High End Multiservice Networking:

Innovationen & Optimierung von konvergenten Netz-Infrastrukturen in Unternehmen

(Symposium II-4)

Extranet

VPN-Technik zum Aufbau sicherer Unternehmensnetze

Dipl.-Ing. Kai-Oliver Detken (http://kai.nord.de) war Leiter des Geschäftsbereichs *wwl network* der WWL vision2_market GmbH in Bremen, welcher aus drei Competence Centern (Consulting, Operation System, Internetworking) bestand. Dieser Geschäftsbereich ist für die Beratung bis zur Realisierung von IT-Plattform für E-Commerce- und E-Business-Projekten zuständig. Anfang 2001 machte er sich als Senior Consultant selbstständig und arbeitet seitdem in verschiedenen Projekten für die WWL Internet AG, in Forschungsprojekten für die Europäische Union und andere Auftraggeber. Seine Hauptbetätigungsfelder sind High-Speed-, Security- und Internet-Lösungen. Zusätzlich ist er für verschiedene Verlage aktiv, in denen er Artikel oder Bücher veröffentlicht. Sein aktuelles Buch mit dem gleichnamigen Titel „Extranet – VPN-Technik zum Aufbau sicherer Unternehmensnetze“ ist im Dezember 2000 im Verlag Addision-Wesley erschienen und behandelt die hier angesprochene Thematik im Detail.

INHALTSVERZEICHNIS

1 Einleitung

Die wachsende Bedeutung der Dezentralisierung von Geschäfts- und Produktionsprozessen, begleitet durch Outsourcing und internationale Kooperationen erfordert flexible und globale Informations- und Kommunikationsstrukturen und -prozesse. Es werden sogenannte virtuelle Organisationen gebildet, die ein Höchstmaß an Flexibilität und Effizienz erfordern. Eine virtuelle Organisation, die kontextspezifisch definiert und gebildet werden kann, stellt hohe Anforderungen an die Informationslogistik, da eine kommunikationsintensive Kooperation zwischen einer Vielzahl von meist geographisch verteilten Projektbeteiligten notwendig ist. Für die komplexen Strukturen wächst die Bedeutung von virtuellen Netzen bzw. Unternehmensnetzen (Virtual Private Networks bzw. Corporate Networks). Zu diesem Zwecke werden sog. Corporate Networks (CNs) eingesetzt, die das Ziel der Integration der privaten Netze der im Verbund agierenden/operierenden Organisationen haben. Diese Netze sind üblicherweise LANs oder sog. Intranets (falls man Internet-Technologien- und Anwendungen in LAN einsetzt) über Einrichtungen der öffentlichen Netze (WAN) wie z.B. Frame Relay, ISDN oder Mietleitungen/Standleitungen.

Obgleich CNs, als geschlossene Einheiten, Sicherheit und garantierte Bandbreite bieten, sind sie kostenintensiv. Die Kosten schlagen sich besonders im Management (Betrieb und Wartung) der Netzkomponenten nieder. Ein weiterer Nachteil ist die mangelnde Flexibilität in der Anbindung von neuen Partnern „On-Demand“. Jede neue Geschäftsbeziehung würde automatisch eine neue physikalische Verbindung bedeuten. Darüber hinaus wächst der Bedarf an externen mobilen Einheiten bzw. Nutzern, was die Kosten und das Management für die Einrichtung von privaten Einwählpunkten (Dial-Up Access) an beliebigen Orten in die Höhe treibt. Ein weiterer Sachverhalt ist die heterogene Systemlandschaft der Unternehmensnetze – die unterschiedlichen Teilsysteme wie Betriebssysteme, Mainframe und Desktop müssen konvergieren und interoperieren, sodass nur „offene“ IuK-Lösungen in Frage kommen. Aufgrund der Inkompatibilitäten zwischen derzeitigen VPN-Lösungen unterschiedlicher VPN-Anbieter besteht aber noch die Gefahr von Monopol-Abhängigkeiten.

Ein neuer Begriff in der IuK-Landschaft ist das Wort *Extranet*. Dabei ist ein Extranet im Grunde nur ein Intranet, welches nach außen (über die eigenen Unternehmensgrenzen hinweg) hin operiert bzw. geöffnet ist. Ein Extranet ist somit als logisches Netz zu definieren, welches man für eine geschlossene Benutzergruppe etabliert, während die Dienstleistungen über ein öffentliches Netz erbracht wird. Der Anwender betrachtet in jedem Fall die Verbindungen als sein privates Netz. Extranets werden heute oftmals mit VPNs gleichgesetzt und deshalb vornehmlich als die Realisierungsform von Corporate Networks (CNs) großer Unternehmen angesehen. Dabei gibt es unterschiedliche Möglichkeiten ein VPN zu etablieren. Über Leased Lines oder Festverbindungen im analogen oder digitalen Telefonnetz lassen sich eigene VPNs aufbauen. Dabei steht meistens die Nutzung von Leistungsmerkmalen nicht im Vordergrund, sondern Einsparungsmöglichkeiten und Verfügbarkeit. Zusätzlich lassen sich VPNs im Mobilfunkbereich genauso realisieren, wie im Festnetzbereich. Eine Integration von TK-Anlagen in das VPN kann dabei jedoch ohne Fixed-Mobile-Integration nur realisiert werden, wenn die TK-Anlage direkt oder virtuell in das Mobilfunknetz integriert wird. Somit lassen sich unterschiedliche VPNs für unterschiedliche Kundenanforderungen umsetzen.

Die Umsetzung auf ein Extranet wird zu einer Konvergenz von Netz- und Diensteplattformen führen. Somit werden bekannte Dienste auf alternativen Plattformen eingesetzt und neue, kombinierte (Multimedia-)Dienste wie Videoconferencing, E-Mail Handy, IP-

Telefonie, LAN-LAN-Verbindungen, Homebanking, Distant Learning, Multimedia Service, Shopping werden verfügbar sein.

Für die Verbindung der einzelnen Außenstellen werden sog. Tunneling-Verfahren eingesetzt, mit deren Hilfe sichere, private Verbindungen für Netzapplikationen über ein öffentliches oder ein unsicheres Medium zwischen abgesetzten Netzwerken und/oder einzelnen PC-Arbeitsplätzen zu einem zentralen Datennetz aufgebaut werden.

Der Einsatz von Extranets für Unternehmen bedarf der Berücksichtigung unterschiedlicher Anforderungen, die sich in folgende Punkte aufgliedern lassen. Diese Anforderungskriterien muss jedes Unternehmen an ein Extranet individuell berücksichtigen, wenn es effektiv, kostensparend, sicher und leistungsfähig eingesetzt werden soll:

- Verfügbarkeit
- Sicherheit
- Skalierbarkeit
- Performance
- Mobilität
- Netzwerkmanagement
- Accounting/Billing
- Migrationsfähigkeit/Integrierbarkeit

2 Gründe für den Aufbau eines Extranet

Die zunehmende Dezentralisierung und Globalisierung von Unternehmen sind starke Motoren für die Verwendung und Implementierung von Extranets. Hinzu kommt die steigende Konvergenz von Sprache und Daten. Da eine erhöhte Flexibilität bei den sich schnell entwickelnden Märkten erforderlich ist, stellt sich im Grunde nur die Frage nach den Anforderungen an ein Extranet und nicht mehr nach den Vor- und Nachteilen – der Bedarf für eine solche Kommunikationsstruktur ist in jedem Fall vorhanden:

1. An erster Stelle steht dabei natürlich die gewonnene **Flexibilität** eines Unternehmens, welches nun in der Lage ist, Kundenanfragen und Kundenwünsche schneller, effizienter und globaler abzudecken, als dies bislang der Fall war. Dabei stellt ein wichtiger Punkt die mögliche Sicherheit einer solchen logischen Infrastruktur dar, weil die Kommunikation immerhin über ein ungesichertes Netz stattfindet. Das TCP/IP-Protokoll wurde vor ca. 30 Jahren nicht für eine sichere Kommunikation geschaffen. Neue Mechanismen und Protokolle müssen diese in heterogener Umgebung garantieren.
2. Die **Integration von Sprache und Daten** wird zunehmend den IuK-Markt beherrschen. Beispiel für die Wichtigkeit dieser Konvergenz ist die Übernahme von Bay Networks von Nortel, die gleichermaßen Internet-, Netzwerk- wie Telekommunikations-Know-how in einem Unternehmen vereinen. Weitere Fusionen in dieser Größenordnung werden folgen.
3. Weiterhin steht heute neben der Integration von Sprache und Daten die **Mobilität** stark im Vordergrund. Der Teilnehmer möchte nicht mehr zwischen dem Fest- und Mobilfunknetz unterscheiden, wenn er auf die Unternehmensdaten oder Dienste und Applikationen zugreift. Er ist im Gegenteil nicht an Gebundenheit des Ortes oder geringe Übertragungsraten bzw. schlechte Sprachqualität interessiert. Ziel ist es, ungebunden von Ort und Zeit mit der Firma oder dem Kunden in Kontakt zu treten.

4. Das heißt, die **Performance** spielt ebenfalls eine bedeutende Rolle. Hiermit ist auch die Qualität gemeint, in der der Teilnehmer in der Lage ist, mit einer Gruppe zu kommunizieren.
5. Die **Verfügbarkeit und Zuverlässigkeit** der Dienste und Anwendungen stehen dabei auch ganz oben auf der Wunschliste der Anforderungen. Bei Einsatz eines Netzwerkmanagement-Systems kann die Verfügbarkeit stark angehoben werden.
6. Die **Transparenz und Kosteneffizienz** muss dabei natürlich auch berücksichtigt werden. Um dies zu erfüllen muss ein geeignetes Accounting und Billing implementiert sein, dass genaue Abrechnungen zulässt bzw. die eigenen Kosten ständig überprüft, um sich nicht aus dem Kostenrahmen zu bewegen.
7. Weiterhin muss ein Extranet als **offenes System** realisiert werden, welches zukünftige Entwicklungen berücksichtigt. Da momentan der Schwerpunkt klar auf dem Internetprotokoll (IP) liegt, ist der Einsatz von TCP/IP als Quasistandard zu bezeichnen. Hier werden auch zukünftig Entwicklungen stark vorangetrieben, um das Internet als Dienst-Integrationsplattform zu etablieren.

