Virtual Private Networks auf IPsec-Basis[1]

– Test und Evaluierung ausgewählter Produkte –

Jochen Schlichting[2]; Jörg Hartmann[3], Hartmut Pohl [3];

1. Zusammenfassung

Virtual Private Networks (VPN) werden zur vertrauenswürdigen Kommunikation über unsichere Netze eingesetzt, wenn die Maßnahme benutzer- und anwendungstransparent erfolgen soll. IPsec ist ein Protokoll für VPN zur Sicherung der Kommunikation auf IP-Ebene. IPsec-Konformität ermöglicht Kompatibilität der Produkte verschiedener Hersteller.

Entsprechend dem für eine site-to-site Anwendung durchgeführten reproduzierbaren Test der Sicherheitseigenschaften sind einige der verfügbaren Produkte für den Unternehmenseinsatz geeignet. Ein einfacher Bewertungsansatz mit Vorschlägen zur Verbesserung des IPsec-Standards wird vorgelegt.

2. Motivation

Unternehmen sind auf das Internet als eine umfassende und globale Kommunikationsinfrastruktur angewiesen. Dabei wird das Internet nicht mehr nur zur Kommunikation mit Dritten (Versenden und Empfangen von e-mails und zum Lesen von HTML-Seiten) verwendet, sondern auch zur vertrauenswürdigen Vernetzung der eigenen Unternehmensstandorte. Darüber hinaus benötigen moderne Arbeitsformen wie Telearbeit und Mobile Computing eine vertrauenswürdige Kommunikationsinfrastruktur. Damit können z.B. Außendienstmitarbeiter und Geschäftspartner auch von außerhalb des Unternehmens Dienste und Informationen des Intranet nutzen. Virtual Private Networks gewährleisten eine vertrauenswürdige Kommunikation zwischen dezentralen Standorten.

Viele Unternehmen gehen derzeit dazu über, ihre heterogene Welt der Hardware- und Software-Produkte zu vereinheitlichen und nur noch kompatible Sicherheitsprodukte und insbesondere nur noch Standard-konforme Verschlüsselungsverfahren einzusetzen.

So werden z.B. zur Verschlüsselung (Konzelation), für die digitale Signatur, die Authentifizierung etc. benötigte Schlüssel nicht mehr in dem jeweils benutzten Produkt - und damit mit jeweils unterschiedlichem Sicherheitsniveau - generiert, sondern vielmehr von einer sog. Public Key Infrastructure (PKI). Vergl. hierzu die Abbildung 'Ebenen der Verschlüsselung'. PKI enthalten über das hier relevante Key Management hinaus weitere allgemein nutzbare Funktionen.

---

[1] Erschinen in: Bauknecht, K; Teufel, S.: Sicherheit in Informationssystemen – SIS 2000. Zürich 2000

[2] Lessing & Partner Unternehmensberatung für EDV-Sicherheit GmbH,
Schloss Kellenberg, Jülich.

[3] Labor für Informationssicherheit, Fachbereich Angewandte Informatik,
Fachhochschule Bonn-Rhein-Sieg, Sankt Augustin.

