geringeres Gefährdungspotenzial hervorgeht als das eigentliche Transportnetz.[51]

Man kann die Tunneling- Protokolle in zwei verschiedene Klassen einteilen: Die Layer-2 Tunneling- Protokolle und die Layer-3 – Tunneling Protokolle. Die Unterscheidung basiert auf der Schicht des OSI oder IP – Schichten – Modells, deren Pakete eingekapselt. Layer-2 Protokolle kapseln Pakete der Sicherungsschicht in andere Pakete, meist solche der Schicht 3 ein. Layer – 3 – Protokolle kapseln Pakete der Netzwerkschicht(Layer 3) in andere Pakete der Netzwerkschicht ein.[52]

Normalerweise werden die Daten einer Anwendung zum Transport in Pakete des jeweiligen Netzprotokolls unterteilt und mit dem für die Paketsteuerung im Netz erforderlich Paketkopf (Header) versehen. Da so entstanden Datenpaket der Ebene 3 wird im Datenfeld eines Rahmens der Ebene 2 entsprechend der verwendeten Netzwerktechnologie transportiert.

Das Besondere an VPN- Verbindungen besteht nun darin, dass die normalerweise für die Übertragung fertigen Rahmen nochmals in das Ebene- 3- Protokoll IP eingepackt werden. Das

---

[50] Charlie Scott, Paul Wolfe, Mike Erwin, Virtuelle Private Netzwerke, S 6

[51] Gerhard Lienemann, Virtuelle Private Netzwerke Aufbau und Nutzen 2002, S 85

[52] Manfred Lipp VPN- Virtuelle Private Netzwerke Aufbau und Sicherheit, S 172

resultierenden IP- Paket fungiert praktisch wie ein Container und kann über jedes IP – Netz transportiert werden, das sein Inhalt für die Übertragungssysteme nicht von Bedeutung ist.[53]

3.2 Layer 2 Protokolle

Die hier beschriebenen Protokolle sind in Schicht 2 des OSI- Referenzmodells für Kommunikationsprotokolle, der sogenannten Sicherungsschicht (Data Link Layer), angesiedelt. Der Data- Link Layer wird auch oder Network Access Layer genannt. Es ist die niedrigste Schicht im TCP/IP – Protokollstack. Beispiele für den Data- Link Layer sind unter anderem Ethernet (IEEE 802.3), Token Ring (IEEE 802.5) und ATM (Asyncronous Transfer Mode). Von diesen 3 ist Ethernet am weitesten verbreitet.

Jedes Gerät im Netzwerk untersucht die Pakete und stellt fest, ob die Medium access controll (Mac)- Adresse, auch Hardwareadresse genannt, mit der Zieladresse des Pakets übereinstimmt. Empfängt der Data-Link- Layer ein Paket vom Network- Layer, der Schicht über ihm, so versieht er dieses mit einem passenden Header (Encapsulation), beispielsweise mit einem Ethernet-Header, bevor er es sendet. Der Ethernet- Header beinhaltet Information, wie zum Beispiel die Quell- und Zielhardwareadresse. Diese Sicht benutzt IP- Adressen, um Elemente im Netzwerk zu identifizieren. Wie auch immer, der Data-Link Layer arbeitet mit Hardwareadressen.[54]

Die Protokolle der Sicherungsschicht(Layer-2) unterstützen alle Zugangsverfahren, angefangen vom High Level Data Link Control (HDLC), Logical Link Control (LLC), CSMA/CD, Token-Bus und Token- Ring bis zu FDDI.[55]

Sie sind für das Tunneling durch IP zuständig. In Schicht 2 arbeitet zum Beispiel auch das Protokoll PPP. PPP wird üblicherweise dazu eingesetzt, IP und andere Protokolle über serielle

---

[53] Jörg Buckbesch, Rolf- Dieter Köhler, VPN Virtuelle Private Netze, Sichere Unternehmenskommunikation in IP-Netzen, S 32

[54] Carlton R. Davis, IPSec Tunneling im Internet, 2002, S 18

[55] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005, S 206

und digitale Verbindungen zu leiten. PPP- Verbindungen verlaufen normalerweise zwischen einem Client und einem fernen Rechner, zum Beispiel einem Remote- Access- Server. Dementsprechend dienen PPTP, L2F und L2TP zum Tunneling von PPP- Verbindungen über das Internet, so dass sie auf einem fernen Rechner terminiert werden können.[56]

3.2.1 Point- to- Point Tunneling Protocol

Das Point -to- Point Tunneling protocol (PPTP) wurde in der Zusammenarbeit der Firma von Ascend Communications, Us Robotics, 3Com Corporation, Microsoft Coraration und ECI Telematics entwickelt. Ziel war die Bereitstellung eines virtuellen privaten Netzes zwischen Remote- Access- Benutzern und Servern im Netz.

Es stellt eine Erweiterung des Point- to- Point Protokolls (PPP) der und ist als Access- Technologie relativ weitverbreitet. Gerne wird es für einen Internetzugang im Endanwenderbereich eingesetzt. So ist dieses Protokoll bereits Bestandteil der Microsoft Betriebsysteme Windows NT, Windows 98 und Windows 95.

PPTP ermöglicht den Fernzugriff (Dial- In) auf ein Unternehmens- LAN über das Internet technologisch einfacher zu gestalten.[57]

PPTP kapselt PPP- Rahmen in IP- Datagrammen, um sie über ein IP- Zwischennetzwerk wie Beispielweise das Internet zu übertragen. PPTP benutzt für die Tunnelverwaltung eine TCP-

[56] Charlie Scott, Paul Wolfe, Mike Erwin, Virtuelle Private Netzwerke, S 63

[57] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005, S 211

Verbindung und zum Kapseln der PPP- Rahmen mit den getunnelten Daten. Die Nutzdaten der gekapselten PPP- Rahmen können verschlüsselt, komprimiert oder beides sein.[58]

Die besondere Bedeutung dieses Tunnel- Protokolls liegt in seiner Verfügbarkeit für alle Computer mit einem Microsoft Betriebssystem ab Windows 95. Es kann somit als Industriestandard bezeichnet werden.

3.2.2 Layer 2 – Tunneling Protocol

Das Layer 2 Tunneling Protocol wurde primär für den Einsatz im Provider- Enterprise – Modell entwickelt. Das L2TP – Protokoll ist das prominenteste Protokoll der Layer- 2 – Technologie. Es gibt etliche Hersteller, die Produkte auf der Basis von L2TP ein als RFC 2661 veröffentlichter Internet- Standard anbieten, und es ist als Industriestandard anerkannt nicht zuletzt, weil Cisco maßgeblich zur Entwicklung beigetragen hat.[59]

L2TP ist eine Mischform seiner beiden Vorbilder bzw. Konkurrenzprodukte L2F und PPTP. L2TP vereint die besten Eigenschaften PPTP und L2F, wobei Verbindungen vom Client oder vom Remote- Access- Server eingeleitet werden können. Bei der Entwicklung von L2TP wurden die Vorteile von PPTP und L2F kombiniert, während man zugleich versucht hat, die Nachteile beider Tunnelverfahren weitgehend zu vermeiden. Es ist überall dort einsetzbar, wo PPTP oder L2F verwendet werden.[60]

Das L2TP Grundprinzip basiert auf einer Verbindung zwischen einem L2TP- Client und einem L2TP – Server, die über einen Tunnel miteinander verbunden sind und verkapselte PPP- Pakete übertragen.

---

[58] Joseph Davies, Elliot Lewis, Virtuelle Private Netzwerke mit Windows Server 2003 Sichere Netzwerkanbindung mit VPNs, 2004, S 22

[59] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005

[60] Charlie Scott, Paul Wolfe, Mike Erwin, Virtuelle Private Netzwerke, S 64

L2TP über IP- Zwischennetzwerke nutzt UDP und eine Reihe von L2TP- Nachrichten für die Tunnelverwaltung. L2TP sendet außerdem L2TP- gekapselte PPP- Rahmen mit Hilfe von UDP als die getunnelten Daten.[61]

3.2.3 Layer 2 Forwarding (L2F)

Das Layer 2 Forwarding ist ein Layer- 2- Tunneling – Protokoll, das hauptsächlich gemeinsam von der Firma Cisco, Northern Telekom und Shiva zum Einsatz im Provider Enterprise Modell entwickelt wurde. Es gibt praktisch keine Client Implementierungen, sondern nur Softwaremodule für Remote – Access- Konzentratoren und Router. L2F ist sehr eng mit L2TP verwandt, viele L2TP- Netzwerk- Server können auch als Endpunkt für einen L2F – Tunnel dienen.[62]

Weiterhin unterstützt L2F mehr als eine Verbindung gleichzeitig ein weiterer Vorteil gegenüber PPTP. L2F erreicht diese Eigenschaft, indem in der aufgebauten Tunnelverbindung mehrere logische Kanäle geschaltet werden können.

Der L2F- Tunnel existiert nur zwischen PoP und dem Sicherheitsgateway (Router, Firewall, VPN- Gateway) und dem Netzzugangsserver (NAS) des Unternehmens.

Datenpakete werden bei L2F durch den virtuellen Tunnel zwischen den Endpunkten einer PPP-Verbindung ausgetauscht. L2F vollzieht dies auf einer unteren Protokollebene. L2F biete eine zuverlässige, sichere und skalierbare Lösung für VPN und hatte seinen technologischen Höhepunkt gegen Ende der 90er Jahre.[63]

---

[61] Joseph Davies, Elliot Lewis, Virtuelle Private Netzwerke mit Windows Server 2003 Sichere Netzwerkanbindung mit VPNs, 2004, S 22

[62] Manfred Lipp VPN- Virtuelle Private Netzwerke Aufbau und Sicherheit, S 180

[63] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005, S 210

3.2.4 Layer 3 Protokolle

Zu den Layer- 3- Techniken, die in der VPN- Technologie Verwendung finden, zählt das IPSec-Protokoll sowie das unterstützende Schlüsselaustauschprotokoll (IKE). IPSec setzt symmetrische kryptographische Schlüssel ein, um einen IP- Pakettransport gemäß den IuK- Schutzzielen abzusichern. Allerdings besitzt IPSec keinerlei Mechanismen, um die notwendigen Schlüssel für die Kommunikationspartner zu erzeugen oder zu verteilen.[64]

Das Layer- 3- Tunneling arbeitet eine Schicht höher als Layer- 2- Protokolle. Hier werden Pakete der Netzwerkschicht in andere Pakete dieser Schicht eingekapselt. Der Paket – Overhead ist geringer als der von Layer-2 –Protokoller. Allerdings muss der Tunneling- Prozess die von den höheren Schichten ankommenden Pakete analysieren und im Tunnel- Header vermerken, welche Art von Protokoll getunnelt wird.
In the case of Layer 3 tunneling protocols, all of the configuration issues are set up out of band, usually manually. For these protocols, there may be no tunnel maintenance phase.
Once the tunnel is established, it can then send the tunnelled data. The tunnel client or server uses a tunnel data transfer protocol to transfer the data. Essentially, when the tunnel client sends a payload to tunnel server, the tunnel client first appends a tunnelling protokcol header to the payload. Then the client sends the encapsulated payload across the internetwork, where it is routed to the tunnel server. Once the tunnel server receives the packets, it removes the tunnelling protocol header and then forwards the payload inside to ints intended destination.
Layer 3 protocols address the basic VPN requirements as follows:

- *User authentication: Many Layer 3 tunneling schemes assume that the endpoints are already known and authenticated prior to tunnel establishment.*
- *Token card support _ Layer 3 tunneling protocols can use methods similar to those used by Layer 2 tunneling protocols.*
- *Dynamic address assignment: Layer 3 tunneling schemes assume that an address has already been assigned before initiating the tunnel.*

---

[64] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005, S 226

- *Data encryption: Layer 3 tunneling protocols can use methods similar to those für Layer 2*
- *Key management*
- *Multiprotocol support* [65]

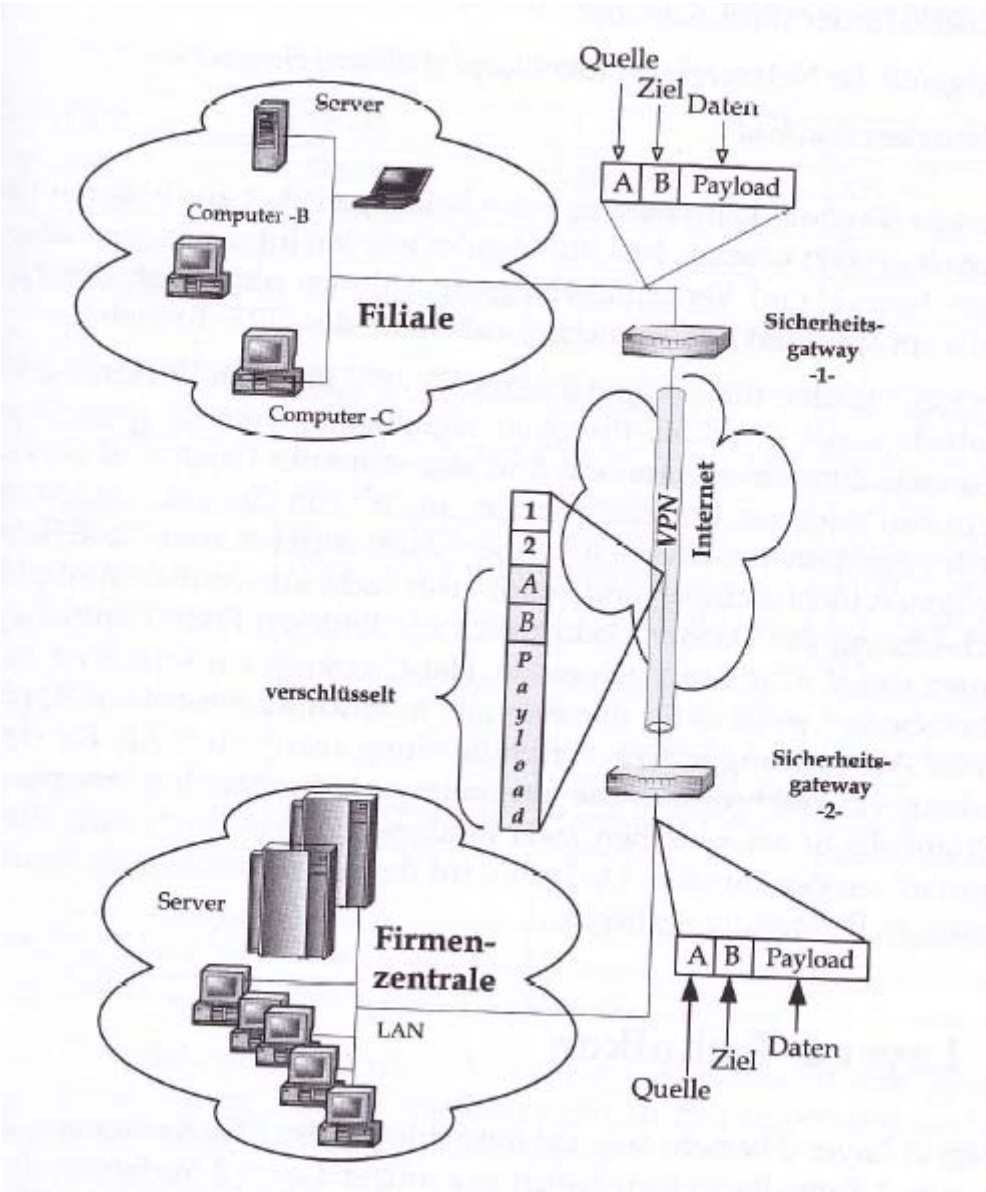

Abb. 5 : IP - Paket- Transport zwischen Filiale und Firmenzentrale mittels Tunnel durch das Internet

Quelle: Wolfgang Böhmer , VPN Virtual Private Networks, S 207

[65] John Mairs, VPNs: A Beginner`s Guide, S 264

3.2.5 IP Security (IPSec)

Der heute zu beobachtende Boom des Internet dürfte zumindest zum Teil auch darauf zurückzuführen sein, dass dieses weltweite Netz keiner Firma oder Organisation gehört und folglich keinen dementsprechenden Rechtsansprüchen und Restriktionen unterliegt. Andererseits resultiert aus eben diesem Sachverhalt ein Problem für die zunehmende geschäftliche Nutzung des Netzes, denn die Gewährleistung der erforderlichen Sicherheit gestaltet sich entsprechend schwierig. Das Internet ist nach allgemeiner Einschätzung das unsicherste Netzwerk überhaupt.[66] Ein grundsätzliches Problem des Internet Protokolls (IP) liegt darin begründet, dass es heutigen Sicherheitsanforderungen längst nicht mehr genügt. Dieses zu den ältesten Standards gehörende Protokoll der dritten Kommunikationsschicht weist einige gravierende Sicherheitsdefizite auf und ist daher für den Einsatz innerhalb Virtueller Privater Netzwerke über öffentliche Netze nicht geeignet.[67]

IPSec stellt, bezogen auf das OSI- Referenzmodell, den Sicherheitsstandard auf Layer 3 dar. IPSec ist standardisiert gemäß IETF, mit dem herstellerübergreifend ein sicherer und geschützter Datenaustausch durch das IP ermöglicht werden kann. Die Normungsaktivitäten laufen seit 1995 unter Führung von Jeffrey Schiller und Marcus Leech. Die IPSec- Arbeitsgruppe ist innerhalb der IETF der Security Area untergliedert.