3 Wachstum des Extranet-Markts

Die Dienstumsätze mit sprachbasierten VPNs in Deutschland sollen nach Dataquest weiterhin stark zunehmen: 175 Mio. waren es bereits 1999! Die Prognosen der Dataquest gehen davon aus, dass eine weitere Steigerung stattfindet (269 Mio. im Jahr 2000, 377 Mio. im Jahr 2001 und 489 Mio. im Jahr 2002). Zusätzlich wird die Verbreitung von Extranets, den datenbasierten VPNs, ebenfalls stark ansteigen. Zwar nutzen bereits 30% der Unternehmen in Deutschland das Internet für eigene Präsentationszwecke aus, jedoch nutzen nur wenige Firmen momentan die Möglichkeiten eines Extranets. Hier wird es zu einem starken Wandel kommen, wenn das Internet die Sicherheitshürde überwunden hat.

Demnach wird es laut Dataquest zu einer Konvergenz von Netz- und Dienstplattformen kommen. Das heißt, bekannte Dienste werden auf alternativen Plattformen eingesetzt und neue, kombinierte Multimedia-Dienste wie Videokonferenzen, E-Mail über das Handy, IP-Telephonie, LAN-LAN-Verbindungen, Homebanking, Tele-learning, Multimedia-Service und Shopping werden verfügbar sein. Dann werden durch sinkende Tarife die Dienste in den Vordergrund treten.

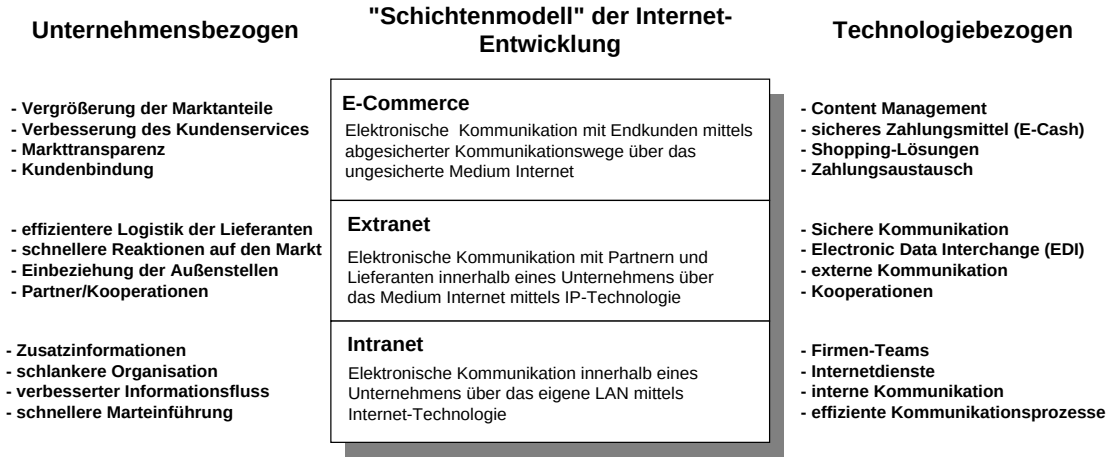

Abbildung 1: „Schichtenmodell“ der Internet-Entwicklung

Abbildung 1 zeigt die Abgrenzung des Intranet von einem Extranet bzw. der Anwendung E-Commerce. Neue Anforderungen des Marktes bzw. neue Anwendungen erfordern ganzheitliche Ansätze in der Informations- und Telekommunikationsstruktur. Die Vorteile bei der Kommunikation und Ausnutzung der Dienste eines Intranet werden in ein Extranet übernommen und für die Realisierung eines Virtual Private Network (VPN) umgesetzt. Dadurch können nicht nur die eigenen Mitarbeiter effizient Informationen miteinander austauschen, auch externe Unternehmensstandorte und Kooperationspartner profitieren davon. Zusätzlich werden in absehbarer Zeit Märkte für E-Commerce entstehen, die den Kunden in das Szenario integrieren werden. [5]

4 Begriffsbestimmungen

4.1 Corporate Network (CN)

Bislang wurden zwischen verteilten Unternehmensnetzen Corporate Networks (CNs) über Leased Lines aufgebaut, da diese Realisierungsmöglichkeit die einfachste und bislang einzige Methode für eine Firma darstellte, mit ihren Außenfilialen in Kontakt zu treten. Diese Lösung beinhaltete ein hohes Maß an Sicherheit, da die Leitungen über herkömmliche Provider oder Carrier gemietet wurden und eine garantierte Bandbreite eingehalten werden konnte. Allerdings war und ist diese Lösung auch mit sehr hohen Kosten verbunden, da Mietkosten monatlich anfallen und ein Management durchgeführt werden muss, um die Verfügbarkeit garantieren zu können. Hinzu kommt, dass eine Flexibilität praktisch nicht gewährleistet ist, da die Leitungen explizit geschwenkt oder hinzugenommen werden mussten, um neue Filialen anzubinden. Die Forderung nach mehr Mobilität erschwerte zusätzlich die Integration in ein bestehendes CN, da man das Zusammenwachsen von Mobil- und Festnetz nicht bedacht hatte. CNs waren zudem auch noch nur als abgeschlossenes System zu betreiben, da nur Lösungen für gleiche Netzstrukturen geschaffen wurden. Die Realität sieht aber heute ganz anders aus: heterogene Netze spiegeln die heutige Netzlandschaft wider, die durch die Einführung von Standards möglich geworden sind. Aufgrund der bestehenden Standards ist man deshalb heute bestrebt, offene Systeme zu implementieren, um auch für zukünftige Entwicklungen vorbereitet zu sein.

CNs bieten als geschlossene Einheiten Sicherheit und garantierte Bandbreite, sind aber sehr kostenintensiv. Die Kosten schlagen sich besonders im Management der Netzkomponenten (Betrieb und Wartung) nieder. Ein weiterer Nachteil ist die mangelnde Flexibilität in der Anbindung von neuen Partnern nach Bedarf. Jede neue Geschäftsbeziehung würde automatisch eine neue physikalische Verbindung bedeuten. Darüber hinaus wächst der Bedarf an externen mobilen Einheiten bzw. Nutzern, was die Kosten und das Management für die Einrichtung der privaten Einwählpunkte (Dial-up Access) an beliebigen Orten in die Höhe treibt. Ein weiterer Sachverhalt ist die heterogene Systemlandschaft der Unternehmensnetze – die unterschiedlichen Teilsysteme wie Betriebssysteme, Mainframe und Desktop müssen konvergieren und interoperieren, sodass nur „offene“ IuK-Lösungen Bedeutung haben können. Aufgrund der Inkompatibilitäten zwischen derzeitigen VPN-Lösungen unterschiedlicher VPN-Anbieter besteht noch die Gefahr von Monopolabhängigkeiten.

4.2 Virtual Private Network (VPN)

Ein weiterer Begriff der im Zusammenhang mit dem Internet immer wieder auftaucht, ist der des Virtual Private Network (VPN). Ein VPN kann man dabei als logisches Netz definie-

ren, welches für eine geschlossene Benutzergruppe etabliert wird. Die Dienstleistungen werden über ein öffentliches Netz erbracht, wobei der Anwender die Verbindungen als sein privates Netz betrachtet. VPNs werden heute vornehmlich als die Realisierungsform von Corporate Networks (CNs) großer Unternehmen angesehen. Dabei gibt es unterschiedliche Möglichkeiten ein VPN zu etablieren. Über Leased Lines oder Festverbindungen im analogen oder digitalen Telefonnetz lassen sich eigene VPNs, die man auch als CNs bezeichnet, aufbauen. Dabei steht meistens nicht die Nutzung von Leistungsmerkmalen im Vordergrund, sondern Einsparungsmöglichkeiten. Eine Realisierung von VPNs im Festnetz kann durch so genannte Intelligente Netze (IN) erfolgen oder durch Vermittlungsstellen-Kopplung wie das beispielsweise bei dem Produkt der Deutschen Telekom AG (DTAG) Centrex der Fall ist. Zusätzlich lassen sich VPNs im Mobilfunkbereich genauso realisieren wie im Festnetzbereich. Eine Integration von TK-Anlagen in das VPN kann dabei jedoch ohne Fixed-Mobile-Integration nur realisiert werden, wenn die TK-Anlage direkt oder virtuell in das Mobilfunknetz integriert wird. Hier kommt es zu einer Konvergenz auf Dienstebene mit Mailsystemen, Nummerierungsplan, Remote Access, Home und Mobile Office. Somit lassen sich VPNs für unterschiedliche Kundenanforderungen umsetzen.

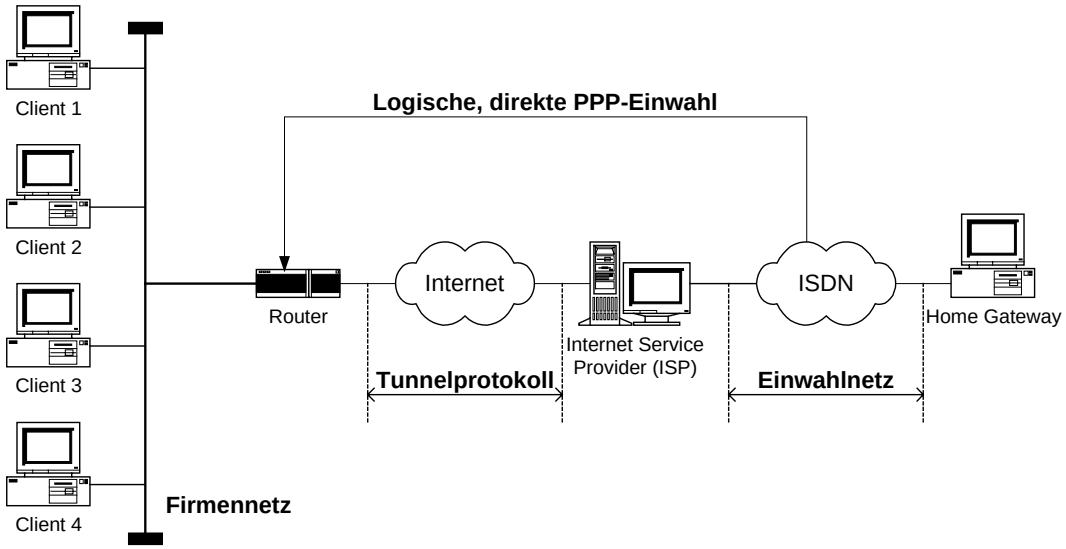

Abbildung 2: Aufbau eines Extranet über ein Tunnelprotokoll

Im Gegensatz dazu steht der Ansatz, IP-VPNs über das ungesicherte öffentliche Internet zu etablieren. Hier hat die Schaffung eines Zugangs zum Firmennetz mit der notwendigen Sicherheit und Funktionalität die oberste Priorität, damit kein Unterschied zum direkten Anschluss ans Firmennetz auftritt. Weitere wichtige Merkmale sind Verfügbarkeit, Zuverlässigkeit, Sicherheit, Performance, Transparenz und Kosteneffizienz, die für eine Remote Access VPN-Lösung sprechen.