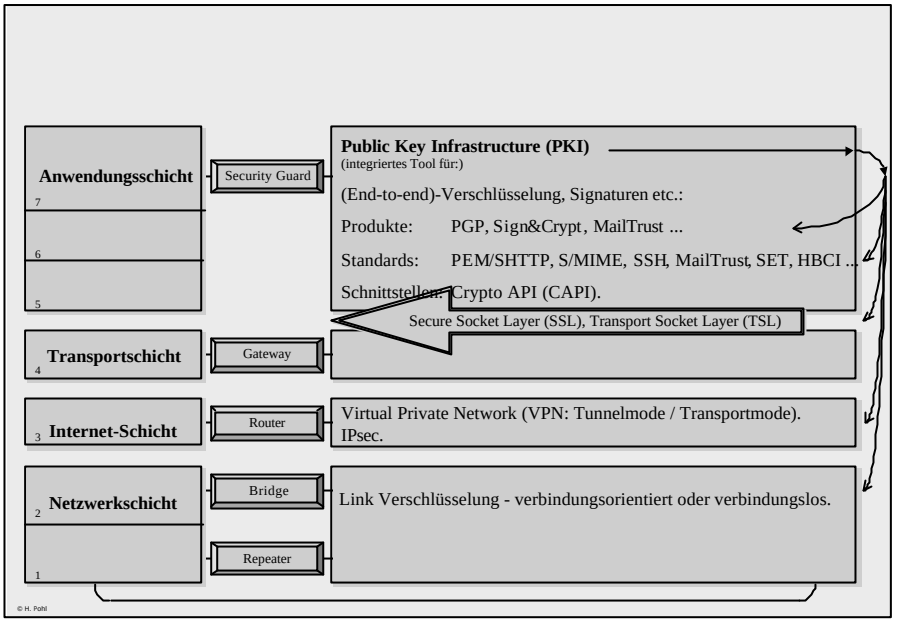

Abbildung 1: Ebenen der Verschlüsselung

Auf dem Markt werden eine Reihe von Produkten angeboten, die IP-Verkehr zwischen zwei Intra- oder Extranets (site-to-site) verschlüsseln können. Es handelt sich dabei häufig um proprietäre Systeme, die nicht mit Systemen anderer Hersteller kompatibel sind und daher nicht mit diesen kommunizieren können. Beim Einsatz proprietärer Systeme müssen beide Unternehmen das Produkt desselben Herstellers verwenden, anderenfalls ist eine (vertrauenswürdige) Kommunikation nicht möglich.

Der Begriff Virtual Private Network wird umgangssprachlich vielfältig benutzt mit völlig unterschiedlichen Bedeutungen.

Vorgestellt wird ein Test der Sicherheitseigenschaften von VPN-Produkten auf IPsec-Basis. Anderweitige – insbesondere Management- und Performance-Aspekte überprüfende Tests – sind veröffentlicht [Kesd99, Schü99].

Einige Hersteller benutzen den Begriff für jede Verbindung zwischen Clients oder Servern eines Unternehmens. Weiterhin benutzen Hersteller den Begriff als Oberbegriff für jegliche Verschlüsselung unabhängig von der ISO-Ebene. Unter dem Schlagwort VPN werden daher auch Produkte angeboten, die auf den Ebenen 2 bis 7 arbeiten. Vergl. hierzu die Abbildung 'Ebenen der Verschlüsselung'.

Im Rahmen dieser Ausarbeitung soll die folgende Definition von Virtual Private Network benutzt werden [Pohl99b]:

> *Ein Netzwerk wird physisch innerhalb eines (anderen) Netzwerks (meist offenen, öffentlichen Netzwerks - Internet) betrieben - (aber) logisch getrennt. Die (logische) Trennung wird (allein) durch Verschlüsselung der Kommunikation auf Ebene 3 des ISO-7-Schichten Modells erreicht und ist damit anwender- und anwendungsunabhängig.*

Die grundlegenden Mechanismen eines VPN werden im IPsec-Standard [Doro00, Kent98c, Smit98] definiert.

3. IPsec als Basistechnologie

3.1 Sachziele

Virtual Private Networks müssen mindestens folgende Sachziele der Informationssicherheit erfüllen :

Vertraulichkeit: Eigenschaft eines Systems der IV, nur berechtigten Subjekten bestimmte Objekte verfügbar zu machen und unberechtigten Subjekten den Zugriff auf Objekte zu verwehren.

Integrität: Eigenschaft eines Systems der IV, bei dem die Korrektheit der Objekte (Daten

auf dem aktuellen Stand) und die korrekte Verfügbarkeit des Systems sichergestellt ist.

Verbindlichkeit: Eigenschaft elektronischer Kommunikation oder Transaktion, rechtsverbindlich zu sein: Authentisch (Sender) und vom Empfänger nicht-rückweisbar (non-repudiation).

Verfügbarkeit: Wahrscheinlichkeit, ein System zu einem vorgegebenen Zeitpunkt, in einem funktionsfähigen Zustand anzutreffen [DIN 40042].

3.2 Der IPsec-Standard

Der Begriff IPsec bezeichnet eine Menge von offenen Standards [Kent98a], die von der Internet Engineering Task Force (IETF) vorgelegt wurden. IPsec (IP security) bietet Vertraulichkeit, Integrität und Authentizität bei der Kommunikation über das (ungesicherte) Internet. IPsec arbeitet auf der IP-Ebene (Schicht 3 im OSI-Modell, Internetschicht) und sichert, unabhängig von der jeweiligen Anwendung, Kommunikation im Internet mit Verschlüsselung und digitalen Signaturen vertrauenswürdig ab.

Der Standard wird fortentwickelt - u.a. auch durch Funktionen zum Key Recovery [Pohl98, Pohl99a, Mark00, Bale00].

Verschlüsselungsalgorithmen werden heutzutage (bei angemessen großer Schlüssellänge von mind. 128 Bit bei symmetrischen Verfahren) als hinreichend widerstandsfähig angesehen. Auch können Veränderungen an den übertragenen Daten erkannt werden (Integritätsprüfung). IPsec-Implementierungen bieten die freie Wahl zwischen Algorithmen wie Triple DES, IDEA, BLOWFISH etc. Parameter wie Schlüssellänge usw. sind frei einstellbar. Dies gilt auch für verwendete Hash-Algorithmen zur digitalen Signatur wie MD5 und SHA1.