IPSec beeinflusst weder die Kommunikationsprotokolle nach Anwendungsprogramme, so dass einen Zusammenarbeit über verschiedene IP- Netze nicht beeinträchtigt wird. IPSec ist im TCP/IP Schichtenmodel unterhalb der Transportschicht angesiedelt und setzt auf die Internet-Schicht (IP) auf. [68]

---

[66] Jörg Buckbesch, Rolf- Dieter Köhler, VPN Virtuelle Private Netze, Sichere Unternehmenskommunikation in IP-Netzen, S 55

[67] Gerhard Lienemann, Virtuelle Private Netzwerke Aufbau und Nutzen 2002, S 80

[68] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005, S 227

Als erstes ist festzustellen, dass es sich bei IP Security (IPSec) nicht, wie oft vermutet, um einen Standard handelt. Vielmehr sind einzelne Bestandteile des Systems IPSec auf ein ganzes Bündel unterschiedlich kombinierbarer Standards verteilt. Es handelt sich dabei im Wesentlichen um RFCs 2401 bis 2412, welche die älteren RFCs 1825 bis 1829 ablösen.

RFC 2401 legt die allgemeine Architektur des IPSec- Systems fest. Dessen Ziel ist die Bereitstellung von Sicherheitsfunktionen auf IP- Ebene sowohl für IPv4 als auch für IPv6. Es ist im Prinzip für jede Art von IP- Kommunikation nutzbar und so gestaltet, dass die resultierenden Datenströme auch über Netzkomponenten transportiert werden können, die IPSec nicht unterstützen.[69]

Zum Transport der nach IPSec modifizierten IP- Pakete sind zwei unterschiedliche Arbeitsmodi- der Transportmodus und der Tunnelmodus- definiert worden. Beide unterscheiden sich im Wesentlichen durch den Aufbau der Paketergänzungen und durch ihre Einsatzmöglichkeiten.

3.2.6. Secure Socket Layer (SSL) und Transport Layer Sicherheit (TLS)

Mit zunehmender Beliebtheit des Internet hat sich eine andere Art, ein VPN einzurichten, durchgesetzt: Bestehende http- Verbindung wird zwischen Browser und Server kryptographisch gesichert, um ein Aggression oder Verfälschen von Informationen zu abblocken. Außerdem wird nur autorisierten Kommunikationspartner miteinander Datenaustausch sichergestellt. Die aufgebaute sichere Client- / Server- Verbindung wird für Anwendungsschicht auch als SSL- VPN bezeichnet. Die gleichnamigen Browser Netscape entwickelt 1994 Socket Layer- Protokoll (SSL).

---

[69] Jörg Buckbesch, Rolf- Dieter Köhler, VPN Virtuelle Private Netze, Sichere Unternehmenskommunikation in IP-Netzen, S 55

Das Zeil, das damals von Netscape verfolgt wurde, galt der Absicherung der Transportschicht, die bis dahin Daten ausschließlich im Klartext über das Netz schickte. Mit SSL war mit der Netscape Technologie eine Verbindungsorientierte Ende-zu- Ende – Kommunikationssicherheit (Vertraulichkeit) zwischen einer Browser – Anwendung und einem Webserver möglich.[70]

Die Grundlagenfunktion von SSL – Architektur sieht das SSL- Record- Protokoll wie Vertraulichkeit und Integrität vor.

- SSL- Connection: Eine Verbindung ist im Sinne des ISO / OSI – Referenzmodells eine Transportverbindung, die geeignete Dienste bearbeitet.
- SSL- Session: Eine Session ist eine Verbindung zwischen einem Client- Browser und einem WWW- Server, die durch das Handshake – Protokoll erreicht wird. Eine Session legt unter anderem die kryptographischen Parameter für gültige SSL- Connection fest.
- SSL – Record- Protokoll: Es handelt sich um Encapsulation. Bei einer Verbindung zwischen Client und Server werden die Daten von der Anwendungsschicht gekapselt. Daten werden nicht direkt dem Betriebssystem übergetragen, sondern erst von der SSL-Schicht bearbeitet.

Eine Weiterarbeitung durch die Arbeitsgruppe (TLS Working Group) der IETF aufbaute auf SSLv3.0, führte im Jahre 1999 zu einem allgemeinen Standard. Dabei kann die erste Version des Transport Layer Sicherungsprotokoll (TLS) als eine inhaltlich geringfügige Ergänzung zur SSLv3.0 angesehen werden.[71]

---

[70] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005, S 283

[71] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005, S 283

4. Point- to- Point Tunneling Protocol (PPTP)

4.1 Funktionsweise im Überblick

Das Point-to- Point Tunneling Protocol (PPTP) ist eine Erweiterung des Point-to- Point Protocol (PPP), welches in einem als RFC 1661 bekannten Dokument der Internet Engineering Task Force (IETF) mit dem Titel "The Point to Point Protocol" (PPP) verankert ist.

PPTP wurde maßgeblich von den Firmen Microsoft und 3Com Inc. entwickelt. Die besondere Bedeutung dieses Tunnel- Protokolls liegt in seiner Verfügbarkeit für alle Computer mit einem Microsoft Betriebssystem ab Windows95. [72]

PPTP bietet den Fernzugriff (Dial- In) auf ein Unternehmens- LAN über das Internet technologisch einfacher zu erstellen. Diese Technologie wird durch die Erweiterung des PPP-Protokolls ausgerichtet.
PPTP kann sowohl als Basis für das Ende- zu –Ende- Modell bieten als auch durch Implementierungen in Remote- Access- Konzentratoren im Provider- Enterprise- Modell eingesetzt werden. Aufbau des PPTP sicht einen dem L2TP Aufbau aus. PPTP verwendet für den Steuerungskanal jedoch als TCP- Protokoll.

Generic Route Encapsulation (GRE) wurde von der Firma Cisco zum Einpacken verschiedenster Protokolle in IP entwickelt und in den RFCs 1701 und 1702 generiert. PPTP verwendet diese genannten Verfahren. PPTP kapselt als Layer- 2- Protokoll PPP Rahmen mit einem modifizierten GRE- Header ein. Sie wird erricht, indem PPP mit einem GRE- Header gekapselt und mit einem zusätzlichen Tunnel- IP- Header versehen wird. Über eine logische PPP- Verbindung kann protokollunabhängig kommuniziert werden Die Einbindung des GRE- Headers bietet dabei die Möglichkeit, andere Protokolle als IP, wie z.B. IPX und NETBUI, zu übertragen. Deshalb wird PPTP vielfach eingesetzt.

---

[72] Jörg Buckbesch, Rolf- Dieter Köhler, VPN Virtuelle Private Netze, Sichere Unternehmenskommunikation in IP-Netzen, S 25

Zu den weiteren Besonderheiten von PPTP gehören:

- Zwischen zwei gegebenen Tunnel-Enden kann immer nur ein Tunnel existent sein, in dem aber mehrere Anwendungssesions gleichzeitig aktiv sein können.
- Mit einer GRE- Headerlänge von 16 Byte generiert PPTP verhältnismäßig wenig zusätzliche Overhand beim Einpacken der Daten.
- Die Fragmentierung der Daten im transportierenden IP- Netz ist erlaubt.
- Durch die Paket Folgenummern ist eine Flusssteuerung mit Sliding- Window- Verfahren möglich.
- Die Empfangsbestätigung kann für mehrere Pakete auf einmal erfolgen. Die Wiederholung nicht empfangener oder fehlerhafter Pakete wird jedoch dem Anwendungsprotokoll der höheren Ebene überlassen.
- Die transportierenden IP- Pakete können in anderer Reihenfolge empfangen werden, als sie ausgesendet wurden.[73]

Die Verwendungsmöglichkeiten dieses Protokolls werden aus den beschriebenen Eigenschaften von PPTP sich ergeben können.

- Zwischen Tunnel-Start- und Endpunkt unter Verwendung eines IP- Netzes wird eine PPP Übertragung von PPTP erhaltet können.
- Wenn es keine Einschränkungen durch die Implementierungen der verschiedenen Hersteller gibt, kann PPTP im Prinzip jeder Anwendungssession über eine serielle PPP- Verbindung transportieren.
- PPTP ist gut geeignet für Aufbau heterogener VPN- Lösungen. Insbesondere wird PPTP das Tunnel- Protokoll der Wahl begünstigt, wenn mit Windows95 oder Windows NT4.0 gearbeitet werden soll.

[73] Jörg Buckbesch, Rolf- Dieter Köhler, VPN Virtuelle Private Netze, Sichere Unternehmenskommunikation in IP-Netzen, S 29

4.1.1 Arbeitsweise von PPTP

In seiner Rolle als Tunnel- Protokoll verpackt PPTP Netzprotokoll- Datagramme in eine IP-Hülle. Nach der Kapselung werden die Datagramme von jedem Router oder System wie IP-Pakete behandelt. Der Vorteil der IP- Kapselung besteht darin, dass verschiedenste Protokolle über ein Medium wie das Internet, das nur mit IP arbeitet, gerichtet werden können.[74]

Nachdem eine entsprechende virtuelle TCP- Verbindung von einem Eingangskonzentrator (PAC) und einem Endpunkt (PNS) aufgebaut werden, werden einen PPP- Verbindung aufgebaut werden kann. Zwischen Eingangskonzentrator (PAC) und Ausstiegspunkt (PNS) kann jeweils nur ein Tunnel aufgebaut werden. Das Out- Band- Verfahren kann zum eigentlichen Tunnel erstellen. Sie wird als Kontrollverbindung des Tunnels verwendet. Kontrollinformationen und Datenpakete werden getrennt über das Netz geleitet. Die Kontrollverbindung lässt sich in Analogie zu ISDN mit dem Kanal. Neuerdings wird der PPTP Access Concentrator einheitlich mit PAC für den Tunneleinstieg am Point- of- Present (PoP) bezeichnet. Der PPTP- Network- Server ist in (PNS) abgeändert worden und stellt den Tunnel ausstieg dar.

4.1.2 Analyse eines PPTP- Paketes

Die Kapselung von PPTP beruht auf einem weiteren Internet- Standard, dem GRE- Protokoll. Dies kann zum Tunneling von Protokollen über das Internet eingesetzt werden. Die PPTP-Version GREv2 enthält zusätzlich Funktionen wie Call IP und Verbindugsgeschwindigkeit.

Dem eigentlichen Datagramm werden 4 Header vorangestellt. PPTP- Paket besteht aus einem Delivery- Header, einem IP- Header, einem GREv2- Header und dem Payload- Paket. Als erstes kommt der Delivery- Header, der als einige Erweiterungen und den Protokollrahmen für das Transportmedium, sei es Ethernet, Frame Relay oder PPP enthält. Anschließend der GREv2 – Header, der neben der Datenfluss- und Kollisionskontrolle leitet, enthält Informationen über die

[74] Charlie Scott, Paul Wolfe, Mike Erwin, Virtuelle Private Netzwerke, S 65

Art des gekapselten Pakets sowie PPTP- spezifische Daten über die Verbindung zwischen Client und Server. Der eigentliche Header, der Tunnel- IP- Header, wird nur für die Tunnelstrecke benötigt. Der IP- Header enthält Informationen zum IP- Datagramm wie die Paketlänge sowie die Quelle- und Zieladresse. Das Payload- Paket ist das gekapselte Datagramm selbst. Im Fall von PPP beinhaltet es die ursprünglichen zwischen Client und Server ausgetauschten Daten innerhalb der PPP- Sitzung. Da Kernstück einer PPTP Verbindung auf ein GRE- Protokoll kann zurückführen, damit dieser Header am Ende des Tunnel ebenso wie der GRE- Header entfernt wird.

4.1.3 Verlauf der Kapselung

Wenn sich ein Benutzer bei einem ISP mit PPTP- Unterstützung einwählt, verläuft die Kapselung wie folgt.

- Benutzer wählt sich mit PPP beim Remote- Access- Switch des ISP ein. Zwischen Client und Remote- Access- Switch werden PPP-Pakete gesendet, die zur Auslieferung in die für das PPP- Protokoll spezifischen Frames eingeschlossen.
- Am Switch werden die medienspezifischen Frames entfernt. Durch die Einwahl wird er veranlasst, eine PPTP- Tunnelsitzung über das Internet zu dem PPTP fähigen NT- RAS-Server zu öffnen, der im Profil des Benutzers festgelegt ist. Der Remote- Access- Switch kapselt das PPP- Payload – Paket in einen GREv2- Header und dann in einen IP- Header.
- Der RAS- Server behandelt die eingehende PPTP- Verbindung nicht anders als einen Anruf, der per Modem eingeht. Der Delivery- Header, der IP- Header und der GREv2-Header werden aus dem Payload- Paket entfernt.
- Bevor die Pakete vom Client das LAN erreichen, werden die PPP- Frames von den eingeschlossenen IP-, NETBEUI –oder IPX- Datagrammen entfernt.[75]

[75] Charlie Scott, Paul Wolfe, Mike Erwin, Virtuelle Private Netzwerke, S 71

4.2 Sicherheit

Wie die meisten Sicherheitssysteme besteht auch PPTP aus zwei Komponenten, nämlich der Authentifizierung zur Verhinderung unerwünschter Verbindung und der Verschlüsselung von Daten, die über eine hergestellte Verbindung gesendet werden.[76]

Microsoft hat eine spezielle Verschlüsselung, die Microsoft Point- to- Point Encryption (MPPE), entwickelt, wodurch die Vertraulichkeit einer PPP- Verbindung abgesichert wird. Auch einige Sicherheitsfunktionen wie Datenverschlüsselung (MPPE, Microsoft Point-to-Point Encryption) und Benutzer- Authentifizierung, die allerdings bei weitem nicht die stärke von IPSec aufweisen, werden durch PPTP dargestellt. Einige erfolgreicher Angriffe haben insbesondere Abteilung der verschlüsselten Daten, aus der Benutzer Authentifizierung blockiert.