Von rund 800 Millionen Dollar im Jahr 2001 auf 2,3 Milliarden Dollar in 2003 wird nach einer Studie der International Data Corporation (IDC) der europäische Markt für IP-VPNs anwachsen. Service-Provider richten sich mit IP-basierten VPNs an Firmen, die ihre Standorte weder über das öffentliche Internet noch über kostspielige Frame-Relay- und ATM-Dienste verbinden möchten. Ein Pluspunkt von IP-VPNs ist, dass über diese künftig neben Daten auch Sprache übertragen werden kann. Weitere Vorzüge sind die gute Skalierbarkeit und die vielfältigen Zugangstechniken. Allerdings weisen IP-Netze im Vergleich zu ihren Pendants auf Basis von ATM und Frame-Relay noch eine Reihe von Schwachpunkten auf, so die Experten. So seien beispielsweise die Verfahren für die Reservierung von Band-

breite unausgegoren. Auch was die Garantie einer bestimmten Verfügbarkeit oder Leistungsfähigkeit eines Dienstes angeht, erreichen IP-basierten Services noch nicht das Niveau der Konkurrenten.

Weitere Problemfelder sind die Sicherheit und das mangelhafte Zusammenspiel von IP-VPN-Komponenten unterschiedlicher Hersteller. Sie empfehlen, dass der Anwender ein IP-VPN zunächst für weniger kritische Aufgaben nutzen sollte, beispielsweise für den File-Transfer. Erst nach Abschluss dieser Testphase sei es angebracht, dem VPN unternehmenswichtige Prozesse anzuvertrauen.

Ein großes Verbesserungspotenzial im Markt für Virtual Private Networks (VPNs) hat die Unternehmensberatung Frost & Sullivan ermittelt. 500 europäische Großunternehmen, die entweder VPN-Nutzer sind oder planen, dies zu werden, bescheinigten den Anbietern Mängel in wesentlichen Punkten:

1. Produktanpassung
2. Kundenbetreuung
3. Produktinnovationen

Dass sich der Markt bisher immer noch in der Entwicklungsphase befindet, zeigt sich in den gegenwärtigen Bedürfnissen der Kunden. Der Studie zufolge stehen derzeit grundlegende Faktoren wie Preis, Verfügbarkeit des Dienstes, Zuverlässigkeit und Sicherheit im Vordergrund. Mehrwertfunktionen wie direkter PC-Zugang zu Telefonnetzen, abteilungsweise aufgeschlüsselte Abrechnung und Konvergenz von Daten und Sprache sowie von drahtloser und drahtgebundener Kommunikation spielen heute noch keine entscheidende Rolle für den Absatz von VPNs. Dies solle sich jedoch innerhalb der nächsten zwei Jahre ändern. Als wichtigste VPN-Anbieter nennt die Studie die Firmen AT&T, Unisource, Cable & Wireless, Concert, Equant, Global One, IBM, Infonet und MCI Worldcom.

4.3 Extranet

In diesem Zusammenhang fällt auch häufig der Begriff des Extranet. Dabei ist, wie schon gesagt, ein Extranet im Grunde nur ein Intranet, welches nach außen (über die eigenen Unternehmensgrenzen hinweg) über das Internet kommuniziert. Dementsprechend kann man es mit den Begriffen CN und VPN fast gleichgesetzt werden. Extranets beinhalten aber, im Gegensatz zu VPNs und CNs, immer die Verwendung der Internettechnologie. Das heißt, es werden in jedem Fall Internetdienste und Protokolle verwendet, was bei den anderen beiden Begriffen explizit angegeben werden müsste. Hinzu kommt, dass Extranets die Einbeziehung von Lieferanten und Partnern in das Unternehmensnetz beinhalten; für die Verbindung der einzelnen Außenstellen wird dabei ein Tunnel verwendet. Der Begriff Tunnel beschreibt allgemein eine Technologie, mit deren Hilfe sichere, private Verbindungen für Netzapplikationen über ein öffentliches, unsicheres Medium zwischen abgesetzten Netzwerken und/oder einzelnen PC-Arbeitsplätzen zu einem zentralen Datennetz aufgebaut werden.

Die Nutzungspotenziale von Extranets gegenüber privaten Netzen lassen sich wie folgt zusammenfassen:

1. Extranets bieten die Möglichkeit zu enormen Kosteneinsparungen.
2. Kundengewinnung und -bindung erfordert schnelle und einfache Mechanismen für Informationsverarbeitung und Kommunikation.

3. Der Aufbau eines Extranets löst die Kommunikationsengpässe von verteilten Geschäftsprozessen, wie beispielsweise in Produktion und Logistik.
4. Durch die Ausweitung des Unternehmensnetzes auf die Integration externer oder geschlossener (definierbarer und gestuft authentisierter) Benutzergruppen (wie Handelspartner, Lieferanten, Zulieferer oder ausgewählte Kunden) eröffnet neue Arten der effizienten Geschäftskommunikation
5. Auch durch die flexible Einbeziehung von mobilen Mitarbeitern (z.B. Außendienstmitarbeitern) oder die Anbindung von Telearbeitsplätzen in bestehende firmeninterne Informations- und Kommunikationsstrukturen wird der Informationsaustausch erheblich gefördert, Entscheidungswege verkürzt und somit ein flexibleres Agieren am Markt möglich.
6. Auch „kleine“ Geschäftspartner können kostengünstig in die Wertschöpfungskette integriert werden, was bei VPN zu kostenintensiv bzw. bei privaten Netzen technisch aufwändig war.
7. Ein Extranet begünstigt viele Bereiche in Organisationen und Unternehmen, wie Produktion, Angebotsbearbeitung, Bestellvorgänge, Auftragsabwicklung, Verkauf, Kundendienst, After-Sales, Projektmanagement, Aus- und Weiterbildung, Informationsteilung usw.
8. Extranets sind die zukünftige Netzplattform für Business-to-Business- (B2B) sowie Business-to-Customer- (B2C, d.h. E-Commerce) Kommunikation

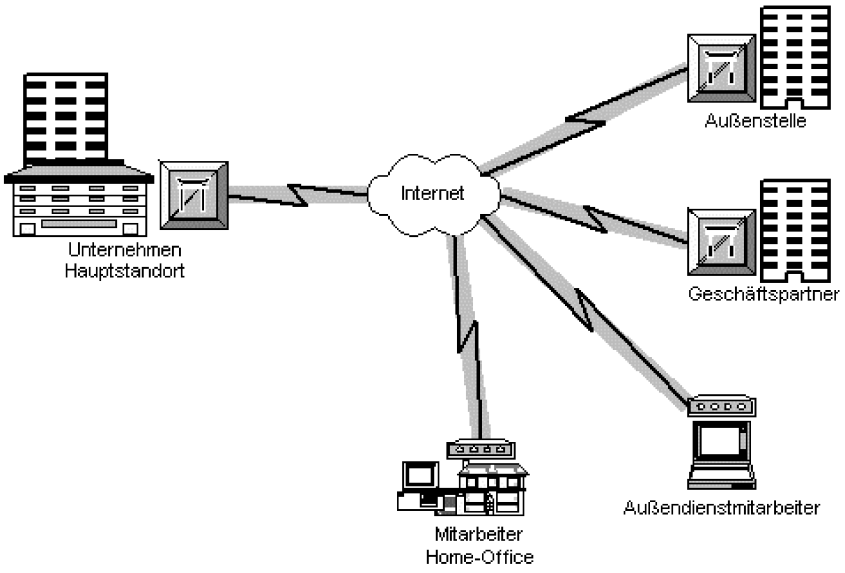

Abbildung 3: Globaler Aufbau eines Extranets

Seit 1999 installieren Firmen und Behörden verstärkt Extranets, um Kosten zu sparen und Außenstellen, Kunden oder Partner über das Internet ans Unternehmensnetz anzubinden. Einige Faktoren sprechen allerdings noch gegen den Einsatz von Intranets oder Extranets:

1. mangelnde Sicherheit
2. Probleme bei der Netzwerkadministration
3. Einsatz unausgereifter Techniken

4. Komplettlösungen sind kaum vorhanden
5. schwierige Integration von Anwendungen
6. Mangel an globalen Verzeichnissen
7. Schwächen bei der Replizierung von Daten

Diese Schwachpunkte werden gegenwärtig beseitigt, insbesondere mit Hilfe neuer Standards. Ein Beispiel dafür ist IPsec, eine Norm für die sichere Datenübertragung; die Arbeiten an diesem Standard sind noch im Fluss. Nicht zufriedenstellend geregelt sind unter anderem die Verschlüsselung und die Authentifizierung. Zudem kann die Performance bei Einsatz von IPsec-Implementierungen drastisch sinken, wenn es sich um reine Software-Implementierung handelt. Bei Hardware-Unterstützung werden momentan 60-90 MBit/s (z.B. Newbridge- und Cisco-Lösung) erreicht.