Wichtig ist die Adaptierbarkeit von IPsec. Je nach gefordertem Sicherheitsniveau können Authentifikations- und Konzelationsalgorithmen in frei wählbaren Kombinationen eingesetzt werden. Wenn Schwachstellen in einem Algorithmus bekannt werden, kann er gegen einen anderen ersetzt werden.

3.3 IPsec-Modi

IPsec bietet zwei Übertragungsmodi: Transport-Mode und Tunnel-Mode.

Im **Transport-Mode** werden die realen IP-Adressen verwendet. Der AH- bzw. ESP-Header wird zwischen den IP-Header und die übrigen Header bzw. Daten eingefügt.

Bei Verwendung des **Tunnel-Mode** ist es möglich, innerhalb der IPsec-Verbindung private IP-Adressen zu verwenden, beispielsweise für ein VPN. Mit dem Tunnel-Mode läßt sich - im Gegensatz zum Transport-Mode - eine Verkehrsanalyse insofern verhindern, als die IP-Adresse des Endanwenders nicht erkennbar ist sondern lediglich der (zusätzlich eingefügte) Tunnel-IP-Header.

3.4 IPsec-Protokolle

IPsec beinhaltet zwei Protokolle, die spezifische Aufgaben erfüllen.

Das **AH-Protokoll (Authentication Header)** bietet die Möglichkeit, IP-Pakete vollständig mit einer digitalen Signatur zu versehen, um die Authentizität und Integrität überprüfen zu können. Dazu werden Hash-Algorithmen wie MD5 oder SHA1 eingesetzt.

Das **ESP-Protokoll (Encapsulating Security Payload)** bietet die Möglichkeit, IP-Pakete vollständig mit einer digitalen Signatur zu versehen, um die Authentizität und Integrität überprüfen zu können. Der IP-Header wird dabei nicht mit in die Authentifikation einbezogen.

Die Nutzdaten des IP-Paketes können darüber hinaus verschlüsselt werden. Der eingesetzte Algorithmus (z.B. DES, Triple DES, IDEA, CAST) kann ausgewählt werden und ist in IPsec nicht festgelegt.

ESP und AH sind IP-Protokolle auf der OSI-Ebene 3. Der Aufbau eines AH-Pakets ist in RFC 2402 [Kent98b], der eines ESP-Pakets in RFC 2406 [Kent98c] beschrieben.

3.5 Security Association (SA)

Eine SA ist eine einfache uni-direktionale „Verbindung“, die Sicherheitsdienste für eine Datenübertragung bietet. Ein Sender benötigt für jeden Kommunikationspartner eine eigene SA. Die beiden an der Kommunikation beteiligten IV-Systeme speichern in der SA die IP-Adresse, den Mode, das Protokoll, die Algorithmen und die benutzten Schlüssel. Da eine SA nur für eine Kommunikationsrichtung benutzt wird, sind für eine bi-direktionale Kommunikation zwei SA notwendig. Jede SA kann jeweils nur einen Mode und ein Protokoll beinhalten. Wenn verschiedene Modi oder Protokolle (z.B. AH und ESP für ein Paket) eingesetzt werden sollen, sind auch verschiedene SA notwendig.

Zur eindeutigen Identifizierung der SA beim Empfänger des IP-Pakets wird der Security Parameter Index (SPI) eingesetzt. Der SPI ist ein 32-Bit langer String, der in jedem AH- bzw. ESP-Header enthalten ist.

3.6 Security Policy Database (SPD)

In der Security Policy Database wird spezifiziert, welche SA benutzt wird. Für jedes gesendete bzw. empfangene Paket liefert die SPD Informationen über dessen Behandlung. Die SPD kann 3 Verarbeitungsarten unterscheiden:

- Verwerfen des Pakets.
- Keine IPsec-Verarbeitung.
- IPsec-Verarbeitung.

Die SPD besitzt sehr flexible und fein abgestufte Mechanismen, die eine stark graduierte Behandlung für jedes einzelne Paket erlauben.

3.7 ISAKMP

ISAKMP (Internet Security Association and Key Protocol Management) definiert die grundlegende Struktur der Protokolle, die für die Einrichtung der SAs und zur Durchführung anderer Key Management Funktionen benötigt werden. ISAKMP unterstützt verschiedene Domains of Interpretation (DOI), wovon eine die IPsec-DOI ist. ISAKMP spezifiziert nicht die gesamten Protokolle, aber es unterstützt den Aufbau von Blöcken für die verschiedenen DOIs und Key-Exchange Protokolle.