MPPE arbeitet ideal mit MS-CHAP zusammen und stützt sich auf MD4 Hash- Algorithmus. Zur Authentifizierung benutzt PPTP die bestehenden Authentifizierungsprotokolle Protocol Authentication Protocol (PAP), Challenge Handshake Authentication Protokoll (CHA), MS-CHAP v1 oder MS-CHAP v2. Allerdings wurde MS-CHAP v2 für erhebliche Sicherheitslücken in MS-CHAP v1 erweitert. Bruce Schneider und Peter Mudge deckten schon 1999 diverse Schwachstellen insbesondere in MS-CHAPv1 auf und ein 2001 erfolgter Laborangriff zeigte sogar, dass sich PPTP- Passwörter mit maximal acht Zeichen wenigen Tagen knacken lassen.
PPTP arbeitet mit der RAS- Authentifizierung von Windows NT. Die verschiedenen Authentifizierungsverfahren, die der RAS- Server akzeptiert, stehen in den RAS- Eigenschaften bei den Verschlüsselungseinstellungen zur Auswahl. Die Authentifizierung wird festgelegt können, die der RAS- Server beim Login des Client durchführt.[77]

---

[76] Charlie Scott, Paul Wolfe, Mike Erwin, Virtuelle Private Netzwerke, S 73

[77] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005, S 215

4.3 Verschlüsselung

Die Verschlüsselung stellt sicher, dass jeglicher Verkehr der durch ein VPN über ein öffentliches Netzwerk, wie Z.B das Internet, übertragen wird gesichert ist. Die Pakete werden im PPP Protokoll verschlüsselt und dann an das PPTP übergeben.

Der PPP Standard sieht die Möglichkeit vor, mit dem Microsoft Point to Point Encryption Protokoll (MPPE) zu verschlüsseln. Mit dem Windows Server 2003 Durchführung von PPTP, sowohl 40 Bit Verschlüsselung als auch 128 Bit Verschlüsselung wird unterstützt. Dabei wird von jeder Seite ein Session- Key generiert, der entweder 40, 56 oder 128 Bit lang sein kann. Lange Zeit war aufgrund von Exportrestriktionen außerhalb der USA nur ein 40 Bit Schlüssel zulässig. Diese Schlüssellänge kann heute nicht mehr als sicher angesehen werden. Es ist dringend zu empfehlen, einen 128 Bit Schlüssel zu verwenden. [78]

Der Schlüssel wird unter Benutzung des Passwortes des Partners erzeugt. Auf jeden Fall sollten mehr als 8 Zeichen enthalten, um die beliebige Gefahr nicht zu entstehen. Auf diese Weise kann der Schlüssel nicht geknackt werden.

Der Verschlüsselung von PPTP bietet nicht nur neben der Verschlüsselung mit MPPE sondern auch bintec Router die Möglichkeit höheren Verschlüsselung mit den Verfahren DES, Tripple DES sowie Blowfish. Diese Verschlüsselungsart funktioniert nur, wenn das bintec Gerät mit entsprechender Lizenz geeignet ist.

Die verschlüsselte Authentifizierung in RAS entspricht dem Internet Authentifizierungsstandard CHAP (Challenge Handshake Authentication Protocol). CHAP wird erweitert, in der zwischen Client und Server keine Passwörter im Klartext übertragen werden. CHAP- Authentifizierung verlaufen wie folgt:

- Der Server fordert den Client für Verbindung an, sich zu identifizieren.

[78] http://www.funkwerk-ec.com/prod_bintec_vpn_pptp_encryption_de.html

- Der Client schickt das Geheimnis durch den Hash- Algorithmus MD5 von RSA. Ein Hashwert wird zufällig erzeugt.
- Der Server vergleicht den übermittelten und selbst berechneten Hashwert. Wenn die beiden Werte übereinstimmen, ist die Verbindung erfolgreich authentifiziert.

In den RAS – Eigenschaften von Windows NT gibt es ein Kontrollkästchen mit dem Sie die Datenverschlüsselung für die RAS- Verbindung aktivieren können. Mit dieser Option werden alle Daten, die der Verbindung durchlaufen, in unleserliche Form gebracht. Das Kästchen kann nur in Kombination mit der verschlüsselten Authentifizierung von Microsoft mit MS- CHAP aktiviert werden.[79]

[79] Charlie Scott, Paul Wolfe, Mike Erwin, Virtuelle Private Netzwerke, S 74

5. Layer-2 Tunneling Protocol (L2TP)

5.1 Funktionsweise im Überblick

Das L2TP – Protokoll ist das prominenteste Protokoll der Layer-2- Technologie. Es gibt etliche Hersteller, die Produkte auf der Basis von L2TP anbieten, und es ist als Industriestandard anerkannt nicht zuletzt, weil Cisco maßgeblich zur Entwicklung beigetragen hat. Voraussichtlich wird die Verbreitung von L2TP weiter zunehmen, da es Bestandteil von Windows 2000 und auch Windows XP geworden ist und somit in der Bürokommunikation weitflächig eingesetzt werden kann.[80]
L2TP ging als Synthese eine Mischform seiner beiden Vorbilder bzw. Konkurrenzprodukte L2F und PPTP hervor. Die Leistungsfähigkeit des L2F- Protokolls mit dem Vorteilen des PPTP-Protokolls wird verknüpft. Das Grundprinzip von L2TP wird eine Verbindung zwischen L2TP-Client und einem L2TP- Server, die über einen Tunnel miteinander verbunden sind, bezeichnet und verkapselte PPP- Pakete übertragen.

Für das Verständnis des L2TP ist hilfreich, einige wesentliche Elemente des Point- to- Point-Protocol zu verstehen. Durch folgende Eigenschaften wird PPP charakterisiert.

- Es verfügt über eine Methode zur Verkapselung von Datagrammen (HDLC- basierend)
- Zum Aufbau von Data- Links, ihrer Konfigurierbarkeit und ihrer Überprüfung wird das Link Control Protokoll (LCP) eingesetzt.
- Eine Familie von Netzwerk- Steuer- Protokollen (NCP) ermöglicht die Steuerung und Konfigurationen verschiedene Netzprotokolle, die parallel betrieben werden können.[81]

Ein Endgerät wird ins firmeneigene Intranet über einen Remote- Access- Zugang gewählt. Die Telefonverbindung wird nicht für Zugang zum Unternehmen erfolgt, sondern über die Ortsvermittlung zum Zugangspunkt (PoP) eines Internet Service Providers (ISP). Zum

---

[80] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005, S 217

[81] Gerhard Lienemann, Virtuelle Private Netzwerke Aufbau und Nutzen 2002, S 120

Sicherheitsgateway der Firma wird eine Verbindung vom PoP mittels Point- to- Point- Protokoll (PPP) aufgebaut. Um eine Kontrollverbindung zu erreichen, muss der Aufbau von einer PPP-Verbindung erfolgt werden. Auf diese Weise verhält sich ein L2TP- Tunnel wie eine In- Band-Lösung. Daten wie Management und Wartungsinformation gehen über dieselbe Verbindung.

Über einen L2TP- Tunnel können mehrere unabhängig logische PPP- Verbindung von den anderen PPP- Verbindungen kommuniziert werden. Dabei sind alle Protokolle nutzbar, die von PPP unterstützt werden.

Ein L2TP- Tunnel kann entweder auf Anforderung von einem Endgerät oder als Mandanten-Tunnel initiiert werden. Weiterhin ist der L2TP- Tunnel für den Nutzer des Endgerätes transparent und erfordert keine zusätzlichen Installationen außer der ISDN / PSTN-Einwahlmöglichkeit zum PoP. Mehrere Tunnel können zwischen Eingangskonzentrator (LAC) und Ausstiegspunkt (LNS) mit ihrer eigenen Kontrollverbindung aufgebaut werden.[82]

Das Layer- 2- Tunneling Protocol kann zwei Tunnelmodelle unterschieden werden, dem Provider- Enterprise- Modell (Compulsory Tunneling) und dem Ende- zu- Ende – Modell (Voluntory Tunneling). Die beiden Modelle unterscheiden sich durch den Punkt, an dem der L2TP- Tunnel initiiert wird. Der Remote- Access- Client wählt sich in den Einwahlkonzentrator eines Service Provider ein. Das „Compulsory Tunneling“ zwingt den sich wählenden Client dazu, den am LAC des Providers bereitgestellten Tunnel für seine Kommunikation zu benutzen. Der Client selbst hat keinen Einfluss auf den Tunneln.

Voluntary Tunneling, das der freiwillige Tunnel ist, kann mit L2TP realisiert werden. In dieser Variante ist der Remote- Access- Concentrator (RAC) der Service Providers in keiner Weise in den Tunneln involviert.

---

[82] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005, S 218

5.1.1 Analyse Paketformat von L2TP

Zwei Paketformattypen werden nach L2TP- RFC 2661 unterschieden. Das Datenpaket wird über den Transport der PPP- Pakete übernimmt. In Steuerungspaketen werden so Attribute Value Pair (AVP) genannt. AVPs enthalten die Befehle und Optionen, die zwischen LAC und LNS ausgetauscht werden. Diese Datenstrukturen, die aus einem festen Header bestehen, werden über einen Header- Erweiterung transportiert.

Für die Kommunikation zwischen LAC und LNS werden Steuerinformationen benötigt, die die Charakteristik eines L2TP- Tunnels bestimmen. Die Proxy- Authentifizierung ist eine praktische Anwendung für versteckte, beziehungsweise verschlüsselte AVPs. Vom LAC werden die User-ID und das Passwort des PAP- Protokolls zum LNS geschickt. Beim Transport werden die Informationen über ein öffentliches Netz verschlüsselt, weil diese Informationen im Klartext vorliegen.

5.2 Sicherheit

L2TP hat über keinen ausreichenden Sicherheitsmechanismen und muss daher die Sicherheit über Zusatzfunktionen und –Protokolle ausrichtet werden. In L2TP werden nur minimale Sicherheitsmechanismen eingebaut. Hauptsächlich beschränkt es sich auf den Bereich der Control Connection und Tunnelauthentifizierung. Abgesehen von einer Basissicherheit, die über ein „Shared Secret“ die beiden Tunnel- Endpunkte (LAC und LNS) absichert, existieren keine nennenswerten Sicherheitsfunktionen. Diese Sicherheitslücke kann daher durch den Einsatz von Sicherheitsprotokollen, gelöst werden.

L2TP bietet wie IPSec Protokolle keinen Schutz der Datenvertraulichkeit und der Datenintegrität, und es enthalt keine Paketauthentifizierung.

Falls hierfür Bedarf vorhanden ist, dann wird vom L2TP – Standardisierung- Gremium empfohlen, die Sicherheitsdienste der darunter liegenden Transportprotokolle zu benutzen, also

im Falle von L2TP/UDP beispielsweise IPSec im Transport- Modus einsetzen. Auf diese Weise wird die Verbindung zwischen LNS- und LAC vollständig also Steuerung und Datenkanäle geschützt.[83]
Eine Kombination von L2TP und IPSec stellt allerdings aufgrund der erhöhten Rechenleistung für die Sicherheitsfunktionen besondere Anforderungen an die einzusetzende Hardware. Hier spielt insbesondere die Prozessorleistung eine herausragende Rolle, so dass ihre Verwendung in normal dimensionierten PCs oder Routern nicht zu empfehlen ist.[84]

Wie den Ausführungen, zum L2TP- Protokoll zu entnehmen ist, sind keine Mechanismen vorgesehen, die die Vertraulichkeit der übertragenden Daten sichert. Nur beim Aufbau der Kontrollverbindung Start- Control- Connection- Request (SCCRP) und der darauf folgenden Start- Control- Connection- Reply (SCCRP) der Gegenseite ist es möglich, nach dem Challenge- Response- Verfahren mit dem CHAP Protokoll eine beiderseitige Authentifizierung vorzunehmen.

Das L2TP- Protokoll isst zwar eine kostengünstige Lösung für den Fernzugriff auf ein Unternehmensnetz, doch müssen hinsichtlich der Vertraulichkeit etliche Bedenken angemeldet werden, wenn keine zusätzlichen Sicherungsmaßnahmen getroffen werden. Ein L2TP- Tunnel agiert, indem ein L2TP- Frame in einem UDP- Paket gekapselt transportiert wird. Dabei definieren die Quell- und Ziel- IP Adressen den Beginn und das Ende des Tunnels. Um die Vertraulichkeit zu gewährleisten, kann bei der Datenübertragung ergänzend IPSec eingesetzt werden.[85]

---

[83] Manfred Lipp VPN- Virtuelle Private Netzwerke Aufbau und Sicherheit, S 304

[84] Gerhard Lienemann, Virtuelle Private Netzwerke Aufbau und Nutzen 2002, S 122

[85] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005, S 223

5.3 Verschlüsselung

Spezifisierte Verschlüsselung in L2TP ist vom Sicherheitsstandpunkt aus gesehen nicht gerade reichlich. Der Algorithmus enthält eine schlichte Exlusiv- Oder- Verknüpfung des Klartext mit einem 128- Bit großen Schlüsseln, um zu ver- und entschlüsseln.

L2TP selbst bietet eine zugegebenermaßen recht simple Authentifizierung von LNS und LAC beim Aufbau eines Tunnels. Diese Authentifizierung basiert auf einem dreiphasigen Handshake-Verfahren, ähnlich wie CHAP, das die Existenz eines Shared Secret auf den beteiligten Gegenstellen voraussetzt. Dieses Shared Secret ist auch gleichzeitig der Schwachpunkt des Verfahrens, denn es wird in den meisten Implementierungen eine Kombination aus Buchstaben, Ziffern und Sonderzeichen im Klartext gespeichert.[86]

Die Verschlüsselung beschäftigt in einem Output- Feedback- Modus mit einem expliziten Initialisierungsvektor. Ein 128 Bit großer Wert wird aus dem Shared Secret, dem Attributwert und dem Initialisierungsvektor über MD5 erzeugt. Die ersten 16 Bytes sind verschlüsselt, denn es wird mit den ersten 16 Bytes des originalen AVP- Subformats Exlusiv- Oder verknüpft. Wieder ein 128- Bit Wert wird aus diesem Wert und aus Shared Secret über MD5 erzeugt, mit dem die nächsten 16 Bytes verschlüsselt werden. Wenn der originale Wert vollständig verschlüsselt ist, wird dies nicht weitergeführt.

Aus Sicherheitsgründen wird die Länge des originalen Wertes im Value- Feld verschleiert, in dem man als weitere Sicherheitsmaßnahme Hidden- AVP- Subformat erzeugt, das aus einem Längenfeld, dem beschriebenen Verfahren verschlüsselt und als Wert in das Value- Feld des AVP eingetragen.

---

[86] Manfred Lipp VPN- Virtuelle Private Netzwerke Aufbau und Sicherheit, S 300

Die Verwendung von Hidden- AVPs innerhalb der Steuerungsverbindung wird möglich bei der Vorstellung des H-Bit erläutert. Wenn diese Verschlüsselung zu Algorithmen mit DES oder IDEA vergleichet wird, ist leider diese eher rudimentäre Verschlüsselung.