Weiterhin ist eine Internet Key Exchange (IKE) -Plattform nach RFC-2409 notwendig, um eine Schlüsselverwaltung durchführen und die Information nur einer bestimmten Benutzergruppe zur Verfügung stellen zu können. Die TeleSec (http://ww.telesec.de) stellt bereits heute Zertifikate für sichere Verschlüsselung her. SSL ist heute kein großes Thema mehr, da es nur TCP-Verbindungen verschlüsselt und applikationsabhängig ist. IPsec ist auch in Windows 2000 bereits vorhanden und ist in der IETF als der Sicherheitsstandard gekennzeichnet worden. Im ATM-Bereich gibt es ebenfalls einen ersten Standard, der auf die Verschlüsselung und Authentifizierung eingeht. Dies ist für High-Speed-Netze einzigartig und ermöglicht Echtzeitverschlüsselung auf Hardware-Basis. Hinzu kommt, dass unabhängig von der Anwendung verschlüsselt wird, sodass der Benutzer in seiner Arbeitsweise nicht eingeschränkt wird. [5]

5 Anforderungen an eine Extranet-Umgebung

Der globale Wettbewerb hat das heutige Geschäftsleben stark verändert und bietet innovativen Unternehmen neue Chancen. Ein entscheidender Wettbewerbsvorteil ist hierbei die jederzeit und überall garantierte Verfügbarkeit von Informationen. Das Thema Extranet steht dabei im Mittelpunkt von heutigen Überlegungen rund um die interne und externe Unternehmenskommunikation und betrifft sowohl die Daten- als auch die Sprachkommunikation. Experten sehen in dem Aufbau von Extranets die Möglichkeit zu enormen Kosteneinsparungen, einem großen Zuwachs an Leistungsmerkmalen und die immer wichtiger werdende Anbindung von Telearbeitsplätzen sowie Außendienstmitarbeitern, was mittlerweile auch unter dem Begriff SOHO (Small Office Home Office) subsummiert wird. Die Kundengewinnung und -bindung erfolgt neben den Kosten auch über die Entwicklung und Einrichtung von technischen Standards, die eine schnelle und einfache Kommunikation ermöglichen. Diese werden vom Anwender ebenso gefordert, wie die problemlose Anbindung an die bestehende Infrastruktur, insbesondere in heterogenen Netzwerkumgebungen.

Im diesem Zusammenhang sind neben der Qualität, die Geschwindigkeit und die Sicherheit, mit der Informationen verfügbar gemacht werden müssen, entscheidende Wettbewerbsfaktoren. Die IuK-Technologien greifen dabei mehr und mehr in die Gesamtheit der Geschäftsprozesse ein. Dem Extranet als Transportnetzwerk kommt dabei eine hohe Bedeutung zu, da es Anforderungen wie hohe Verfügbarkeit, einfache Skalierbarkeit, hohe Performance, einfaches Netzwerkmanagement und hohe Sicherheit genügen muss. Letzterer Punkt ist das Entscheidungskriterium beim Einsatz in Unternehmen und kann eine wesentliche Einstiegsschwelle darstellen.

5.1 Verfügbarkeit

Die Verfügbarkeit eines Netzes spielt heute für ein Unternehmen eine entscheidende Rolle und besitzt die höchste Priorität gegenüber anderen Anforderungen. Die Nichtverfügbarkeit eines Netzes bzw. die daraus resultierenden Verzögerungen in der Informationsverarbeitung und Kommunikation ist aus unternehmerischer Sicht untragbar, da sie monetäre und rechtliche Auswirkungen haben und dadurch immense Verluste bedeuten können. Paradigmen sind Verspätungen bei Transaktionen, Angeboten und Lieferungen.

Eine hohe Systemverfügbarkeit erfordert die redundante und ausfallsichere Auslegung von Komponenten (Hot-stand-by-Konfigurationen), um kleine Mean-Time-to-Repair Zeiten zu erreichen. Ein Extranet ist dabei in jedem Fall ein sog. Single-Point-of-Failure. Das heißt, ein Ausfall an einem Punkt (Netzübergang, Server, Firewall, Router usw.) muss ausgeschlossen werden. In diesem Zusammenhang sind Helpdesks und Hotlines unverzichtbare Elemente für den User Support.

In diesem Zusammenhang ist eine genaue Prüfung der Elemente Quality-of-Service (QoS), Verfügbarkeit und Zuverlässigkeit wichtig, da diese nicht unbedingt Bestandteil von Peering-Abkommen sind. Solche Network Interface Agreements, wie z.B. für Frame Relay (über Switched Virtual Circuits – SVC) sollen und werden in naher Zukunft, laut GartnerGroup, auch in Internet-Diensten Wirkung finden. Durch sinkende Tarife werden die Dienste in den Vordergrund treten. Die Verfügbarkeit wird allerdings nach wie vor den größten Stellenwert in Extranets einnehmen.

5.2 Sicherheit

Da das Extranet als Erweiterung des Intranets über die Organisationsgrenzen hinweg anzusehen ist, ist Sicherheit ein fokaler Punkt in der Entscheidung für den Einsatz von Extranets. Bei der Nutzung des Internet als Netz kommt diesem Sachverhalt eine besondere Bedeutung zu, da unternehmensinterne Informationen öffentlich zugänglich werden können. Sicherheit ist besonders kritisch für Organisationen wie Banken und Finanzinstitutionen, die das Netz zur Transaktion von hohen Geldsummen nutzen. Mangelnde Sicherheit in Systemen, Netzen und beim Transport von vertraulichen Daten sind bisher noch das größte Hindernis. In einer Umfrage der Fa. Security Dynamics Technologies gaben 80% der Netzwerkmanager an, dass mangelnde Sicherheit des Internet die größte Einsatzbarriere für Extranets darstellt [2]. 1996 meldete das Computer Emergency Response Team (CERT) mehr als 2.500 Sicherheitsvorfälle in ca. 11.000 Hosts. Dabei waren die gravierendsten Angriffstypen IP-Spoofing und Packet Sniffing. Wesentliche Kriterien für eine Sicherheitspolicy ist daher die Identifikation von Sicherheitslücken in Betriebssystemen und Systemprogrammen, Applikationen, des TCP/IP-Protokollstacks sowie Angriffstechniken. Die Sicherheitspolicy einer Organisation muss dabei so ausgelegt sein, dass ein ganzheitlicher, zentraler und organisationsweiter Sicherheitsmechanismus zum Tragen kommt. Dabei stützt dieser sich, zur Umsetzung der Sicherheitsanforderungen, auf die Analyse von internen und externen Zugangsprofilen (d.h., wer hat Zugang auf welche Daten über welche Systeme und Bereiche) und notwendigen technischen und organisatorischen Maßnahmen, die aus der Analyse der Zugangsprofile resultieren. Hierzu müssen Mechanismen wie Authentizität (Nachprüfbarkeit von Benutzern und Daten), Integrität (Nachprüfbarkeit bzw. Identifikation von Manipulationen der originären Daten), Nichtleugbarkeit (Sicherstellung der Eindeutigkeit von Quelle und Daten) und Vertraulichkeit (Datenverschlüsselung) eingesetzt werden.

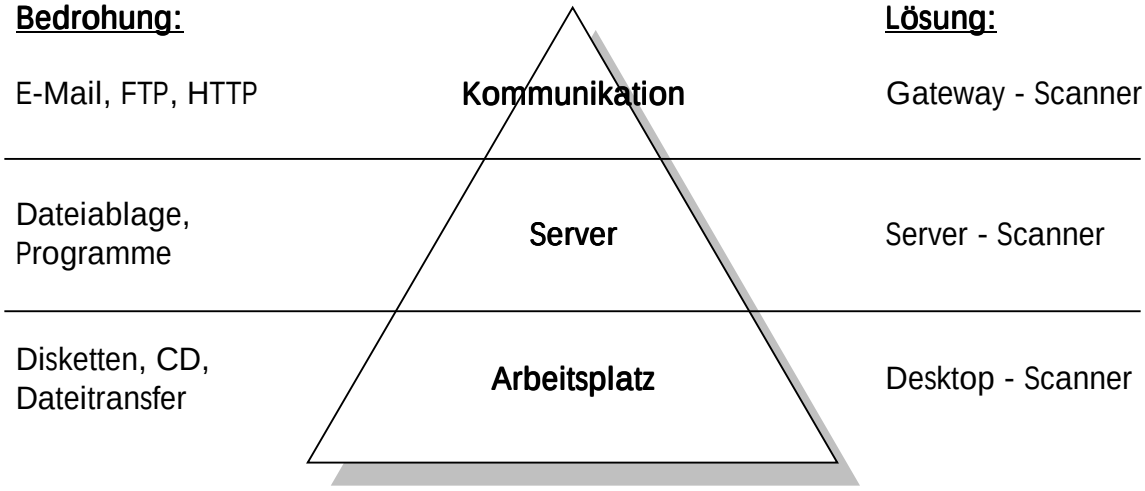

Abbildung 4: Virenbedrohung und Schutz

Extranets erfordern Mechanismen, die Flexibilität in der dynamischen Definition und Zuweisung von verschiedenen Sicherheitsleveln gestatten. Dieses wird immer wichtiger, da eine Globalisierung und Distribution stattfindet, die den weltweiten Austausch über ungesicherte Netze zwischen einer Vielzahl von Kommunikationsbeteiligten beinhaltet.

5.3 Skalierbarkeit

Die hohe Dynamik der Kommunikationsbeziehungen in einem Extranet muss durch eine flexible Skalierbarkeit begegnet werden. Die Skalierbarkeit muss sich auf die Netzwerkarchitektur, die Netzwerkkomponenten und das übergeordnete Netzwerkmanagement beziehen. Die Anzahl und Zugangsberechtigungen der Teilnehmer und Benutzer müssen schnell und effizient gemanagt werden können. Das bedeutet, dass Extranets auf bestehenden oder kommenden Standards aufbauen müssen, um eine feste Skalierbarkeit erreichen zu können. Der neue Standard IPsec wird dies zukünftig mit Verschlüsselung und Authentifizierung ermöglichen.