Man muss sich lediglich das Shared Secret beschaffen und kann damit den benutzen 128- Bit-Schlüssel berechnen, oder man startet eine Kryptoanalyse auf das Ergebnis der Exklusiv- Oder Verknüpfung, die in L2TP als Ver- und Entschlüsselungsalgorithmus verwendet wird.[87]

[87] Manfred Lipp VPN- Virtuelle Private Netzwerke Aufbau und Sicherheit, S 297

Eigenschaften	PPTP	L2F	L2TP
Standard/ Status	RFC 2637(informell)	RFC 2341(informell)	RFC2661(Standard)
Medium	IP/GRE	IP/UDP,FR,ATM	IP/UDP,FR,ATM
Private Adresszuweiseung	ja	ja	ja
Multiprotokoll Unterstützung	ja	ja	ja
Kanäle	Eingang und Ausgang	Eingang	Eingang und Ausgang
Protokoll	Kontrolle über TCP Port 1723	Kontrolle über UDP Port 1701	Kontrolle über UDP Port 1701
Verschlüsselung	Microsoft PPP(Encryption MPPE)	PPP Encryption (MPPE); IPSec optional	PPP Encryption (MPPE/ECP); IPSec optional
Authentifiezierung	PPP-Authentifizierung	PPP-Authentifizierung	PPP-Authentifizierung
Tunnelmodus	typischerweise voluntary Tunnel	compulsory Tunnel-modus	voluntary&compulsory Tunnel-modus
Mehrere Kanäle pro Tunnel	nein	ja	ja
PPP multilinkUnterstützung	nein	ja	ja

Tab. 1 : Vergleich der Layer- 2 Techniken

6. IP – Security (IPSec)

6.1 Funktionsweise im Überblick

Zu des beginn des Internets fand eine Kommunikation in offenen Systemen ohne jegliche Absicherung statt. Dies wurde zunächst nicht als nachteilig empfunden, da am Datenaustausch über das Internet nur ein kleiner wissenschaftlich geprägter Personenkreis teilnahm. Mit zunehmender Kommerzialisierung des Internets änderten sich die Sicherheitsanforderungen grundlegend.[88]
Ein grundsätzliches Problem des Internet Protokoll besteht darin begründet, dass es heutigen Sicherheitsanforderungen längst nicht mehr genügt. Dazu ist wichtiges Thema für VPN-Administratoren das IPSec Projekt der IETF, das die Anforderungen für ein sicheres IP-Protokoll erarbeitet. Dieses zu den ältesten Standards gehörende Protokoll der dritten Kommunikationsschicht zeigt einige gravierende Sicherheitsdefizite auf, deshalb für den Einsatz innerhalb VPN über öffentliche Netze nicht geeignet ist.

IPSec stellt, bezogen auf, das OSI- Referenzmodell, den Sicherheitsstandard auf Layer-3 dar. IPSec ist standardisiert gemäß IETF, mit dem herstellerübergreifend ein sicherer und geschützter Datenaustausch durch das IP ermöglicht werden kann.[89]
Das Hauptentwicklungsziel von IPSec besteht darin, der IP- Paketaustausch in Kommunikationsnetzen abzusichern. IPSec bietet kryptographische Sicherungsverfahren für Authentifizierung, Datenintegrität, Zugangskontrolle und Vertraulichkeit.[90] Dabei ist die Bereitstellung von Sicherheitsfunktionen auf IP Ebene sowohl für IPv4 als auch für IPv6. Es ist im Prinzip für jede Art von IP- Kommunikation nutzbar und so gestaltet, dass die resultierenden

[88] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005, S 229

[89] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005, S 227

[90] Charlie Scott, Paul Wolfe, Mike Erwin, Virtuelle Private Netzwerke, S 202

Datenströme auch über Netzkomponenten transportiert werden können, die IPSec nicht unterstützen.[91]

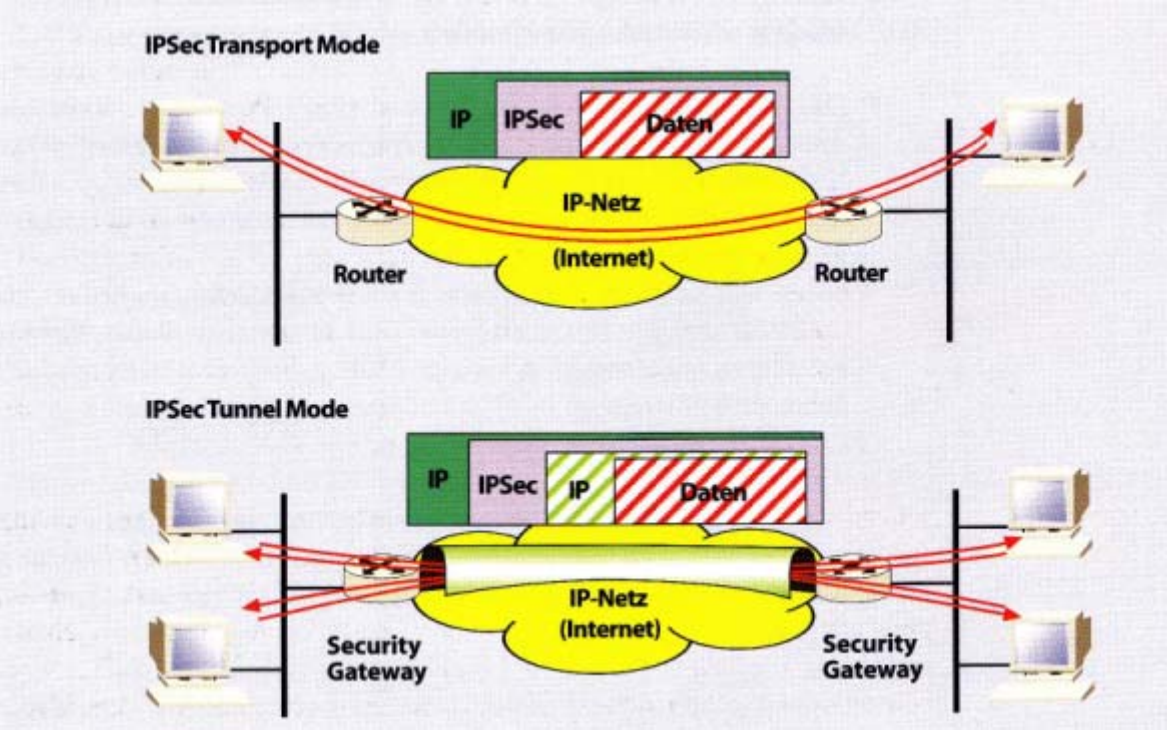

Abb. 6 : IPSec- Funktionsmodelle

Quelle: Jörg Buckbesch, Rolf- Dieter Köhler, VPN Virtuelle Private Netze, Sichere Unternehmenskommunikation in IP- Netzen, S 58

IPSec erreicht dieses Ziele mithilfe zweier Protokolle der Verkehrssicherheit: Die IPSec zugrunde liegende Architektur zeigt einen modularen Charakter auf, so dass die drei Hauptbestandteile von IPSec. Das AH- Protokoll (Authentication Header), das ESP – Protokoll (Encapsulating Security Payload) und das Schlüsselmanagement (Key- Management) nahe zu beliebig zusammen eingesetzt werden können.

.

[91] Jörg Buckbesch, Rolf- Dieter Köhler, VPN Virtuelle Private Netze, Sichere Unternehmenskommunikation in IP-Netzen, S 55

Der RFC 2401 beschreibt die Architekturelemente von IPSec sehr ausführlich. Die wichtigsten Komponenten umfassen.

- ESP und AH
- Verschlüsselungsalgorithmen
- Authentifizierungsalgorithmen
- IPSec Domain of Interpretation (DOI)
- Schlüsselverwaltung
- Policy[92]

IPSec wird nun dahingehend erweitert, dass der IP- Protokollheader um Elemente zur Verschlüsselung und Authentifizierung ergänzt wird. Dabei wird jeweils zwischen dem Transport- und Tunnelmodus innerhalb der beiden Protokollvarianten ESP- AH unterschieden.
IPSec – Datenpakete lassen sich unter Verwendung des Transport- oder Tunnelmodus übertragen. Der Transportmodus umfasst ein Ende zu- Ende- Kommunikation, bei der lediglich die Verschlüsselung des Datenteils eines IP- Paketes vorgenommen wird. Der IP- Header, Quell und Ziel- IP- Adresse, bleiben unverändert.[93]

6.2 Sicherheit

Das Konzept des Sicherheitsassoziation (SA) bildet die Basis von IPSec. In einer SA werden die Kommunikationsrahmenbedingungen, wie beispielweise das Verhalten dieses Sicherheitsprotokolle und von IPSec verwendete Protokolle (AH / ESP), Verschlüsselungsalgorithmen, ihre Lebensdauer, weitere Charakteristika bestimmt.

---

[92] Gerhard Lienemann, Virtuelle Private Netzwerke Aufbau und Nutzen 2002, S 82

[93] Gerhard Lienemann, Virtuelle Private Netzwerke Aufbau und Nutzen 2002, S 83

Der dritte zentrale Bestandteil von IP-Sec, die Security Association (SA) dargestellt, bevor zwei der drei Hauptkomponenten – das AH- Protokoll und das ESP- Protokoll - näher erklärt werden. Diese hilft das Verständnis beim Aufbau einer IPSec- Verbindung. Wenn die zwei Kommunikationspartner mit IPSec abgesicherte Daten austauschen wollen, müssen zuerst Sicherheitsvereinbarungen ausgehandelt werden.

Die Haupt Aufgabe von eine SA ist eine Vereinbarung zwischen Kommunikationspartnern hinsichtlich des IPSec- Protokolls, Betriebsmodus (Tunnel oder Transport) kryptographischer Algorithmen, Lebensdauer der Schlüssel. Sie sind gewissermaßen als Vertragswerk zu verstehen, in dem sämtliche für die gesicherte Kommunikation erforderlichen Parameter enthalten sind und zur Anwendung kommen können.

Für die Übertragung von Daten sind die verschiedenen SAs und unterschiedliche Sicherheitsstufe notwendig, ebenso für die unterschiedliche Protokolle.
In jeden Fall wird Übertragungsrichtung sowohl für die Authentifizierung als auch für die Verschlüsselung separate SAs bestimmen müssen und diese müssen aktiv sein, bevor die Anwendungsdaten übertragen werden können.
SA sind unidirektionale (simplex) Verbindung, die zum Datentransport vom Sender zum Empfänger ausgerichtet sind. Für den Rücktransport der Daten muss eine weitere SA ausgehandelt werden.[94]

Die einzelnen SAs werden in einer lokalen Datenbank (Security Association Database) gespeichert und eindeutig über den SPI (Security Parameter Index), einer IP- Zieladresse und dem Sicherheitsprotokoll (ESP/ AH) identifiziert.

Eine SA ist dabei stets durch mindestens drei Komponenten eindeutig beschreiben.

1. Der Security Parameters Index (SPI) ist eine einfache Nummer, die den Kommunikationspartner auf den entsprechenden Eintrag in seiner Sicherheitsdatenbank verweist, für einen Außenstehenden jedoch bedeutungslos ist.

[94] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005, S 233

2. Die IP- Adresse gibt an, welchem Kommunikationspartner die SA zugeordnet ist.
3. Mit der Transformation wird festgelegt, welches Sicherheitsprotokoll auf die Daten anzuwenden ist.[95]

Eine Security Association beinhaltet alle wichtigen Elemente zum Aufbau einer gesicherten Kommunikationsverbindung. Eine SA für eine gesicherte IPSec- Kommunikation ist für folgende Regelungen verantwortlich:

- Arbeitsmodus des Authentifizierungsalgorithmus, der im AH- Protokoll festgelegt ist; hierzu werden außerdem die Schlüssel definiert.
- Arbeitsmodus des Verschlüsselungsalgorithmus für das ESP- Protokoll, wie CBC weiterhin werden die dazugehörigen Schlüssel definiert.
- Spezifizierung der zeitlichen Gültigkeit aller Schlüssel.
- Spezifizierung der zeitlichen Gültigkeit der SA.[96]

[95] Jörg Buckbesch, Rolf- Dieter Köhler, VPN Virtuelle Private Netze, Sichere Unternehmenskommunikation in IP-Netzen, S 61

[96] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005, S 233

	IPSec	L2TP	PPTP	L2F
Protokolltyp	Layer 3	Layer 2	Layer 2	Layer 2
Standardisiert (RFC)	Ja	Ja	Nein	Nein
Paket- Authentifizierung	Ja	Nein	Nein	Nein
Benutzer- Authentifizierung	Ja	Ja	Ja	Ja
Datenverschlüsselung	Ja	Nein	Ja	Nein
Schlüsselmanagement	Ja	Nein	Nein	Nein
QoS- Signalisierung	Ja	Nein	Nein	Nein
IP- Tunneling	Ja	Ja	Ja	Ja

Tab. 2 : Ein Vergleich verbreiteter Tunneling- Protokolle

Quelle: Mafred Lipp, VPN Virtuelle Private Netzwerk Aufbau und Sicherheit, S 184

6.2 Authentifizierung (AH)

Das Authentication- Header- Protokoll ist Fundament für die Sicherung der Datenintegrität und Authentifizierung der Datenpakete. Authentication Hader ist ein IPSec – Protokoll, das außer der Datenvertraulichkeit alle in IPSec geforderten Schutzmechanismen bietet.[97]

Die Hauptaufgabe des AH besteht mit der IPSec – Authentifizierung, dass das übertragene Paket genau so beim Empfänger ankommt, wie es so vom Sender abgeschickt wurde, ohne Änderungen und ohne ungewollte Wiederholungen. Es bietet Schutz vor wiederholter Sendung, in dem für die

[97] Manfred Lipp VPN- Virtuelle Private Netzwerke Aufbau und Sicherheit, S 206

Datenpakete fortlaufende Sequenznummern generiert werden. Die Datenpakete werden vom Empfänger ausgewertet und so das gesamte IP- Datenpaket wird gesichert. Somit kann auch keinerlei Verwendung von Network Address Translation (NAT) auf Pakete, die mit dem Authentication Header gesichert werden.
AH bietet einen optionalen Replay – Schutz anhand einer fortlaufenden Prüfung der im Header enthaltenen Paketfolgenummer.

Die Unverfälschtheit der Daten (bei ESP) bzw. des gesamten IP- Pakets (bei AH) wird durch kryptografische Hash Funktionen gewährleistet. Dabei handelt sich um mathematische Methoden, die aus einem beliebig langen Klartext ein Komprimat vorgegebener Länge ähnlich einer Prüfziffer erzeugen. Das Komprimat wird Hash- Wert genannt. Es ist so etwas wie ein Fingerabdruck des Klartextes und sollte im Interesse der Eindeutigkeit nicht kleiner als 128 Bit sein.
Die Hash Funktion bezeichnet sich durch die mehrere Eigenschaften aus:

1. Sie bildet den Klartext so auf den Hash- Wert ab, dass auch die kleinste Veränderung des ursprünglichen Textes zu einem gänzlich anderen Hash- Wert.
2. Mit Hilfe der mathematischen Funktion ist leicht zu berechnen.
3. Die Hash- Funktion ist kollisionfrei. Das Heißt, dass mit vernachlässigbarer Unsicherheit ein bestimmter Hash- Wert das Ergebnis eines Klartextes ist.[98]

6.2.1 Die Verarbeitung ausgehender Pakete

Im Transportmodus wird der AH- Header direkt nach dem IP- Header in das IP- Paket eingefügt. Im Next- Header- Felder wird die Nummer des Protokolls eingetragen, das im Nutzdatenbereich eingekapselt ist.
Im Tunnelmodus bekommt das Feld Next Header den Wert 4, und der AH wird zwischen dem inneren und äußeren IP- Header eingefügt. Die restlichen Felder werden wie im Transportmodus

[98] Jörg Buckbesch, Rolf- Dieter Köhler, VPN Virtuelle Private Netze, Sichere Unternehmenskommunikation in IP-Netzen, S 63

bearbeitet. Das Paket wird mit dem in der Sicherheitsassoziation spezifisierten Authenticator authentifiziert, und der Wert wird in das Authentication- Data- Feld eingetragen.
Als letztes wird die Paketprüfsumme berechnet und in den IP- Header eingetragen. Nun kann das Paket verschickt werden.[99]

6.2.2 Die Verarbeitung eingehender Pakete

Die Verarbeitung eingehender AH- Pakete erarbeitet in umgekehrter Reichenfolge. Wenn die aufgrund von SPI und IP-Quelle und Ziel Adresse in der Security Association Database (SAD) in entsprechendem Eintrag mit den notwendigen Optionen und Parametern gefunden werden muss, kann die Verarbeitung erfolgen.

6.3 Verschlüsselung (ESP)

Nach dem AH für IPSec wichtige Protokolle ist das Encapsulating Security Payload- Protokoll (ESP). Es wurde von der IETF im [RFC 2406] entwickelt. Wie im Falle des Authentication Header wurde das Protokoll der Encapsulating Security Payload dazu entwickelt, die Sicherheit des Internet Protokolls (IP) zu verbessern.

ESP wird für die Authentifizierung die gleichen Verfahren wie bei AH verwendet. Das Encapsulating – Security – Payload- Protokoll stellt alle Sicherheitsfunktionen dar, die auch Ah bietet, plus einen zusätzlichen Schutz der Datenvertraulichkeit.

Zweck der Verschlüsselung ist die Gewährlistung der Vertraulichkeit der Daten, d.h. Die Daten werden gegen das Mitlesen durch Unbefugte während der Übertragung verschlossen. ESP bietet den Schutz der Vertraulichkeit, Authentifizierung der Datenquelle, Schutz verbindungsloser Integrität. Anti- Replay und begrenzte Vertraulichkeit des Datenflusses.[100]

---

[99] Manfred Lipp VPN- Virtuelle Private Netzwerke Aufbau und Sicherheit, S 208

[100] Carlton R. Davis, IPSec Tunneling im Internet, 2002, S 212

Eine Anwendung von ESP garantiert die Vertraulichkeit der zu übertragenden Nutzlast, die mit einem reversiblen kryptographischen Verfahren behandelt wird. Im Gegensatz zum AH- Header ist ein ESP- Header in der Lage, sowohl eine Verschlüsselung als auch eine Authentifizierung durchzuführen.[101]
Wenn ESP optional auch zur Authentifizierung verwendet wird, so erfolgt die Verschlüsselung als erstes. Die Authentifizierung wird von dem Empfänger zuerst kontrolliert und dann entschlüsselt. Auf diese Weise können nicht authentisierte Pakete verworfen werden, ohne CPU-Leistung zur Entschlüsselung zu verschwenden.

Nach der Definition des Standards besteht auch die Möglichkeit, ESP nur für die Authentifizierung zu verwenden, in dem als Verschlüsselungsverfahren NULL angegeben wir. Außerdem bietet auch ESP durch die Prüfung der Paketfolgenummer einen optionalen Replay-Schutz.[102]

Das ESP sendet zusätzlich zu den Authentication Header Protokoll zur Verfügung gestellten Mechanismen den Schutz der Datenvertraulichkeit. Ein Teil der IP- Pakets wird verschlüsselt und ein Header sowie ein Trailer in das Datagramm eingefügt, um dies zu erreichen. Die Datenintegritätsprüfung und Authentifizierung umfasst im Gegensatz zum Authentication Header nicht über das vollständige Paket, sondern der IP- Header wird von der Berechnung ausgenommen. ESP nimmt ebenfalls ein IP- Protokoll auf die Nummer 50.

Die Vertraulichkeit wird durch den Einsatz kryptographischer Algorithmen zu Verschlüsselung wichtiger Teile der IP- Datagramms gewährleistet. Die von ESP zu Verschlüsselung von Datagrammen eingesetzten Algorithmen sind ausschließlich symmetrische Verfahren. ESP bietet Authentifizierung mithilfe von Message Authentication Codes (MACs). MACs ähneln

---

[101] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005, S 237

[102] Jörg Buckbesch, Rolf- Dieter Köhler, VPN Virtuelle Private Netze, Sichere Unternehmenskommunikation in IP-Netzen, S 67

kryptographischen Hash- Funktionen, mit dem Unterschied, dass bei MACs ein Schlüssel zur Berechnung des Hashwerts benötigt wird. [103]

Im Transport Mode umfasst die Verschlüsselung über den TCP- Header und den Datenteil, aber vor jeglichem Transport- Protokoll eingefügt und auch vor jedes bereits angewendete IPSec-Protokoll. Im Tunnel Mode wird ESP der originäre IP- Header ebenfalls verschlüsselt und um einen neuen IP- Header eingefügt.
Derzeit sind folgende Verschlüsselungsverfahren vorgesehen:

- zwingend

TripleDES- CBC [RFC 2451] oder
NULL[RFC 2410]

- optional

CAST -128 [RFC 2451]
RC5 [RFC 2451]
AES- CBC mit 128- Bit Schlüsseln [RFC 3602]
IDEA[RFC 2451]
Blowfish [RFC 2451] [104]

[103] Carlton R. Davis, IPSec Tunneling im Internet, 2002, S 211

[104] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005, S 237

6.4 Schlüsselaustauch (IKE)

Während IPSec das Problem des sicheren Schlüsselaustausches grundsätzlich vernachlässigt bzw. diesen manuell erstellt, kann der Prozess Schlüsselaustausches dynamisch durchzuführen. Die manuelle Schlüsselverteilung ist der Übertragung oder der Schlüssel auf Papier oder Datenträger und die manuelle Hinterlegung auf den Sicherheitssystemen. Diese Verfahren bringen sich alle einen Nachteil mit: Auf diese Weise wird die Komplexität meist erhöht und damit das auch in das Unsichere gesamte System meist, die Fehleranfälligkeit.

Das Diffie- Hellman- Verfahren ist ein auf Methoden der Public- Key- Kryptographie beruhender Algorithmus zum sicheren Erzeugen von Schlüsseln durch die Übertragung bestimmter Informationen über ein unsicheres Medium. Auf Basis dieses Verfahrens wurde eine Reihe von Schlüsseltauschprotokollen entwickelt, die zum Teil auch die Grundlage des Internet- Key- Exchange Protokolls (IKE) bilden, das zum Erzeugen einer IPSec- Sicherheitsassoziation eingesetzt wird.[105]

Ein Schlüsselmanagement (IKE- Management) als Teil von IPSec anfordert die Erstellung und Verteilung von geheimen Schlüsseln. Die IPSec Architektur beschreibt zwei grundsätzlich Verfahren:

1. Manueller Austausch: Die Schlüssel des Kommunizierenden Systems und jedes der eigenen Systeme mit den dazugehörigen Schlüsseln werden von einem Systemadministrator manuell vorgenommen.
2. Automatischer Austausch: Ein System erzeugt und verteilt auf Anforderung eine Security Association (SA), die Konfiguration und geeignete Schlüssel an das dazugehörige Management.

IPSec unterstützt sowohl manuellen als auch automatischen Schlüsselaustausch. In kleinen Netzen wird manuelle Konfiguration der Geräte im Allgemeinen verwendet. In größeren

[105] Manfred Lipp VPN- Virtuelle Private Netzwerke Aufbau und Sicherheit, S 221

Netzwerken jedoch insbesondere die Forderung noch ständiger Schlüsselaustausch zu unvertretbar hohem administrativen Aufwand.

Mit IKE ist ein Verfahren entwickelt worden, das den genannten Anforderungen nachkommt. Grundsätzlich ist IKE durch die folgenden sieben Eigenschaften geprägt.

1. Es bestimmt für die beteiligten Kommunikationsteilnehmer, welche Protokolle, Algorithmen und Schlüssel zu verwenden sind.
2. Es wird sichergestellt, dass von Beginn an mit der richtigen Person bzw. Applikation ein Schlüssel zu verwenden ist.
3. Es wird ein sicheres Schlüsselmanagement für die ausgehandelten Schlüssel gewährleistet.
4. Es wird ein sicherer Schlüsselaustausch zugesichert.
5. Es ist über den UDP- Port 500 nutzbar.
6. Es bietet ein Zwei- Phasen- Konzept
7. Es lässt vier unterschiedliche Authentifizierungsverfahren zu.[106]

Im Zusammenhang mit IKE geht es allerdings nicht um die Verwaltung von Informationen lokaler SAs, sondern die relevanten zur Verschlüsselung erforderlichen Daten müssen über Kommunikationsverbindungen übertragen werden und sind somit als höchst sicherheitskritisch einzustufen. Die folgenden Mechanismen bzw. Protokolle sorgen für einen sicheren Austausch von Schlüsseln.

- Internet Security and Key Management Protokocol (ISAKMP)
- ISAKMP Domain of Interpretation (DoI)
- OAKLEY Key Determination Protocol [107]

Das Internet Security and Key Management Protocol (ISAKMP) wird von RFC 2408 spezifiziert und definiert die Prozeduren für die Verwaltung von SAs (Aufbau, Änderung, Löschung). Die

---

[106] Wolfgang Böhmer VPN Virtual Private Networks Kommunikationssicherheit in VPN- und IP- Netzen, über GPRS und WLAN, 2005, S 250

[107] Gerhard Lienemann, Virtuelle Private Netzwerke Aufbau und Nutzen 2002, S 92

Paketformate der austauchenden Pakete werden festgelegt, definiert bestimmte Funktionen. Außerdem legt es die Übergänge zwischen den verschiedenen Zuständen einer ISAKMP – Aushandlung fest.

Das OAKLEY Key Determination Protocol, das in RFC definiert ist, ist ein Schlüsselaustauschprotokoll, das auf dem Diffie- Hellman- Algorithmus basiert. Somit ermöglicht OAKLEY- Verfahren die Vereinbarung für zwei authentifizierte Kommunikationspartner einen gesicherten Austausch von Schlüsseln.

7. VPN an Schulen

7.1 Einfaches und sichere Schulnetz

Das Internet verändert der Welt auch die Schulwelt. Es bietet als neues Unterrichtsmedium viele Vorteile der Informationsbeschaffung. Es eröffnet den Schülerinnen und Schülern, aber auch den Lehrpersonen neue Perspektiven in der Informations- und Kommunikationsgesellschaft. Aus dem Schulzimmer heraus sind weltweit Informationen abrufbereit – wir können aus dem Schulzimmer heraus weltweit mit anderen Menschen kommunizieren, einzeln oder in Gruppen.

Bei allen Chancen und Vorteilen dürfen wir deshalb auch vor den Risiken und Gefahren nicht die

Augen verschließen:

- Ohne spezielle Maßnahmen ist die Sicherheit der Kommunikation nicht gewährleistet: Nicht nur unser Gegenüber kann lesen, was wir ihm mitteilen (keine Vertraulichkeit). Wir wissen nicht unbedingt und können nicht überprüfen, wer unser Gegenüber im Internet oder im E-Mail-Verkehr ist (keine Authentizität). Und was wir bekommen, ist nicht unbedingt das, was unser Gegenüber an uns gesandt hat oder was eine Anbieterin anbietet (keine Integrität).

- Im Internet lauern Gefahren für die Privatsphäre der User, weil Daten auf Websites 24 Stunden 365 Tage weltweit schrankenlos abrufbar und miteinander verknüpfbar, weiter bearbeit und verbreitbar sind, ohne Kenntnis der Betroffenen und außer Kontrolle der Schule.

- Gefahr für die Privatsphäre der User droht auch daher, dass wir bei jedem Besuch einer Website, mit jedem E-Mail, mit jedem Absenden eines Online-Formulars und mit jeder Äußerung in einer Chat Group Datenspuren hinterlassen im World Wide Web, die zum Teil auch mit Hilfe von Cookies gezielt gesammelt und mit der Methode des Data mining miteinander kombiniert werden – bis hin zur Erstellung eigentlicher Persönlichkeitsprofile über uns.

- Es lauern im Internet Gefahren für die Integrität der User und den Ruf der Schule**,** weil wir auf rechtswidrige Inhalte stoßen (Rassismus, Gewalt, Pornografie, Terrorismus, Ehrverletzungen usw.) können, weil wir uns strafbar machen können, wenn wir solche Inhalte weiterverbreiten, oder weil die Schulinfrastruktur für strafbare Aktionen missbraucht werden kann (z.B. durch denial of service attacks, durch von Schulrechnern aus gestartete Web-Angriffe).

- Durch die Informationsbeschaffung im Internet droht Gefahr für die Qualität unserer Arbeit, weil im Internet nicht bloß Wertvolles, Sinnvolles, Interessantes und Gutes verfügbar ist, sondern auch Wertloses, Sinnloses, Komisches, Schlechtes, und sich neue Probleme stellen bei der Prüfung der Seriosität einer Information oder Quelle.

- Außerdem drohen der Schulinfrastruktur Gefahren durch Viren, Trojanische Pferde und andere schädliche Programme, welche im harmloseren Fall den Unterrichtsbetrieb stören, in schwereren Fällen und bei fehlenden Sicherheits- und Abwehrmaßnahmen noch schwerere Schäden anrichten können.[108]

[108] http://www.baselland.ch/fileadmin/baselland/files/docs/jpd/ds/newsletter/news-026.pdf

7.1.1 Schulverwaltung

Der Einsatz von Internet und Neuen Medien stellt Schulen vor aktuelle pädagogische und sicherheitstechnische Herausforderungen. Unter Mitwirkung von Expertinnen aus dem IT-Bereich und den Schulen wurden Empfehlungen für die Gestaltung der Internet Security Schulstandort erarbeitet.

Bei Netzwerk an Schulen ist vor allem die pädagogisch- fachliche Betreuung wichtig. Trotzdem nehmen Sicherheitsfragen einen großen Teil der Alltagsarbeit von Netzwerkbetreuerinnen ein weiters werden von kommerziellen Netzwerken und Softwareindustrie Standards vorgegeben.

Mit dem Aufbruch ins medienpädagogische Zeitalter kommen zunehmend Werkzeuge wie schüler- und lehrereigene Notebooks, elektronische Lernplattformen und Web2.0 Anwendungen zum Einsatz, die in (Intranet) domäne- basierten Netzen Fremdkörper sind und eine zentralen Datenhaltung sowie die Userverwaltung am Schulstandort letztlich über flüssig machen.

Auch in Österreich haben sich Schulen bereits von betreuungs- und kostenintensiven Serverdiensten getrennt und stärker auf Dienstleistungsangebote zurückgegriffen. An vorderster Front stehen dabei zentral angebotene Lernmanagementplattformen für den Unterricht, die im Gegensatz zu lokalen Lösungen „ganz nebenbei“ auch den virtuellen Austausch zwischen Schulen und ihren Lehrenden fördern. Grundvoraussetzung ist allerdings eine zuverlässige und leistungsstarke Internetanbindung, über die eine steigende Anzahl von Schulstandorte bereits verfügt.
Allerdings ist unter datenschutzrechtlichen Gesichtspunkten die Frage der Datenhaltung eine wichtige, die in räumlicher Zuständigkeit in Österreich bleiben muss. Daher wird klar zu definieren sein, welche zentral auf Servern zu hosten sind. [109]
Schulnetze entwickeln sich sehr dynamisch und unterscheiden sich von der Mehrzahl der Firmennetze grundlegend. Lehrer/innen wie Schüler/innen verfügen über keinen fixen

[109] http://www.elearningcluster.com/pdf_s/erlass_08.pdf

Arbeitsplatz: Einmal ist es der Unterrichtsraum oder der EDV Saal, einmal ist es der Arbeitplatz zu Hause oder unterwegs.
Lehrer/innen haben meist im Lehrerzimmer die Möglichkeit einen Schule- PC oder das eigene Notebook zu nutzen. Grundlegende Forderung ist daher den Datentransport und Datenintegrität zwischen diesen Arbeitsplätzen sicherzustellen.