Die Integration von Sprache und Daten schafft eine weitere Voraussetzung: die Skalierbarkeit der Dienste. Im Inhouse-Bereich betrifft dies ISDN-TK-Anlagen, die PC-Vernetzung und den ISDN-Datenverkehr. Extern wird dann die Sprach/Datenintegration auf privaten Mietleitungen mittels Frame Relay oder ATM sowie öffentlichen Netzen wie ISDN und X.25 abgewickelt. Bislang gibt es kein physikalisches Netz für Sprache und Daten, weshalb auch keine einheitlichen Extranet-Dienste existieren. Extranets sind aber wirtschaftlich gesehen ein Managed Network Service mit Dienstfunktionen auf der Vermittlungsebene. Dabei sind Sicherheitsaspekte und Wachstumsraten entscheidend. Dabei spielen wiederum heutige Regulierungsaspekte eine bedeutende Rolle. Die Motivation für den Aufbau von Extranets ist die mögliche kurzfristige Bereitstellung von Diensten sowie die individuelle Gestaltung. Hierbei kann man die Dienstefunktionen als Bausteine betrachten, die flächendeckend über eine zentralisierte Dienstelogik verfügbar gestellt werden können. Der Intelligent Networks Architecture sind hier Grenzen gesetzt, die Herstellerabhängigkeit, traditionelle Signalisierung und Erzeugung von Engpässen durch Zentralisierung der Dienstfunktion betreffen. IN ist auf traditionelle Techniken aufgebaut, die eine Konvergenz im weiteren Sinne nicht ermöglicht. IP schafft hingegen die Voraussetzung für die Integration von Sprache und Daten über Extranets mit der notwendigen Skalierbarkeit.

5.4 Performance

Der Wunsch nach einer garantierten Dienstgüte, der sogenannte Begriff Quality-of-Service (QoS), entstand aus der Entwicklung von ATM heraus, da man ein Zellen-basiertes Verfahren für den Transport von Sprache, Video und Daten entwickeln wollte. Im Gegensatz zu traditionellen LAN-Technologien oder dem Internet waren bislang keine Mechanismen vorhanden, um eine bestimmte Qualität definieren zu können. Weil ATM als erste Netztechnologie diesen Ansatz berücksichtigte, konnten QoS-Mechanismen implementiert und eingesetzt werden. Dies war eine grundlegende Anforderung an ATM, da die gesamte Telefonie einmal über das B-ISDN geroutet werden sollte. Aus der Sicht von Anfang der neunziger Jahre war es deshalb selbstverständlich, dass nur ATM diese Merkmale bieten würde.

Inzwischen hat sich die TCP/IP-Protokollfamilie nicht nur im Internet durchgesetzt. Es entstehen immer mehr Intranets und Extranets, die sich die Dienste des Internets zunutze machen. In ihrer Entwicklung in die sechziger Jahre zurückgehend, fehlen den Protokollen der TCP/IP-Familie jegliche Kontrollstrukturen, die einen QoS ermöglichen könnten. Ansätze, wie beispielsweise das Resource Reservation Protocol (RSVP) versuchen diese inzwischen recht häufig gestellte Anforderung umzusetzen. Dabei muß man allerdings klar zwischen der garantierten Dienstgüte von ATM und den sogenannten Class-of-Services (CoS) unterscheiden. Diese bieten erstens keine garantierte Qualität für die Dauer der Verbindung an und zweitens gehen sie nicht auf Jitter und Verzögerungszeiten ein. Dies ist aber entscheidend für sensitive Daten wie beispielsweise Sprache.

Hohe Performance ist deshalb nur ein Parameter für die Dienstqualität (QoS), die sich im Grunde durch den Durchsatz bzw. Bandbreite ausdrückt. Schließlich ist, neben der Sicherheit, die garantierte Bandbreite für die Adaption von Extranets ein entscheidendes Kriterium. Um die Bandbreite in der Internet-Kommunikation garantieren zu können, werden Ansätze wie RSVP und Weighted Random Early Discards (WRED) verfolgt. Zusätzlich vertrauen ISPs immer mehr auf Technologien wie ATM und Frame Relay, um den Anforderungen nach Sicherheit und garantierter Bandbreite gerecht werden zu können.

5.5 Mobilität

Die steigende Notwendigkeit (GartnerGroup projizierte für 2002 weltweit eine Zahl von 100 Mio. Tele-Commutern) der externen Anbindung mobiler Nutzer im Sinne des „virtuellen Büros“ (z.B. Außendienstmitarbeiter) für den Zugriff auf Firmenressourcen, bedingt die flächendeckende Bereitstellung von Einwahlmöglichkeiten (Dial-In Remote Access). Die Anforderungen werden hierbei von Anzahl, Zugriffsverhalten, geographischer Verteilung und Zugangsberechtigungen (Autorisierung/Authentifizierung) der Nutzer bestimmt. Hier muss in den Gateways (Router, Firewalls, Server, etc.) eine angepasste Sicherheits- und Zugangsberechtigung Wirkung finden, da diese Klasse von Nutzern auf Netzressourcen wie Server und Drucker zugreifen. Eine Umfrage der IDC im Jahre 1998 unter WAN-Managern ergab, dass 93% der kleinen und mittelständischen Unternehmen (KMUs) und 96% der großen Unternehmen auf Remote Access Lösungen angewiesen sind. Dabei betreiben 57% Remote Access als Inhouse-Lösung, d.h. das Unternehmen realisiert selbst den Zugang von Außen. Das Outsourcing wird allerdings auch immer beliebter, da Authentifizierung (Überprüfung der Login ID und Passwort der Benutzer), Autorisierung (Klassifikation der Benutzerprivilegien), Accounting (Benutzerverhalten), Routing (Zugang zu spezifischen Netzen oder Systemen), Verschlüsselung, Fernüberwachung und -

management (externe Steuerung der Sicherheitssysteme) zum Service Provider verlagert werden kann. Organisationen profitieren von der höheren Flächendeckung der Service Provider, insbesondere ISPs, und brauchen keine multiplen Verbindungen nach außen.

GSM, DECT und Satellitenanbindungen wie über Inmarsat schaffen erste Voraussetzungen um bei geringen Datenraten zwischen 9,6 bis 384 kBit/s mobil auf das Extranet zuzugreifen. Neue Zugangsmöglichkeiten schafft die nächste Mobilfunkgeneration UMTS (Universal Mobile Telecommunication System). Hier werden Datenraten bis zu 2 MBit/s ermöglicht – allerdings nur in sog. Pikozellen. UMTS wird allerdings noch standardisiert und nicht vor 2002 verfügbar sein. Zukünftig werden aber Extranets in Kombination mit Mobilfunknetzen ohne Einschränkung der Funktionalität entstehen, sodass ein Zugriff auf die Firmendaten von überall her möglich wird.

5.6 Netzwerkmanagement

Im Vordergrund eines jeden Dienstes steht selbstverständlich das Management des zugrundeliegenden Netzes und Dienstes, welches Komponenten wie Authentifizierungs-Server, Remote Access Server, Router, Firewall, usw. umfasst. In diesem Zusammenhang ist die Frage zu klären, wem die Aufgabe des Managements obliegt. Dieser Punkt ist Bestandteil der Unternehmenspolitik und klärt die Fragestellung, ob Dienste ausgelagert (Outsourcing) oder intern betrieben werden sollen. Hierbei stellen Administrierbarkeit und der damit verbundene Personaleinsatz für den täglichen Betrieb wesentliche Entscheidungskriterien dar.

Weiterhin ist für den täglichen Betrieb, der eine hundertprozentige Verfügbarkeit voraussetzt, ein effizientes Netzwerkmanagement unverzichtbar. Hier sind allerdings noch Defizite zu verzeichnen, da eine einheitliche Standardisierung der Schnittstellen nicht vorliegt. Das heißt, die Hersteller waren bis vor einiger Zeit nicht bereit ihre Spezifikationen offen zu legen. Der Normalfall sind deshalb heute proprietäre Systeme, die nur in der jeweiligen Herstellerumgebung einsetzbar sind. In der IP-Umgebung hat sich allerdings das Simple Network Management Protocol (SNMP) etabliert, welches in heterogenen Netzen eingesetzt werden kann. Trotz einiger Defizite wird sich dieses Protokoll durchsetzen. In Extranets besteht deshalb die Chance auf Netzprotokollebene von Anfang an einheitliche Managementstrukturen zu schaffen. Erst durch die einheitliche Verwendung von SNMP kann dann im nächsten Schritt an ein Outsourcing gedacht werden, um den Verwaltungsaufwand möglichst gering zu halten. Dies impliziert jedoch auch ein Vertrauen gegenüber dem Service Anbieter, da dieser zwangsläufig Einsichten in die firmeninternen Intranet-Strukturen bekommen wird.

5.7 Accounting/Billing

Als weitere wichtige Anforderung an das Extranet sind aus betrieblicher Sicht das Accounting/Billing. Das Accounting sollte auf den Daten in den Authentifizierungs-Servern aufsetzen, um entsprechend daraus die Billing-Informationen für die Organisation zu generieren. Die Verarbeitung von Accounting-Informationen für Billing-Mechanismen, d.h. eine Kopplung zwischen Accounting und Billing ist besonders vorteilhaft, wenn die Authentifizierung beim Service Provider erfolgt. Die Billing/Accounting-Informationen beinhalten beispielsweise. Benutzernamen, Domain-Name der Organisation, Call ID, gewählte Nummer, Anfangs- und Endzeit bzw. Dauer, Anzahl der simultanen Verbindungen oder Tunnel für einen berechtigten Benutzer sowie Menge der gesendeten und empfangenen Pakete bzw.

Bytes. Von Vorteil wäre die Einbeziehung von protokollspezifischen Informationen, Dienstetyp (z.B. über die genutzten Protokoll-Ports) sowie Quelle- und Ziel-IP-Adresse.