Notebooks erlauben eine flexiblere Handhabung von Lern- und Arbeitsphase über den Unterricht hinaus und bereiten die Schüler/innen besser aufs Berufsleben vor. Im Zusammenhang mit dem laufenden Arbeitsplatz wechsele (Schule, zu Hause, unterwegs) ergibt sich die Forderung, dass die Notebooks in den unterschiedlichen Umgebungen ohne wesentliche Einschränkungen betrieben werden können. Dabei sollten nicht nur dieselben Programme und Daten zur Verfügung stehen, sondern nach Möglichkeit mit derselben Benutzeroberfläche gearbeitet werden können.
Das tägliche Eindocken von mehreren hundert Notebooks wie an Notebookschulen stellt das Schulnetz auch vor neue Herausforderungen im Bereich Malware und Attacken.

Eine wichtige Balance, die an der Schule hergestellt werden muss, ist das Spannungsfeld zwischen Sicherheit und Offenheit des Netzes. „Hochsicherheitsnetze“ mögen aus zentraler Sicht optimal erscheinen, erzeugen aber viel unnötige Arbeit. Aus der Sicht der Lernenden wäre es wichtig, dass die Netzwerkstruktur bis zu einem gewissen Grad transparent ist und sich „unschädliche“ Netzwerkbefehle für Unterrichtszwecke auch absetzen lassen. [110]

Für den Bereich der Schulverwaltung legt das Votum 2000 des Beraterkreises für Schulrechner folgendes fest:

„Beim Einsatz der EDV in der Schulverwaltung muss die Vertraulichkeit, Integrität und Verfügbarkeit aller sensiblen Daten dauerhaft gewährleistet sein. Daher muss sicher gestellt sein, dass unautorisierten Personen ein Zugriff auf personenbezogene Daten und die zugehörigen Programme nicht möglich ist. Die Verantwortung hierfür liegt bei der Schule.

[110] http://www.elearningcluster.com/pdf_s/erlass_08.pdf

Gemäß der Dienstvereinbarung mit dem Hauptpersonalrat ist bei EDV- mäßiger Verwaltung von Lehrerdaten die Einbindung von Rechnern für Verwaltungs- und Unterrichtszwecke in ein einziges Netz nicht zulässig. Da ein optimaler Schutz nach wie vor nur in einer physikalischen Trennung der jeweiligen Netze gesehen wird, sind grundsätzlich Verwaltungsnetze von Rechnern zu Unterrichtszwecken physikalisch getrennt zu halten.

Wenn zur Nutzung der Datenfernübertragung ein Internetzugang aus dem Verwaltungsnetz nötig ist, so sind besondere Schutzmaßnahmen vor nicht autorisierten Zugriffen auf personenbezogene Daten zu treffen. Als mögliche Sicherheitsmaßnahmen werden empfohlen: Zugangskontrolle über die Einrichtung einer „Firewall“, die den gesamten Datenverkehr zwischen Internet und Schulverwaltungsbereich überprüft und filtert; zeitlich begrenzter Wahl-Zugang zum Internet, keine nach außen bekannte, feste IP-Adresse; Beschränkung des Zugriffs auf als sicher bekannte Adressen mit Identifizierung; eigener Mail-Server mit Beschränkung der angewandten Dienste (z. B. nur gesicherte E-Mails); sichere Nachrichtenübermittlung und zuverlässige Prüfung der eingehenden E-Mails, z. B. durch Virenscanner, Authentifizierung.

Eine detaillierter Zusammenstellung von Schutzmaßnahmen ist in der Neufassung der Erläuternden Hinweise zum Datenschutz bzw. in der Dienstvereinbarung mit dem Hauptpersonalrat enthalten.“ [111]

7. 1. 2 Unterricht

Für den Bereich außerhalb der direkten Schulverwaltung muss grundsätzlich unterschieden werden:

- Technischer Schutz der lokalen Rechner im LAN (Local Area Network)
- Inhaltlicher Schutz vor unerwünschten Inhalten im Internet

Beides ist Voraussetzung einer verantworteten Nutzung des Internets im Rahmen der Schule. Während für ersteren Bereich bereits umfangreiche Ausarbeitungen zur Verfügung stehen (siehe

[111] http://www.schule.bayern.de/texte/Sicherheit_im_Schulnetz.pdf

‘Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet’, erstellt vom Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Mai 2000 bzw. ‘IT Grundschutzhandbuch’ des Bundesamtes für Sicherheit in der Informationstechnik), ist der zweite Bereich noch wenig bearbeitet und unterliegt doch wachsender Nachfrage.

Diese Broschüre versucht, konkrete Umsetzungsmöglichkeiten für beide Bereiche anzubieten. Dabei werden speziell Produkte vorgestellt, die im Rahmen der an der Schule zur Verfügung stehenden Ressourcen beschafft und verwaltet werden können. Speziell der Bereich von technischen und inhaltlichen Schutzmöglichkeiten eines kompletten LANs ist derzeit noch nicht umfassend darstellbar, da die Produkte einerseits noch sehr hohe Kosten nach sich ziehen würden, sie andererseits noch nicht in einer komplexen Schulsituation getestet werden konnten.

Daher kann der Anspruch, eine für alle Schulen gleichermaßen finanzierbare, einfach handhabbare und gleichzeitig flexible Lösung für ein komplettes Schulnetz zur Verfügung zu haben, noch nicht erfüllt werden. [112]

7.2 Datensicherheiten

Daten sammeln, speichern, bearbeiten oder austauschen ist heute einfach. Die neuen Informations- und Kommunikationsmittel machen es möglich. Die Kehrseite der Medaille: Die Computertechnologie birgt Gefahren, auch und besonders für die Schule. Nicht selten werden unnötige, heikle oder schützenswerte Daten erhoben. Manchmal werden diese sensiblen Informationen leichtfertig weitergegeben. Zwar ohne böse Absicht, aber vielleicht zum Schaden der Schülerin oder des Schülers. Und manchmal werden dabei unwissentlich Amtsgeheimnis oder Persönlichkeitsrechte verletzt. Als Lehrerin, als Lehrer müssen wir die Bestimmungen über den Datenschutz kennen. Wir müssen wissen, wie wir sie im Schulalltag praktisch umsetzen

[112] http://www.schule.bayern.de/texte/Sicherheit_im_Schulnetz.pdf

können. Und wir müssen wissen, wie wir die Persönlichkeitsrechte wahren. Denn diese zu verletzen, kann disziplinarische, zivilrechtliche oder auch strafrechtliche Folgen haben.[113]

In Lerneinheit wird einen Überblick über die verschiedenen Bedrohungen, denen PC bzw. die Daten ausgesetzt sind, erhaltet. Wie wird die Datenverlust vorbeugen können?

- den verschiedenen Bedrohungen für die Daten- und Netzwerksicherheit,
- Methoden zur Erhöhung der Verfügbarkeit von Servern und Systemen sowie,
- mit den verschiedenen Schadprogrammen, gegen ein System geschützt müssen wird.

7.2.1 Bedrohungen

Ein Netzwerkadministrator ist für die Sicherheit seines verantwortlich. Er muss sich über die aktuellen Bedrohungen laufend informieren, um diese bekämpfen zu können. Ohne entsprechende Sicherheitsvorkehrungen stehen die Türen in ein Netzwerk weit offen. Für Unternehmen und Behörden ist dies eine sehr ernste Gefahr, denn Spione, Betrüger, Hacker gibt es überall auf der Welt.

Ein schlechtes Passwort ist eine offene Tür in ein Netzwerk. Hat ein Hacker erst einmal Zugriff, kann ihn nichts mehr aufhalten. Mittels Viren, Trajonern und Rootkits treibt er sein Unwesen und benutzt den geknackten PC als Plattform für weitere Angriffe.

[113] http://Shule-Leitfade-Datenschutz.pdf

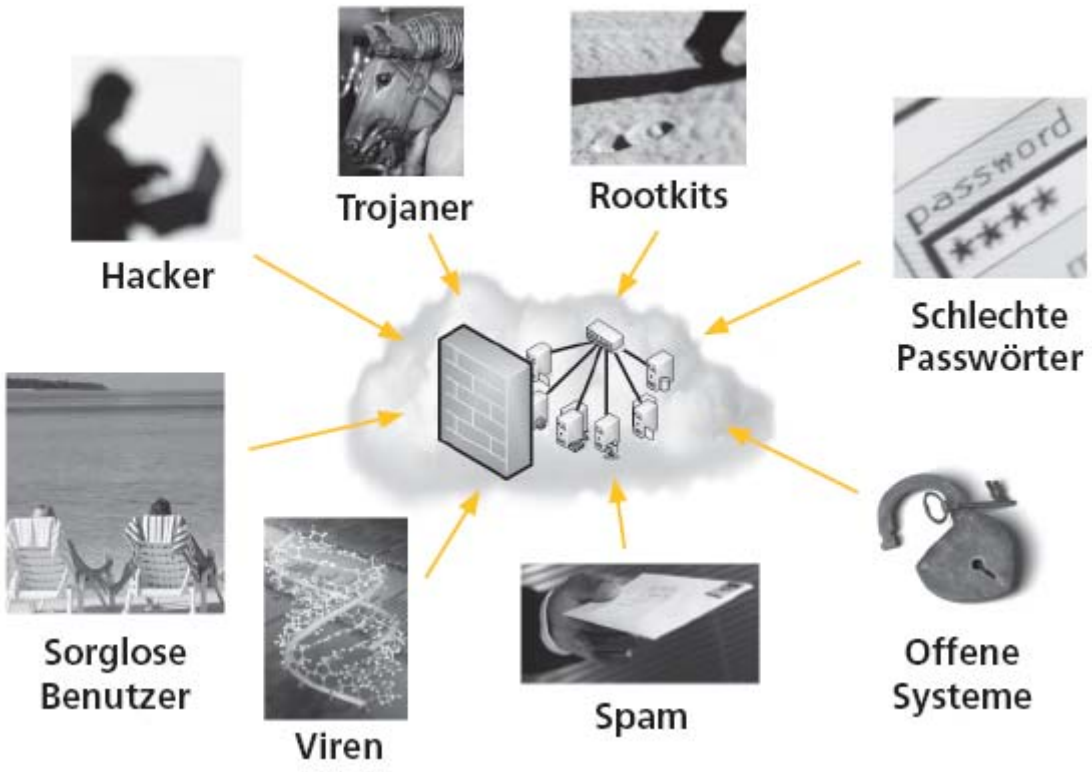

Abb. 7 : Bedrohungen für die Netzwerksicherheit

7.2.2 Angriffe aus dem Internet

7.2.2.1 Schadenstypen

In der Literatur finden sich grundsätzlich mehrere Beschreibungen von Schäden, die durch Angriffe auf das System unterschieden werden können. Die wesentlichen sind (aus Erkennung und Behandlung von Angriffen aus dem Internet, Wolf, Häger, Schorn, Gastbeitrag in Handbuch zur Datenschutz CD, Klaus Utech, Juni 2000):

- Manipulation von Dateien (z. B. Veränderung /Löschung von Dokumenten)
- Außer-Betrieb-Nehmen der Dienste (Denial-of-Service) (z. B. Ausschalten eines WEB-Servers)
- Vorspiegeln falscher Identität (z. B. Versand einer E-Mail unter falschem Namen)

- Unberechtigte Vertraulichkeit erwerben (z. B. fremde Daten mitlesen)

7.2.2.2 Trojanische Pferde

Diese Form von Programmen führt neben der Funktion, die dem Anwender bekannt ist und die dieser durchaus wünscht (z. B. Fernwartung eines entfernten Systems über das Internet) noch weitere, verborgene Funktionen aus, die unberechtigten Personen die Manipulation von Daten auf dem befallenen System ermöglicht. Die bekanntesten Vertreter sind Programme namens ‘Back Orifice ‘ für Windows-95/98 oder ‘rootkit’ für Unix- Systeme.

7.2.2.3 Ausführbare Dateien auf dem lokalen Rechner

Hier muss unterschieden werden zwischen Cookies, JavaScript, JavaApplet, ActiveX und Activ Scripting: Cookies sind kleine Datenmengen, die in einem speziellen Verzeichnis (meist gleichen Namens im Systemverzeichnis) abgespeichert werden, um üblicherweise Benutzereinstellungen beim Besuch einer Web-Site auszulesen und damit zu personalisieren. Beispielsweise wird beim Besuch der Website einer Bank das Datum des letzten Besuchs abgespeichert, um beim nächsten Aufruf die Kontenauszüge ab diesem Termin anzuzeigen. Eine Manipulation von Daten im System durch Cookies selbst ist nicht möglich. Dennoch kann die Analyse der vorhandenen Cookies auf einem Rechner Aufschluss über das Nutzerverhalten auf diesem System ermöglichen.[114]

[114] http://www.schule.bayern.de/texte/Sicherheit_im_Schulnetz.pdf

7.2.3 Schutz vor Schadprogrammen

Ein wichtiges Thema beim Schutz des heimischen PCs ist der Umgang mit Computeranomalien. Jeder Computernutzer hat schon einmal von Viren, Würmern und Trojanischen Pferden sowie von Dialern gehört. Hierbei handelt es sich um Schadprogramme, die überwiegend über das Internet verbreitet werden und auf den PCs ahnungsloser Nutzer ihre Wirkung entfalten.

In den in der gleichen Reihe erschienenen Arbeitsmaterialien zum Thema „Viren, Würmer, Trojaner“ werden verschiedene Typen von Computeranomalien ausführlich beschrieben sowie weiterführende Links und Übungsaufgaben empfohlen. An dieser Stelle möchten wir daher nur die wichtigsten Hinweise zum Schutz vor Schadprogrammen auflisten:

Schadprogramme gibt es praktisch nur für Windows-Systeme. Wer ein anderes Betriebssystem verwendet (z.B. Apple Mac OSX oder Linux), hat in der Regel damit bislang keine Probleme. Dies ist jedoch keine Gewähr dafür, dass die Betriebssysteme auch in Zukunft von Schadprogrammen verschonen bleiben werden. Windows-Nutzer sollten eine Antivirensoftware installieren und diese durch regelmäßige Updates auf dem aktuellen Stand halten.

ActiveX, eine Komponente der DirectX- Technologie von Microsoft, ist ein häufiges Einfallstor für Schadprogramme. Daher sollte ActiveX deaktiviert werden. Alternativ empfiehlt es sich, Programme zu nutzen, die ActiveX von vornherein nicht verwenden. E-Mails unbekannter Absender sollten ungelesen gelöscht werden. E-Mail-Anhänge sollten nur geöffnet werden, wenn der Absender bekannt ist. Auch dann ist jedoch nicht sichergestellt, dass die E-Mail wirklich vom Absender stammt. Die Absenderkennung könnte gefälscht sein.

In Browsern und E-Mail-Programmen können zudem Java und Javascript deaktiviert werden. Dies führt bei Browsern allerdings dazu, dass einige Internetseiten nicht mehr korrekt angezeigt

werden. Ein E-Mail-Programm hingegen braucht niemals Java oder Javascript – hier können diese also deaktiviert werden.[115]

7.2.4 Schutz der Daten vor unberechtigtem Zugriff durch andere Benutzer

Oft teilen sich mehrere Benutzer einen Computer. Ist dies der Fall, so kann durchaus ein Interesse daran bestehen, dass gespeicherte Daten vertraulich bleiben. Doch selbst, wenn dies nicht erforderlich sein sollte, ist es aus Gründen der Betriebssicherheit wünschenswert, den Zugriff auf „fremde“ Daten zu beschränken. Letztlich schützt dies auch vor unbeabsichtigten Änderungen oder gar dem Löschen von Dateien.

Moderne Betriebssysteme sind für den Mehrbenutzerbetrieb ausgelegt. So können Benutzer eingerichtet werden, die sich unter Angabe ihres Benutzernamens und ihres Passwortes beim System anmelden müssen, bevor sie mit der Arbeit beginnen können. Die Systeme bieten die Möglichkeit, die Zugriffsrechte auf Dateien und Verzeichnisse für die jeweiligen Benutzer einzustellen.

Dabei werden in der Regel „Rechte zum Lesen“ und „Rechte zum Schreiben“ der Dateien unterschieden. Je nach System kann es aber auch sehr viel feinere Differenzierungen geben. Die meisten heimischen Computer arbeiten mit Microsoft Windows als Betriebssystem. Oft ist dieses beim Kauf des PCs bereits installiert. Es gibt jedoch auch Alternativen zu Windows, die vor allem unter Sicherheitsaspekten interessant sind. Prinzipiell können zwei große Gruppen von Betriebssystemen für Arbeitsplatz- PCs unterschieden werden: zum einen die Windows-Versionen, zum anderen die „Abkömmlinge“ des ursprünglich von Großrechnern und Computern der mittleren Datentechnik stammenden UNIX-Systems. Letztere bilden ganze

[115] http://www.secure-it.nrw.de/_media/pdf/schule/pc_sicher_06_05.pdf

Betriebssystemfamilien, zu denen unter anderem Linux, Mac OSX, FreeBSD und Solaris gehören.[116]

7.3 Datenschutzen – Schutz der Persönlichkeitsrechte

Datenschutz ist Schutz der Persönlichkeitsrechte. Alle Menschen haben einen Anspruch auf den Schutz ihrer Privatsphäre, ihrer "privacy" Das Datenschutzgesetz nimmt deshalb auch die Schule in die Pflicht für den Schutz der Persönlichkeitsrechte, wenn sie ihre Schülerinnen und Schüler mit den neuen Medien vertraut machen will. Die Schule hat die ihr anvertrauten Menschen zu schützen – auch vor den neuen Gefahren, die mit der Einführung neuer Medien entstehen. Dabei hat sie nach dem Bildungsgesetz die Privatsphäre zu achten.

Wann kommt denn bei den neuen Medien der Datenschutz ins Spiel? Einmal, wenn die Schule selber Personendaten über Schülerinnen oder Lehrerinnen im Internet veröffentlicht, zum andern auch, wenn die Schule das User-Verhalten aufzeichnen und überwachen will, um auf diese Weise die Einhaltung von Nutzungsregeln zu überwachen. Und schließlich auch, wenn sie den Schülerinnen und Schülern Nutzungsverhalten nahe bringen will, welches die Privatsphäre schont.

Zur Unterstützung haben wir bei verschiedenen Schulen und Schulgremien Informationsveranstaltungen durchgeführt, um für die Gefahren und Risiken zu sensibilisieren und um Wege aufzuzeigen, wie die Schule ihre Verantwortung tragen kann und Privatsphäre schonend die Chancen und Vorteile der neuen Medien nutzen kann.

Letztlich geht es um die Vermittlung einer neuen Medienkompetenz und die Förderung der Selbstverantwortung im Umgang mit den neuen Medien. Dazu gehört eine ganze Palette von Maßnahmen, unter anderem auch der Privatsphäre schonende Umgang mit den neuen Medien, sei es in der Nutzung des Internets und seiner Dienste, aber auch in der Betreuung und Aufsicht über die Nutzung und beim Aufbau von Schulwebsites. [117]

---

[116] http://www.secure-it.nrw.de/_media/pdf/schule/pc_sicher_06_05.pdf

[117] http://www.baselland.ch/fileadmin/baselland/files/docs/jpd/ds/prak/prak-018.pdf

7.3.1 Empfehlungen für Datenschutz

Wir haben aus datenschutzrechtlicher Sicht Empfehlungen zu den folgenden Punkten formuliert:

- **Verantwortlichkeiten klar regeln** – nicht bloß für die technische Umsetzung, auch für die Information der Schülerinnen und Schüler, der Erziehungsberechtigten, für die Schulung und Unterstützung der Lehrpersonen, für die Aufsicht und Betreuung der Schülerinnen und Schüler und für die Betreuung von Schulwebsites.

- **Klare Nutzungsregeln aufstellen** – für die Nutzung (Netiquette4, Ehrencodex), über den Nutzungszweck, das Nutzungs- "Umfeld" (im Unterricht, außerhalb des Unterrichts, nur mit oder auch ohne Aufsicht) sowie für die Durchsetzung dieser Regeln.

- **Mit Information bei den Erziehungsberechtigten das Vertrauen gewinnen** – gerade bei den unteren Schulstufen wird es in der ersten Zeit entscheidend sein, bei den Erziehungsberechtigten durch sachliche Information über Nutzen und Risiken, über Regeln, Aufsicht und Betreuung Ängste und Befürchtungen abzubauen und das Vertrauen in die Wahrnehmung der Verantwortung durch die Schule zu stärken.

- **Den Lehrpersonen mit Schulung einen Vorsprung verschaffen** – insbesondere im Bereich der Medienkompetenz und der Betreuung der Schülerinnen und Schüler.

- **Die Schülerinnen und Schüler informieren und sensibilisieren** – aufklären über Nutzen und Risiken, über Regeln (Netiquette, Nutzungsregeln) und ihre Durchsetzung, über Möglichkeiten zur sicheren Nutzung der neuen Medien (Sicherheitstipps6), und damit die Selbstverantwortung fördern.

- **Mit Aufsicht, Betreuung und Überwachung die Einhaltung der Nutzungsregeln sicherstellen** – die Schülerinnen und Schüler in die Pflicht nehmen, primär transparent durch persönliche Aufsicht und Betreuung, allenfalls durch nicht personenbezogene Systemüberwachung; personenbezogene Überwachung erst bei konkretem Verdacht und nach ausdrücklicher Ankündigung (beim Verdacht auf strafbare Handlungen Strafverfolgungsbehörden einschalten).

- **Datensicherheit gewährleisten** – durch technische, organisatorische und rechtliche Maßnahmen, insbesondere auch durch die Durchsetzung der Benutzungsregeln, durch Virenschutz, Datensicherung und Optimierung der Sicherheitseinstellungen des Browsers. Mittelfristig wird das nicht anders gehen als durch den Aufbau eines Schulnetzes mit professioneller Betreuung. [118]

7.4 Schutzmöglichkeiten

Welche Möglichkeiten gibt es, die Rechnersysteme einer Schule vor Missbrauch zu schützen?

7.4.1 Räumliche Sicherungen

So selbstverständlich der Hinweis klingen mag, so oft wird er immer wieder missachtet. Räume, in denen Computer mit sensiblen Daten untergebracht sind, müssen physikalisch abgeschlossen und bei Bedarf mit zusätzlichen Sicherungen versehen sein. Alle logischen, softwaremäßigen Sicherheitseinstellungen helfen nicht, wenn der gesamte Rechner gestohlen oder die Festplatte ausgebaut und entwendet wird.

7.4.2 Physikalische Zugriffssicherung

Auf eine Festplatte, die nicht läuft, kann nicht zugegriffen werden. Diese einfache Wahrheit sollte genutzt werden, um physikalisch zu verhindern, dass Missbrauch mit schützenswerten Daten betrieben wird. So kann beispielsweise mit relativ geringem finanziellen Aufwand zusätzlich zu einer ersten Festplatte, die das Betriebssystem und wesentliche Programme enthält, eine zweite Festplatte zur Aufnahme der sensiblen Daten in einem Wechselrahmensystem installiert werden, dessen Stromzufuhr bei Nichtbenutzung der Daten mit dem eingebauten

[118] http://www.baselland.ch/fileadmin/baselland/files/docs/jpd/ds/newsletter/news-026.pdf

Schlüsselschalter unterbrochen wird. Bei Abwesenheit des Betreuers kann sie mit einem Handgriff entfernt und an einem sicheren Ort, beispielsweise dem Schulsafe, untergebracht werden.

Durch eine derartige Lösung ist sichergestellt, dass mit einem Gerät sowohl gefahrenfrei im Intra- und/oder Internet gearbeitet werden kann (bei abgeschalteter 2. Platte), als auch die zu schützenden Daten verarbeitet werden können, wenn die Platte eingeschaltet ist. [119]

7.4.3 Passwörter

Zitat aus dem IT- Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnik 2000:

„Folgende Regeln zum Passwortgebrauch sollten beachtet werden:

- Das Passwort darf nicht leicht zu erraten sein wie Namen, Kfz-Kennzeichen, Geburtsdatum.
- Innerhalb des Passwortes sollte mindestens ein Zeichen verwendet werden, das kein Buchstabe ist (Sonderzeichen oder Zahl).
- Das Passwort sollte mindestens 6 Zeichen lang sein. Es muss getestet werden, wie viele Stellen des Passwortes vom Rechner überprüft werden.
- Voreingestellte Passwörter (z. B. des Herstellers bei Auslieferung von Systemen) müssen durch individuelle Passwörter ersetzt werden.
- Passwörter dürfen nicht auf programmierbaren Funktionstasten gespeichert werden.
- Das Passwort muss geheim gehalten werden und sollte nur dem Benutzer persönlich bekannt sein.

[119] http://www.schule.bayern.de/texte/Sicherheit_im_Schulnetz.pdf

- Das Passwort sollte nur für die Hinterlegung schriftlich fixiert werden, wobei es dann in einem verschlossenen Umschlag sicher aufbewahrt wird. Wird es darüber hinaus aufgeschrieben, ist das Passwort zumindest so sicher wie eine Scheckkarte oder ein Geldschein aufzubewahren.
- Das Passwort muss regelmäßig gewechselt werden, z. B. alle 90 Tage.
- Ein Passwortwechsel ist durchzuführen, wenn das Passwort unautorisierten Personen bekannt geworden ist.
- Alte Passwörter sollten nach einem Passwortwechsel nicht mehr gebraucht werden.
- Die Eingabe des Passwortes sollte unbeobachtet stattfinden. Falls IT- technisch möglich, sollten folgende Randbedingungen eingehalten werden:
- Die Wahl von Trivialpasswörtern („BBBBBB“, „123456“) sollte verhindert werden.
- Jeder Benutzer muss sein eigenes Passwort jederzeit ändern können.
- Für die Erstanmeldung neuer Benutzer sollten Einmalpasswörter vergeben werden, also Passwörter, die nach einmaligem Gebrauch gewechselt werden müssen.
- In Netzen, in denen Passwörter unverschlüsselt übertragen werden, empfiehlt sich die dauerhafte Verwendung von Einmalpasswörtern.
- Nach dreifacher fehlerhafter Passworteingabe sollte eine Sperrung erfolgen, die nur vom Systemadministrator aufgehoben werden kann.
- Bei der Authentisierung in vernetzten Systemen sollten Passwörter nicht unverschlüsselt übertragen werden.
- Bei der Eingabe sollte das Passwort nicht auf dem Bildschirm angezeigt werden.

7.4.4 Firewall

Die am meisten vorgeschlagene Lösung zum Schutz von Arbeitsstationen vor Angriffen aus dem Internet ist die Errichtung einer Firewall (engl. etwa Brandschutzmauer). Generell wird darunter eine „Anordnung von Hard und Software verstanden, die als Übergang zwischen 2 zu trennenden TCP/IP- Netzen dient, von denen das eine einen höheren Schutzbedarf hat“ [Chapman95]. Neben der rein technischen Einrichtung sollten zusätzlich die Entwicklung einer passenden Sicherheitspolitik, die Protokollierung und das Management dieser Einrichtung berücksichtigt werden. Speziell die beiden letzteren, zeit- und personalintensiven Anforderungen können bei einer Schutzeinrichtung, die nicht nur Schutz suggeriert, sondern tatsächlich ernsthaft realisiert, nicht durch den Einkauf von Hard- und Software alleine erfüllt werden.

Technisch realisiert wird die Einrichtung einer Firewall durch Installation eines Softwarefilters (Packet-Filter bzw. Applikation - Gateway s. u.) am Übergang zwischen Internet und LAN (Local Area Network). [120]

7.5 Netzwerksicherheit mit VPN

Gerade Schulen müssen abgesicherte Kommunikation zum zentralen Schulamt gewähren. Vor allem im Hinblick auf Datenverschlüsselung, Internetzugriffe für die Schüler, Lehrkörper und nicht zuletzt Abschottung der einzelnen Bereiche mit dem dafür definierten Regeln. Aufgrund der permanenten Budget- Knappheit entsteht ein Spagat zwischen der geforderten Sicherheit und finanziellen Mitteln. In diesem Anwendungsbeispiel wird anhand einer virtuellen Stadt mit 25 Schulen kann ein tragbares Sicherheitskonzept umgesetzt und vor allem einfach administrierbar aufgebaut werden.

Ein „Standard IPSec VPN Konzept“ geht von „Site-to-Site“ Verbindungen aus. D.h. in jeder Lokation steht ein Gateway, dass sich mit einem zentralen Gateway tunnelt und somit sichere Kommunikation ermöglicht. Hierzu sollten alle Gateways vom gleichen Hersteller sein. Aber der

[120] http://www.schule.bayern.de/texte/Sicherheit_im_Schulnetz.pdf

zentrale Gateway muss entsprechend dimensioniert werden. Die Kosten übersteigen sehr schnell die ohnehin knappen Budgets.

Ein zentraler Gateway genügt und die einzelnen Server an den Schulen arbeiten als „Clients“. Man dreht quasi den Client um. Es ist jedoch zu berücksichtigen, dass stets ein Client eine Verbindung aufbauen muss. Im Klartext sollte der Client, also der Server, keine Verbindung aufbauen können, ist er auch nicht mehr erreichbar- man muss Vorort eingreifen. Dies kann allerdings ebenfalls bei „Site- to- Site “ Verbindung vorkommen.

Dabei wurde der datenschutzrechtliche Rahmen der Internet- Nutzung durch Schulen thematisiert, u.a. in welcher Form Internet- Auftritte an Schulen zu gestalten sind, wie elektronische Postfächer administriert werden dürfen.