Die Lage auf dem IuK-Markt stellt sich heute jedoch anders dar. Zwar haben fast alle Hersteller ihre Produkte mit entsprechenden Schnittstellen für Accounting/Billing ausgerüstet, sind jedoch nicht standardisiert. Zusätzlich werden Tools zur Auswertung der Daten nicht in ausreichendem Maße angeboten. Auch werden die Logfiles von Geräten verschiedener Hersteller nicht einheitlich ausgewertet, wodurch Inkompatibilität und redundante Ergebnisse zustande kommen können. Auch die Qualität der Protokolldateien lassen sich nicht vereinheitlichen, da teilweise nur die Verbindung und Datenmenge festgehalten wird, anstatt auch die Zugriffsdauer und die Dienstart aufzuzeichnen. Die Auswertung der entstandenen Logfiles unterschiedlicher Geräte sind deshalb schwer auszuwerten. Das Ziel muss es sein, ein benutzerspezifisches Accounting/Billing zu schaffen, um statt des bislang oft angewandten Flat-Rate Modells auch verschiedene Dienste mit entsprechenden Service Level Agreements (SLA) anbieten zu können. Diese könnten verschiedene Klassen einnehmen, die in der Dienstgüte (QoS) bzgl. Performance (Bandbreite, Round Trip Time bzw. Latenzzeit), Zuverlässigkeit (Paketverlustrate, Ausfallzeiten), Service (Multicast), Verfügbarkeit (POP-Zugang), User-Support (Help-Desk, 1st, 2nd und 3rd Level-Support) differieren. SLAs sind bereits Bestandteil von Verträgen mit und unter Service Providern geworden, für den Nutzer als Garantie betrachtet werden.

5.8 Migrationsfähigkeit/Integrierbarkeit

Konzepte zum Aufbau von Extranets haben grundsätzlich die Aufgabe existierende IuK-Strukturen und -Infrastrukturen (insbesondere Legacy-Systeme) so einzubinden, dass eine einfache und investitionsschützende Migration ermöglicht wird. Das umfasst auch den Support unterschiedlichster Netzwerkprotokolle wie IP, IPX, ATM, AppleTalk, DECnet, SNA usw. Zur Unterstützung von Migrationen ist das Internet-Protokoll wie geschaffen, da es immer schon in heterogener Umgebung eingesetzt wurde. Zusätzlich sind verschiedene Request-for-Comments (RFCs) vorhanden, die das Einbinden von Protokollen in IP beschreiben. Nur so lassen sich zentrale Standorte aufbauen, auf dessen Applikationen (z.B. SAP-Server) dann einheitlich zugegriffen werden kann. Alternativ zur direkten Umsetzung, die nicht für alle Protokolle angeboten wird, können Tunnel eingesetzt werden. Da der Einsatz von Tunnelmechanismen ohnehin beim Aufbau von Extranets gefordert ist, können zwei Anforderungen gleichzeitig erfüllt werden. [5]

6 Beurteilung der derzeitigen IPsec-Spezifikation

Die Spezifikation IPsec (u.a. RFC-2401, RFC-2402, RFC-2406) stellt die Grundlage für den einheitlichen Aufbau von Extranets heute dar. Eine ganze Reihe von Herstellern implementiert inzwischen IPsec, sodass die Anwender nicht mehr auf proprietäre Lösungen angewiesen sind. Allerdings ergeben sich durchaus noch Probleme in der Interoperabilität, da die Spezifikationen mitunter unterschiedlich interpretiert werden bzw. proprietäre Funktionen hinzu kommen. Um die Kompatibilität zwischen den Produkten zu erhöhen und die Sicherheit zu garantieren, stellt das Sicherheitsgremium ICSA (http://www.icsa.net) Zertifizierungen aus. Auf diese Zertifizierung sollte man achten, obwohl es nachweislich momentan auch noch keine Garantie für die Interoperabilität gibt. Bei IPsec müssen bezüglich dem Aufbau von Extranets folgende Punkte beachtet werden:

- Performance
- Migration

- Zugriffssicherheit
- Key Management
- Zertifikate

6.1 Performance

Die Performance im eigenen Intranet wird nicht von den Sicherheitsmechanismen von IPsec beeinträchtigt. Das liegt daran, dass diese nur innerhalb des Extranets und am Netzrand in der Firewall oder dem Router angewendet werden. Allerdings kommt es natürlich zu Einschränkungen zwischen den Teilnehmern eines Extranet. IPsec beinhaltet zwei grundlegende Sicherheitsmechanismen, die die Encapsulated Security Payload (ESP) und den Authentification Header (AH) beinhalten. ESP ist ein Mechanismus für die Integrität und Vertraulichkeit sowie teilweise für die Authentifizierung (z.B. in Verbindung mit AH) von IP-Paketen. Der ESP-Header ermöglicht Vertraulichkeit durch Verschlüsselung der zu übertragenen Daten. Hier werden zwei Modi unterschieden:

- Transportmode: Hier werden lediglich die Nutzlast verschlüsselt.
- Tunnelmode: Hier wird sowohl das komplette IP-Paket (Header und Daten) verschlüsselt sowie mit einem neuen IP-Header und Adresse versehen. Dabei bleibt die wahre Zieladresse, wie bei den Tunnelverfahren, verborgen und wird erst beim Empfänger entschlüsselt.

AH ist ein Mechanismus für Integrität und Authentizität von IP-Paketen. AH fügt direkt vor dem TCP-Header einen verschlüsselten Authentifikator ein, der mit einer kryptographischen Einwegfunktion (MD5) erzeugt wird. Die Nutzdaten dagegen sind unverschlüsselt. Zur Erzeugung des AH verwendet der Sender einen zu Beginn des Kommunikationsflusses vereinbarten gemeinsamen Schlüssel (gemäß dem Key Management Protokoll), den der Empfänger zur Überprüfung des Paketes einsetzt. AH kann alleine oder in Kombination mit ESP eingesetzt werden. Viele Kombinationen die zwischen beiden Verfahren möglich sind, kann man dabei im praktischen Einsatz vernachlässigen. AH sollte in jedem Falle eingesetzt werden, wenn der benutzte ESP-Algorithmus keine Integrität der verschlüsselten Daten garantiert.

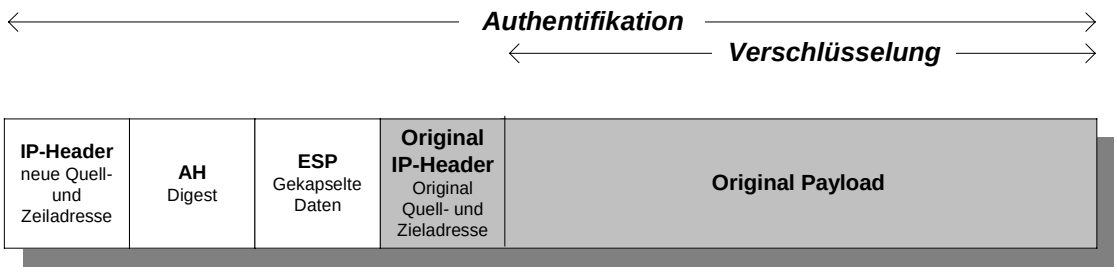

Abbildung 5: IPsec-Header mit AH und ESP

Asymmetrische Verschlüsselungsverfahren sind ungefähr um den Faktor 1000 langsamer im Vergleich zur symmetrischen Variante. Allerdings kann man eine höhere Sicherheit durch asymmetrische bzw. Public Key Verfahren durch größere Schlüssellängen erreichen. Kryptographische Algorithmen auf Hardware implementiert können die Performance erheblich steigern. Hier muss letztendlich zwischen Kosten/Nutzen bzw. Leistung/Sicherheit entschieden werden. Wenn man eine höhere Sicherheit sprich Verschlüsselung erhalten will, muss man Einschränkungen in der Performance hinnehmen. Hinzu kommt, das Au-

thentifizierung und Verschlüsselung die Leistungsfähigkeit mehr einschränkt, als wenn man nur über AH arbeiten würde.

In einem konkreten Beispiel wurden Performance Messungen zwischen zwei Linux-Systemen mittels durchgeführt. Das Testtool ttcp ermittelte auf einem Pentium-133 MHz-Rechner mit 32 MByte RAM über eine Fast-Ethernet-Verbindung 88 MBit/s im unverschlüsselten Modus. Mittels AH (HMAC-MD5) sank die Performance auf nur noch 20 MBit/s, während mit ESP (Triple-DES-MD5) der Durchsatz sich auf 2,56 MBit/s verringerte. Bei Einsatz beider Verfahren wurde der Wert 2,48 MBit/s erreicht. Hieran wird deutlich, dass ESP den Datenverkehr erheblich beeinflusst.

6.2 Migration

IPsec schütz IP-Pakete vor Modifikation und Abhören und beeinflusst keine anderen Protokolle oder Anwendungen. Ausnahmen bestätigen allerdings auch hier die Regel: SNA über IP. Hier wird Einfluss auf die Übertragung genommen, da einige für SNA notwendige Informationen durch IPsec verschlüsselt werden, sodass eine einfache Migration nicht gewährleistet ist. Normalerweise findet die Datenübertragung über IPsec aber transparent statt. IPsec-Pakete werden so über Router oder Switches weitergeleitet, ohne dass eine Softwareangleichung erfolgen muss. Das liegt daran, dass IPsec unterhalb der Transportschicht des OSI-Referenzmodells arbeitet. Somit ist es unabhängig bezüglich der vorhandenen Client/Serversoftware. Dadurch lässt sich eine End-to-end-Kommunikation über beliebige Netze herstellen, ohne auf die bestehende Hard- und Software Rücksicht nehmen zu müssen. Demnach ist IPsec einfach in bestehende IPv4-Umgebungen integrierbar.

6.3 Zugriffssicherheit

Der Transportmodus von IPsec schützt vorrangig höhere Schichtenprotokolle, was wiederum für den Einsatz End-to-end-Kommunikation spricht. Für Extranets ist allerdings die Authentifizierung als auch die Verschlüsselung bedeutsam. Deshalb wird der Einsatz von ESP und damit dem Tunnelmodus eine höhere Bedeutung zukommen. AH oder ESP verwenden aber zur Zeit noch Algorithmen wie Keyed MD5 und DES, die eine Nichtleugbarkeit nicht garantieren können. Der Einsatz von RSA ist hier sinnvoll und notwendig.