Es wird festgelegt, dass durch organisatorische Maßnahmen (z.B. kein Betreten der EDV- Räume ohne Lehrkräfte eine solche Anordnung der Computer, dass von den Lehrkräften während des Unterrichts alle Bildschirme gesehen werden können) einer missbräuchlichen Nutzung des Internet bereits entgegengewirkt wird. Bei der Überprüfung von Download- Verzeichnissen auf den Ausbildungsrechnern fielen keine rechtswidrigen Inhalte auf. Technischer Handlungsbedarf besteht bei der Absicherung der Netze für die pädagogische Ausbildung, den Servern und Arbeitsplatzrechnern.[121]

[121] http://www.hob-networking.de/news/VPN/HOBLink_VPN_Schulen.pdf

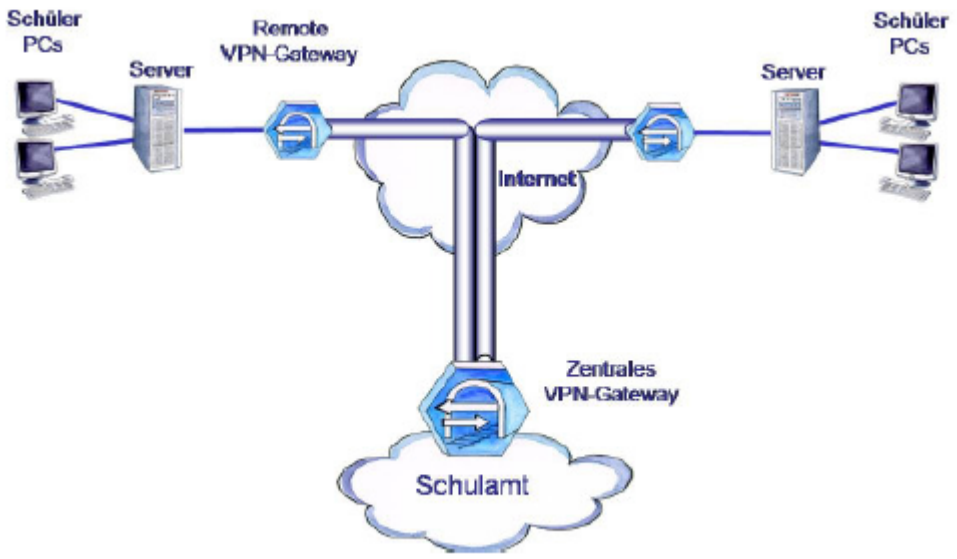

Abb. 8 : Site- to- Site VPN

Quelle: http://www.hob-networking.de

Bei der Vernetzung in Schulen kommen inzwischen auch Funknetze (WLAN- Wireless Local Area Network) zum Einsatz, weil diese insbesondere die Flexibilität und Mobilität im Arbeiten mit neuen Medien unterstützen. Da Funknetze offene Netze sind zusätzliche Absicherungen erforderlich.

Netzwerksicherheit in Schulen wird gemeinsam eine technische Musterlösung entwickelt, um den Schulen, die erforderlichen Sicherheiten zur Verfügung zu erstellen.

Die zusätzliche Sicherung erfolgt über die Einrichtung eines so genannten Virtuell Private Netzwerk (VPN) und dem Einsatz digitaler Zertifikate.

Jeder Rechner, der das Funknetz nutzen soll, bekommt ein eindeutig zuzuordnendes Zertifikat von TC Trustcenter GmbH. Anhand dieses Zertifikates kann ein Server überprüfen, ob der Computer die Berechtigung hat, sich an dem Netz anzumelden Vorteile von Zertifikaten sind.

- Nicht autorisierte Computer können sich nicht am Schulfunknetz anmelden.
- Es ist möglich, Zertifikate zu sperren (z.B. wenn ein Gerät gestohlen wurde) wieder zuzulassen.

Mittels eines Virtuellen Privaten Netzwerks erfolgt die Verbindung vom Funknetz in das Schulnetz verschlüsselt. Die Verbindung der Netze wird über einen Tunnel zwischen dem Client im Funknetz und dem so genannten VPN- Server ermöglicht.[122]

Die wesentliche Komponente der Sicherheitslösung basiert auf der Verwendung eines Virtuellen Privaten Netzwerks und bietet den Schulen die erforderliche Sicherheit. In einem VPN funktioniert eine Verbindung in das Netzwerk ausschließlich über einen so genannten VPN-Tunnel. Sämtliche Netzwerkkommunikation ist hierbei auf Basis des Secure Socket Layer Protokolls (SSL) verschlüsselt und noch außen geschützt. Für den Aufbau eines VPN- Tunnels muss sich ein Rechner im WLAN gegenüber dem VPN- Server mit einem Zertifikat authentifizieren.

7.6 Zugang von außen mit OpenVPN

Ein Zugang zum Schulnetz von zu Hause aus – Zugriff auf die Homeverzeichnisse, Moodle, E-Mail, die Webseiten im Intranet, die Schulkonsole – ist mehr als eine reine Arbeitserleichterung; für modernes E-Learning ist dies vielmehr unabdingbar. Aber auch als Administrator schätzt man es schnell, wenn man von zu Hause aus kleinere Wartungsarbeiten am Server durchführen kann. Bei der paedML Linux ist für den Zugang von außerhalb ein so genanntes Virtuelles Privates Netzwerk (VPN) vorgesehen. Die Grundidee eines VPN ist, dass man mit einer Art Tunnel das Schulnetz über das Internet bis zu seinem Computer zu Hause erweitert. Wenn eine VPN-Verbindung hergestellt ist, verhält sich der Computer weitgehend so, als befände er sich im Schulnetz. Man kann also alle Dienste, die im Intranet zur Verfügung stehen, genau so nutzen, als wäre man in der Schule. Die Verbindung des Rechners mit dem Schulnetz wird dabei mit einer

[122] http://3s.hh.schule.de/doc/NEWS-Handout-2007.pdf

besonders starken Methode verschlüsselt und ist somit sehr sicher. Es genügt auch nicht, sich mit einem Kennwort zu authentifizieren, zusätzlich benötigt man ein so genanntes Zertifikat, das man aus der Schule auf einer Diskette oder einem USBStick mit nach Hause nehmen muss. Aus Sicherheitsgründen sollte man es auf keinen Fall per E-Mail versenden. In der paedML Linux ist mit der freien Software OpenVPN ein solches VPN bereits einsatzfertig konfiguriert. Um es zu nutzen, muss ein Schüler oder Lehrer das erwähnte Zertifikat erstellen und dann ein kleines Programm auf seinem Rechner installieren, das mithilfe des Zertifikats das VPN aufbaut. Vorher muss der Administrator das Zertifikat noch aktivieren. Dies alles wird in diesem Abschnitt Schritt für Schritt beschrieben. Einzige Voraussetzung für die Nutzung von OpenVPN ist, dass der Server in der Schule aus dem Internet erreichbar ist. Eventuell sind dafür einige kleinere Vorarbeiten nötig, die später ausführlich beschrieben werden.

7.6.1 Zertifikat erstellen

Jeder Benutzer, der das VPN nutzen möchte, benötigt ein eigenes Zertifikat. Ein solches kann er sich schnell selbst erstellen. Gleich auf der Startseite der Schulkonsole findet sich der folgende Abschnitt:

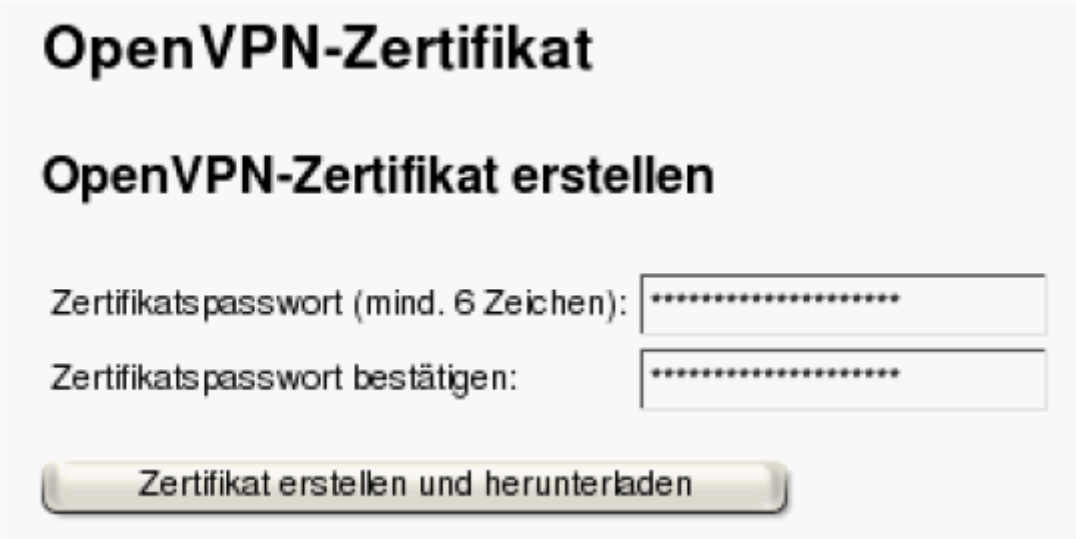

Abb. 9 : OpenVPN- Zertifikat

Quelle: http://www.amg.ka.schule-bw.de

Das Zertifikatspasswort kann später jederzeit geändert werden. Wenn man die Schaltfläche Zertifikat erstellen und herunterladen betätigt, wird das neue Zertifikat erstellt und in das Homeverzeichnis des Benutzers kopiert, und zwar in den Ordner OpenVPN (der Ordner wird dabei erstellt, falls er noch nicht vorhanden ist). Hat man einmal sein Zertifikat erstellt, so wird in Zukunft der Bereich zum Erstellen eines Zertifikates in der Schulkonsole nicht mehr angezeigt. Stattdessen findet man einen Knopf OpenVPN-Zertifikat herunterladen, mit dem man das Zertifikat jederzeit erneut in das Homeverzeichnis kopieren kann. [123]

[123] http://www.amg.ka.schule-bw.de/moodle/file.php/1/Dateien/Zugang_von_Aussen_mit_OpenVPN.pdf

8. Literaturverzeichnis

ALEXANDER, MICHAEL . : Netzwerke und Netzwerksicherheit : das Lehrbuch -1. Aufl. . - Heidelberg : Hüthig, 2006

BANSE, GERHARD , Zur Didaktik der IT-Sicherheit, Ingelheim : SecuMedia-Verl..1999

BECKER, DIRK , OpenVPN, das Praxisbuch/ Dirk Becker. - 1. Aufl. . - Bonn : Galileo Press, 2008

BECKER, PAUL , Sicherheit in der Informationstechnik, Paul Becker und Rudolf Hannig. - Vorabdr. . - Berlin : VDE-Verl. 1989

BENNER, KLAUS-DIETER , Mit IT-Sicherheit gegen Internet-Kriminalität, Bundesamt für Sicherheit in der Informationstechnik. Beitr. von: Klaus-Dieter Benner - Ingelheim : SecuMedia-Verl., 2002

BERGMANN, HERMANN-JOSEF , Datenschutz und Datensicherheit für vernetzte PCs, Hermann-Josef Bergmann ; Jutta Stolp. - Heidelberg : Hüthig, 1997

BERNERT, JÜRGEN , Sicher im Netz : Sicherheit im Internet / Jürgen Bernert. - Augsburg : Maro-Verl., 1999

BEUTELSPACHER, ALBRECHT, Moderne Verfahren der Kryptographie: Albrecht Beutelspacher ; Jörg Schwenk ; Klaus-Dieter Wolfenstetter. - 6., verb. Aufl. . - Wiesbaden : Vieweg, 2006

BÖHMER WOLFGANG, VPN - Virtual private networks. - 2., überarb. Aufl. - München ; Wien : Hanser, 2005

BRANDS, GILBERT ,IT-Sicherheitsmanagement: Protokolle, Netzwerksicherheit, Prozessorganisation - Berlin : Springer, 2005

BRAUN, TORSTEN, IPng: neue Internet-Dienste und virtuelle Netze: Protokolle, Programmierung und Internetworking . - Heidelberg : dpunkt.verlag, 1999

BUCHMANN, JOHANNES , Einführung in die Kryptographie. - 3., erw. Aufl. . - Berlin: Springer, 2004

BUCKBESCH, JÖRG, VPN - Virtuelle Private Netze: : sichere Unternehmenskommunikation in IP-Netzen; Rolf-Dieter Köhler. - Köln : Fossil-Verl., 2001

BUSCH, CHRISTOPH , Netzwerksicherheit. Stephen, D. Wolthusen. - Heidelberg : Spektrum, Akad. Verl, 2002

CHESWICK, WILLIAM R, Firewalls and internet security. - 12. print. - Reading, Mass. : Addison-Wesley, 1999

DAVIS, CARLTON R., IPSec : Tunneling im Internet, - 1. Aufl. . - Bonn : mitp, 2002

DIERSTEIN, RÜDIGER, Datenschutz und Datensicherung, Johannes-Kepler-Universität, Linz / Österreich, 21. - 23. September 1976 / hrsg. im Auftr. d. ÖGI u. GI von R. Dierstein .... - Köln : Bachem, 1976.

DORASWAMY ,NAGANAND IPSec. - München : Addison-Wesley, 2000

GERHARD, LIENEMANN, Virtuelle private Netzwerke : Aufbau und Nutzen. - Berlin : VDE-Verl., 2002

DAVIES, JOSEPH, LEWIS ELLIOT, Virtuelle private Netzwerke mit Windows Server 2003. - Unterschleißheim : Microsoft Press, 2004

KÖHLER, ROLF-DIETER, Auf dem Weg zu Multimedia-Netzen: : VPN, VLAN-Techniken, Datenpriorisierung . - Köln : Fossil, 1999

LEIBNER, PETER , TCP/IP-Netze: : Grundlagen, Anwendungen, Sicherheit / Peter Leibner. - 2. korr. Aufl. - Münster : Krehl, 2000

LIPP, MANFRED, VPN - Virtuelle private Netzwerke: : Aufbau und Sicherheit / Manfred Lipp. - Studentenausg. - München : Addison-Wesley, 2007

LOCKHART, ANDREW, Netzwerk- Sicherheit Hacks, Dt. Übers. von Andreas Bildstein. - 1. Aufl. . - Köln: O'Reilly, 2004

MAIRS, JOHN, VPNs : a beginner's guide - New York : McGraw-Hill/Osborne , 2002

MARTIN, JAMES , TCP-IP-Netzwerke: Architektur, Administration und Programmierung / Joe Leben - München : Prentice Hall, 1994

MEYN, CHRISTIAN , Verschlüsselung und innere Sicherheit. - 1. Aufl. - Wiesbaden : Dt. Univ.-Verl., 2003

PLÖTNER, JOHANNES , Praxisbuch Netzwerk-Sicherheit; Steffen Wendzel. - 1. Aufl. . - Bonn : Galileo Press, 2005

ROSE. MARSHALL T. , Einführung in die Verwaltung von TCP-IP-Netzen. - München ; Wien : Hanser , 1993

SCHWENK, JÖRG, Sicherheit und Kryptographie im Internet. - 2., erw. und verb. Aufl. . - Wiesbaden : Vieweg, 2005

SCHWENKLER THOMAS, Sicheres Netzwerkmanagement. - Berlin : Springer, 2006

SCOTT, CHARLIE, WOLFE PAUL, ERWIN MIKE, Virtuelle Private Netzwerke, - 1. Aufl. . - Köln : O'Reilly , 1999

Internetquelle:

http://3s.hh.schule.de (am 10.05.2009)

http://www.amg.ka.schule-bw.de (am 27.06.2009)

http://www.baselland.ch (am 27.06.2009)

http://www.elearningcluster.com, (am 10.05.2009)

http://www.hob-networking.de, (am 10.05.2009)

http://www.schloss-online.de, (am 28.06.2009)

http://www.schule.at/ , (am 28.06.2009)

http://www.schule.bayern.de, (am 27.06.2009)

http://www.secure-it.nrw.de, (am 27.06.2009)

http://www.voip-information.de/ , (am 28.06.2009)