Weiterhin beinhaltet IPsec zur Zeit keinen Schutz gegen Replay-Attacken. Das heißt, ein altes Paket wird in den Datenstrom wieder eingebracht und erscheint als gültig. Ein solcher Schutz muss momentan noch auf der Anwendungsebene umgesetzt werden. Dies kann erhebliche Einflussnahme auf die Applikationen oder Systemsoftware zur Folge haben. Ein möglicher Erweiterungsvorschlag des IPsec-Protokolls wird diesbezüglich aber gerade diskutiert, sodass mit einer Abhilfe in absehbarer Zeit zu rechnen ist. Um eine höchstmögliche Sicherheit bezüglich der eingesetzten Anwendungen erhalten zu können, muss AH und ESP im Tunnelmodus eingesetzt werden. ESP alleine würde nur die unveränderlichen Daten im Originalpaket inklusive des ESP-Header und Trailer absichern.

6.4 Key Management

Die verzögerte Einführung eines standardisierten Key Management liegt an dem zeitlichen Ablauf der Diskussion der Arbeitsgruppe IPsec der IETF. Diese hatte zunächst die Sicherheitsfunktionen für IP spezifiziert und erst anschließend ein entsprechendes Protokoll für Key Management. Dabei stammt je eine Implementierung von dem National Institute of

Standards and Technology (NIST) und Cisco. Die erste Möglichkeit sieht dabei vor, dass die Schlüsselinformationen mit dem IP-Paket durch zusätzliche Header mitgeschickt werden. Das heißt, das Key Management verbleibt auf der gleichen Schicht. Der zweite Ansatz ist ein separates, universelles Key Management Protokoll, welches auf der Anwendungsebene arbeitet. Suns SKIP (Simple Key Management over IP) ist ein Beispiel für den ersten Ansatz, während ISAKMP die zweite Möglichkeit darstellt.

Um der Sicherheit der Kommunikation und sich schnell ändernden Konfigurationen aber Rechnung zu tragen, muss auf jeden Fall ein Key Management eingeführt werden. Dieses sollte automatisch den Schlüsselaustausch zwischen den Teilnehmern im Extranet vornehmen. Durch die Aufnahme neuer oder den Wegfall bestehender Kommunikationspartner ist daher von einer manuellen Konfiguration abzusehen. Diese wird allerdings in den meisten Produkten, heute verwendet, sollte aber wenn möglich ersetzt werden. Große Installationen sind auf ein automatisches Key Management angewiesen, da eine manuelle Konfiguration der Security Associations (SA) zwischen den Gateways (Firewall-Firewall) und Hosts (Client/Server) zu aufwendig ist. Genau dazu ist das Protokoll ISAKMP beziehungsweise dessen Realisierung in IKE (früher ISAKMP/Oakley) entwickelt worden. Zusätzlich müssen die unterschiedlichen Sicherheitsrichtlinien der Teilnehmer aufeinander angeglichen werden. IKE arbeitet in zwei Phasen, die Authentifizierungs- und Schlüsselgenerierungsphase. Vorteile des Verfahren sind, dass ohne großen Aufwand neue Schlüssel generiert werden können und das Verschlüsselungsverfahren ausgetauscht werden kann. Allerdings sind alle bisherigen Entwicklungen nicht alle frei außerhalb der USA verfügbar.

SA ist eine Art Vertrag über die einzuhaltenden Sicherheitsparameter einer bestimmten Kommunikationsbeziehung, die eindeutig festgelegt sind durch die Zieladresse und einem Security Parameter Index (SPI). Sie bilden einen Satz von Sicherheitsparametern, wie Authentifizierung und/oder Verschlüsselung, Schlüssel, Initialvektor für Verschlüsselung, Gültigkeitszeitraum der Schlüssel und der SA sowie die Adresse des Senders. Der Empfänger definiert den SPI und legt den Inhalt der SA fest.

6.5 Zertifikate

Der Einsatz in globaler Umgebung innerhalb eines Extranets macht den Einsatz und die Nutzung von öffentlichen Infrastrukturen erforderlich. Sie werden Public Key Infrastructure (PKI) genannt und bestehen nach dem Signaturgesetz aus folgenden Instanzen:

- Regulierungsbehörde
- Zertifizierungsstellen bzw. Trust Center
- Prüfstellen für Hard- und Software
- Anbieter von Soft- und Hardware
- Teilnehmer

Das Zusammenspiel dieser unterschiedlichen Instanzen bildet die PKI, die durch global verteilte Trust Center umgesetzt werden könnte. Diese müssen dann Aufgaben, wie Schlüsselmanagement, Zertifikatsverwaltung, Erstellung öffentlicher Schlüssel, Sicherung und Sperrung der Schlüssel sowie die Wiederherstellung wahrnehmen. Zusätzlich muss die Identität des Teilnehmers überprüft werden und ein Austausch zwischen den Trust Centern auf globaler Ebene erfolgen. Letztendlich ist die Qualität bei der Umsetzung dieser Aufgaben für die Vertrauenswürdigkeit und Verwendbarkeit der erteilten Zertifikate ausschlaggebend.

Im Bereich der Authentifizierung sollte die asymmetrische Verschlüsselung angewendet werden. Dabei erhält jeder Teilnehmer ein asymmetrisches Schlüsselpaar (Public Key, Private Key). Public Keys werden dem Teilnehmer in Form von Zertifikaten nach X.509 zur Verfügung gestellt, während die Private Keys die persönlichen Informationen des Eigentümers beinhalten. Ein Zertifikat kann dabei als Ausweis betrachtet werden, das die Identität des Teilnehmers sicherstellt. Nur ein Trust Center oder/und eine Regulierungsbehörde darf ein Zertifikat ausstellen. Dieses wird dem Teilnehmer über öffentlich zugängliche Verzeichnisse nach X.500 zur Verfügung gestellt. Obwohl dieser Ansatz eine sehr sichere Erweiterung für den Aufbau eines Extranets darstellt, welcher gerade bei mobilen Teilnehmern wichtig ist, muss der höhere Verwaltungsaufwand sowie höhere Investitionen für Software auf den Clients und Teilnehmerzertifikate hinzugerechnet werden. Es sollte deshalb eine Kosten/Nutzen-Analyse zuerst vorgenommen werden. [5]

7 Fazit

Der Aufbau eines Extranets beinhaltet eine Vielzahl von Anforderungen an die Planung und Konzeption. Gerade die genannten Punkte spielen dabei eine herausragende Rolle und sind für die Umsetzung entscheidend. Die Kostenvorteile gegenüber o.a. Netztechnologien und die hohe Flexibilität versprechen ein hohes Marktvolumen in der Zukunft. Jedoch erschweren derzeit fehlende Standards und Sicherheitslücken die Akzeptanz von Extranets, gerade bei großen Unternehmen. Dies wird sich in der nahen Zukunft ändern, da mit Hochdruck an den fehlenden Spezifikationen gearbeitet wird.

IPsec ist noch eine sehr junge Spezifikation, die noch wesentlich weiterentwickelt werden muss. Aus diesem Grund wird bereits an der nächsten Version gearbeitet, die u.a. die Einbindung von Certificate Authorities und den standardisierten Tunnelaufbau über variierende Subnetze einbezieht. Grundsätzlich werden IPsec-Tunnel durch zwei Endpunkte bzw. Subnetze definiert. Es müssen aber auch zusätzliche Angaben wie Festlegung der Algorithmen für Authentifizierung und Verschlüsselung vorab festgelegt werden.

Manche Hersteller haben eigene Datenkompression in die Softwarelösung integriert, wodurch es zu Problemen beim Etablieren der Tunnel kommen kann. Trotzdem wird der Spezifikation IPsec die größte Zukunft vorausgesagt, im Gegensatz zu anderen Tunnel- und Verschlüsselungsprotokollen auf Schicht 2 oder 3. Aus diesem Grund sind IPsec-Lösungen auf der nächsten Seite zusammengefasst worden, um Extranets/VPNs aufzubauen. Für eine detailliertere Betrachtung sei das Buch „Extranet – VPN-Technik zum Aufbau sicherer Unternehmensnetze“ empfohlen, welches gerade im Addision-Wesley-Verlag erschienen ist.

8 IPsec – Hersteller und Produkte

Name	Hersteller	IP-Version	RFC-1828/1852	RFC-1829/1851	Transport Mode	Tunnel Mode	Key Management	Plattformen	IPsec Code
Hydrangea	WIDE project	IPv4, IPv6	Ja	Ja	Ja	Nein	Manuell, IKE (ISAKMP + Oakley), Pluto (Photuris)	Free BSD 2.2.2, BSDI BSD/OS 3.0 Geplant: NetBSD	WIDE project
Novell Boarder-Manager	Novell, Inc.	IPv4, IPv6 (geplant)	Ja	Ja	Ja	Ja	Manual, IKE (ISAKMP + Oakley), SKIP	NetWare /Intranet Ware	Refer-enced NRL
e-Lock VPN	Frontier Technologies Corp.	IPv4	Ja	Ja	Nein	Nein	Manual, IKE (ISAKMP + Oakley)	Windows NT 4.0, Geplant: Windows95/98	Eigenes Design
Secure VPN	3COM	IPv4	Nein	Ja	Ja	Nein	Manual, IKE (ISAKMP + Oakley)	NetBuilder	3COM
PERMIT /Gate	TimeStep Corpora-tion	IPv4	Nein	Nein	Ja	Ja	Manuell , IKE (ISAKMP + Oakley)	Embeded	TimeStep IPSec Devel-oper's Toolkit
PERMIT /Client	TimeStep Corpora-tion	IPv4	Nein	Nein	Ja	Ja	Manuell, IKE (I-SAKMP + Oakley)	Windows NT 4.0, Windows 95, Macintosh	TimeStep IPSec Devel-oper's Toolkit
TimeStep IPSec De-veloper's Toolkit	TimeStep Corpora-tion	IPv4	Ja	Ja	Ja	Ja	Manuell, IKE (I-SAKMP + Oakley)	Plattformunab-hängig	TimeStep IPSec Devel-oper's Toolkit
IPv6 for HP-UX 9.05	Swedish Institute of Computer Science (SICS)	IPv6	Nein	Nein	Nein	Nein	Manuell	HP-UX	NRL
Firewall-1	Check Point Soft-ware Technolo-gies	IPv4	Ja	Ja	Nein	Ja	Manual, IKE (ISAKMP + Oakley), SKIP, proprietär	Solaris, SunOS 4, HPUX, AIX, Windows NT	Check Point
CyLAN IPSEC and ISAKMP/Oakley Toolkit	CyLAN Technologies	IPv4	Ja	Ja	Ja	Ja	Manuell, IKE (ISAKMP + Oakley)	Portable Source Code	CyLAN
OpenBSD	OpenBSD Project	IPv4	Ja	Ja	Ja	Ja	Manuell, Pluto (Photuris)	OpenBSD, alle Plattformen	OpenBSD, JI
BorderWare Firewall Server	Secure Computing Corpora-tion	IPv4	Ja	Ja	Ja	Ja	Proprietär	Standalone-Firewall	NRL
ANX	Secure Computing Corpora-tion	IPv4	Ja	Ja	Ja	Ja	IKE (ISAKMP + Oakley)	Proprietär OS basierend auf BSDI 3.0	NRL
Mentat TCP	Mentat Inc.	IPv4	Ja	Ja	Ja	Ja	Manuell,	Alle STREAMS	Mentat Inc.

							IKE (ISAKMP + Oakley)	Plattformen	
Eagle VPN	Raptor Systems Inc.	IPv4	Ja	Ja	Ja	Ja	Manuell, IKE (ISAKMP + Oakley)	Windows NT, Solaris, HPUX	-
SSH IPSec	SSH Communi-cations Security Oy	IPv4	Ja	Ja	Ja	Ja	Manuell, IKE (ISAKMP + Oakley)	*BSD, So-laris/STREAMS (geplant), Mac/ STREAMS (partial), NT (partial)	SSH
Secure Access	Ascend Communic ations, Inc.	IPv4	Ja	Ja	Ja	Ja	Manuell, IKE (ISAKMP + Oakley)	Ascend Router	Ascend
ERP IPSEC	Bellcore	IPv4	Ja	Ja	-	-	Manuell	-	-
NE-Secure	Cabletron /Network Express	IPv4	Nein	Ja	-	-	Manuell, proprietär	Cyberswitch	Cable-tron/Netwo rk Express
Cisco IOS (TM)	Cisco Systems	IPv4	Ja	Ja	-	-	IKE (ISAKMP + Oakley)	Cisco	Cisco Systems
ISAKMP with Oakley Extensions Key Mgmt Daemon	Cisco Systems	IPv4	-	-	-	-	IKE (ISAKMP + Oakley)	Jedes System mit NRL PF_KEY Key Management API	Cisco Systems
CyLAN IPSEC and ISAKMP/Oa kley Toolkit	CyLAN Technologi es	IPv4	Ja	Ja	Ja	Ja	Manuell, IKE (ISAKMP + Oakley)	Portierbarer Source Code	CyLAN
ISAKMPv6 ISAKMP / Oakley Resoluti-onv2	Defence Research Agency - UK	IPv4	Ja	Ja	Ja	Ja	Manuell, ISAKMP + Oakley	Solaris	Modified ETHZ
S/WAN Linux IPSEC	Electronic Frontier Foundation	IPv4	Ja	Ja	Nein	Ja	Manuell	LINUX 2.0.28, 2.1.29 by 4/97; NetBSD-current; BSD/OS 2.0	JI, original BSDI code 12/95, angepaßt für Linux
Enskip	ETH Zürich	IPv4	Ja	Ja	-	-	SKIP (Draft 6)	Solaris 2.4+, IRIX, NetBSD, Nextstep	ETH Zürich
OnNet	FTP Soft-ware	IPv4	Ja	Ja	-	-	Manuell, IKE (ISAKMP + Oakley)	Windows95, Windows 3.11	FTP Soft-ware
Trusted Security Firewall-Guard (GTFW-GD)	Gemini	IPv4	Ja	Ja	-	-	Manuell, proprietär	Gemini Trusted Firewall-Guard	Gemini
IBM SNG	IBM	IPv4	Ja	Ja	-	-	Manuell, proprietär	IBM AIX	IBM
ISI/USC	Information Sciences Institute, USC	IPv4	Ja	Nein	-	-	Statisch zu konfi-gurieren	BSD	NRL-derived and ISI-developed
SafeNet	Information Resources Engineer-	IPv4	Nein	Nein	-	-	SKIP	V.34 Modem, IP over PPP, Ethernet	Informa-tion Re-sources

	ing, Inc.								Engineer-ing
NRL IPv6/IPsec Software Distribution	Naval Research Laboratory (NRL)	IPv4 und IPv6	Ja	Ja	-	-	Manuell, PF_KEY Key Management API, inkl. Ciscos ISAKMP + Oakley Dämon	Jedes 4.4-Lite BSDish Sys-tem, NetBSD, BSDI, 4.4 BSD	NRL
Border-Guard and Security Router	Network Systems	IPv4	TBD	TBD	-	-	Manuell, proprietär	Network Sys-tems Router	Network Systems
NIST/NSA IPSEC Prototype	NIST & NSA	IPv4	Ja	Ja	-	-	Manuell, PF_SADB Interface	BSD/OS, NetBSD, FreeBSD, DTOS	NIST & NSA
Sun SKIP	Sun Micro-systems' Internet Commerce Group (Sun ICG)	IPv4	Ja	Ja	-	-	SKIP	SunOS 4.1.x	Sun ICG
Solaris 2.x	Sun Solaris Internet Engineer-ing	IPv6	Nein	Nein	Ja	Nein	Manuell, Geplant: IKE (ISAKMP + Oakley)	Solaris 2.x	Sun + NRL
Network CryptoGate (NCG)	Toshiba Corporatio	IPv4	Ja	Ja	Nein	Ja	Manuell, SKIP	BSD/OS	Toshiba
TIS Gauntlet	Trusted Information Systems	IPv4	Ja	Ja	-	-	Manuell, proprietär	TIS Gauntlet	NRL-derive
NCP Ad-vanced Remote Access Center (NARAC)	NCPengi-neering	IPv4	Ge-plant	Ge-plant	Geplant	Ge-plant	Manuell	Windows95/98, Windows NT	NCPengi-neering
VPN Ware Systems	VPnet Technologi es	IPv4	-	-	Ja	Ja	SKIP und IKE Key Management (VSU-1010, VSU-1100, VSU-10)	Windows95/98, Windows NT, OS/2	VPnet Technolo-gies

Tabelle 1: IPsec – Hersteller und Produkte

9 Literaturverweis

[1] Detken, Kai-Oliver: Sicherheitsmechanismen bei der Kommunikation über VPNs; IIR-Konferenz; Mit Virtual Private Networks zum Geschäftserfolg; 19.-20.1.; Frankfurt 1999

[2] The Case for Strong User Authentication in VPN Deployments; Whitepaper, May 1998, Security Dynamics Technologies; http://www.securitydynamics.com/

[3] Schwermann, Kai: IP-Billing und Accounting: Auf Heller und Pfennig; Gateway 02/99; Computerwoche Verlag GmbH; München 1999

[4] Detken, Kai-Oliver: Extranets - IP-basierte VPNs; Handbuch "Telekommunikation - Dienste und Netze wirtschaftlich planen, einsetzen und organisieren", Aktualisie-

rungslieferung September 2000; INTEREST-Verlag, ISBN 3-8245-2175-8; Augsburg 2000

[5] Detken, Eren: Extranet - VPN-Technik zum Aufbau sicherer Unternehmensnetze; Addision-Wesley-Verlag; Pearson Education Deutschland GmbH; ISBN 3-8273-1674-X; München 2001

[6] Raepple: Virtuelle Private Netze – Transportsicherung; iX-Magazin 01/99; Heinz Heise Verlag; Hannover 1999

10 Abkürzungsverzeichnis

ACD	Automatical Call Distribution
AH	Authentification Header
ATM	Asynchronous Transfer Mode
CERT	Computer Emergency Response Team
CHAP	Challenge Handshake Authentication Protocol
CIX	Commercial Internet eXchange
CN	Corporate Network
CLIP	Calling Line Identification Presentation
COLP	Connected Line Identification Presentation
DDV	Datendirektverbindungen
DE-NIC	Deutsches Network Information Center
DES	Data Encryption Standard
DMZ	De-Militarisierte Zone
D-GIX	Distributed GIX
DTAG	Deutschen Telekom AG
E-Commerce	Electronic Commerce
ESP	Encapsulated Security Payload
FTP	File Transfer Protocol
GIX	Global Internet Exchange
GSM	Global System for Mobile Communication
HDTV	High Definition Television
HTTP	HyperText Transport Protocol
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IN	Intelligent Networks
IP	Internet Protocol
IPsec	IP Security
IPX	Internetwork Packet Exchange Protocol
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
IuK	Informations- und Kommunikationstechnik
L2F	Layer-2-Forwarding-Protokoll
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
KMU	Kleine und Mittelständische Unternehmen
MD5	Message Digest 5
MIME	Multipurpose Internet Mail Extension
NAT	Network Address Translation

NCSA	National Computer Security Association
NIST	National Institute of Standards and Technology
PAP	Password Authentication Protocol
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
POP	Point-of-Presence
PPTP	Point-to-Point Tunneling Protocol
PSTN	Public Switched Telecommunication Network
QoS	Quality-of-Service
RAS	Remote Access Server
RFC	Request-for-Comments
RFC-2401	Security Architecture for the Internet Protocol
RFC-2402	IP Authentication Header
RFC-2406	IP Encapsulating Security Payload (ESP)
RFC-1828	IP Authentication using Keyed MD5
RFC-1829	The ESP DES-CBC
RFC-1851	The ESP Triple DES
RFC-1852	IP Authentication using Keyed SHA
RIPE	Réseaux IP Européens
RSA	River Shamir Adlemann
RSVP	Resource Reservation Protocol
SA	Security Association
SDH	Synchronous Transfer Mode
SLA	Service Level Agreements
SKIP	Simple Key Management over IP
S/MIME	Secure MIME
SNA	Systems Network Architecture
SNMP	Simple Network Management Protocol
SPI	Security Parameter Index
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
UMTS	Universal Mobile Telecommunication System
VPN	Virtual Private Network
WAN	Wide Area Network
WRED	Weighted Random Early Discards
X.500	Information technology – OSI: Overview of concepts, models, and services
X.509	Information technology – OSI: Authentication framework