3.8 Internet Key Exchange (IKE)

IKE hat drei Funktionen: Die Authentifizierung der Gegenstelle, das Aushandeln eines Verschlüsselungsverfahrens, um alle IKE-Transaktionen zu verschlüsseln und schließlich das Aushandeln der SA für IPsec. Die dazu ausgetauschten Pakete haben eine spezifische Struktur; die gesendeten Informationen werden in inhaltlich zusammengehörende sogenannte Payloads aufgeteilt, mit einem Header versehen und aneinander gefügt. In bestimmten Abständen werden dabei (pseudo-)zufällige Daten eingefügt, damit jede Transaktion einmalig ist. Dieses Verfahren erschwert Replay- und Known-Plaintext-Attacken.

IKE ist das Standard (und im Moment das einzige) Key-Exchange Protokoll für ISAKMP. IKE baut auf ISAKMP auf und dient zum Einrichten einer dynamischen SA. Es benutzt das UDP-Protokoll und übernimmt die Verwaltung der Schlüssel für die IPsec-Verbindungen. Über das IKE-Protokoll werden die Kommunikationspartner erstmalig authentifiziert, die SA ausgehandelt und anschließend die zu verwendenden Schlüssel ausgetauscht.

Das IKE-Protokoll verschlüsselt die Übertragung aller Informationen. Dafür können (noch) keine IPsec-Protokolle eingesetzt werden, da zu diesem Zeitpunkt ja erst eine SA für IPsec ausgehandelt werden muss.

Da Verschlüsselungsalgorithmen weiterentwickelt werden und die Anforderungen an die verwendeten Parameter - wie zum Beispiel die Schlüssellänge - steigen dürften, wurde beim Entwurf des IKE-Protokolls [Hark98] auf Flexibilität geachtet. So können Kommunikationspartner einen Algorithmus aushandeln. Dazu werden verschiedene Möglichkeiten angeboten, geprüft und ggf. auch wieder verworfen. Üblicherweise macht der Initiator einer IPsec-Verbindung bzw. eines IKE-Schlüsselaustauschs (Sender) mehrere Vorschläge, aus denen sich dann der Empfänger einen Algorithmus aussuchen kann. So könnte zum Beispiel der Sender die Algo-

rithmen DES mit 56 Bit Schlüssellänge sowie Triple DES mit 128 Bit Schlüssellänge vorschlagen, von denen der Empfänger dann Triple DES akzeptieren könnte. Auch das IKE-Protokoll ist um neue und weitere Algorithmen erweiterbar.

Arbeitsweise des IKE-Protokolls

Das IKE-Protokoll arbeitet in zwei Phasen [Lab98]:

- Die erste Phase dient dazu, eine verschlüsselte Verbindung zwischen (zwei) IKE-Instanzen herzustellen und beide Teilnehmer zu authentifizieren. Dabei wird eine SA für das IKE-Protokoll selbst erstellt.
- In der zweiten Phase werden die SA's zur Verwendung für IPsec ausgehandelt.

Für die Phasen sind jeweils bestimmte Transaktionen (Exchange Types) definiert, die den Aufbau der IKE-Pakete festlegen. Für den Aufbau der SA in Phase I existieren zwei Arten: Main Mode und Aggressive Mode. Beide erreichen dasselbe Ziel, nämlich das Aushandeln einer SA für die weitere IKE-Kommunikation. Der Aggressive Mode kann schneller abgehandelt werden, er verzichtet jedoch auf die Identitätsprüfung der beiden Teilnehmer. Der Quick Mode wird in Phase II benutzt und dient zum Aufbau der SA's für IPsec. Er kann, wie der Name impliziert, schnell abgehandelt werden, nachdem die Phase I abgeschlossen ist. Zusätzlich existiert noch ein New Group Mode, der in Phase II benutzt werden kann, um neue Parameter für das Diffie-Hellman-Verfahren festzulegen.

Main Mode

Im Main Mode wird in den ersten beiden Paketen der Verschlüsselungsalgorithmus festgelegt. Die nächsten beiden Pakete führen einen Schlüsselaustausch nach dem Diffie-Hellman-Verfahren durch. Die letzten beiden Pakete dienen zur Authentifizierung der beiden Teilnehmer.

Quick Mode

Im Quick Mode werden SAs zur Benutzung für IPsec ausgehandelt. Dazu werden die Angaben der gewünschten Algorithmen übertragen. Der zu verwendende Schlüssel wird nicht übertragen, sondern aus einem Hash-Wert über Teile des Pakets berechnet. Ein drittes IKE-Paket, welches einen Hash-Wert enthält, der aus den vorherigen Paketen berechnet wurde, dient zum Schutz gegen Replay-Attacken.

3.9 Bewertungsansatz

IPsec ist ein Protokoll, durch dessen Einsatz die Kompatibilität mit IPsec-Produkten anderer Hersteller gewährleistet werden kann.

IPsec beinhaltet viele Optionen und eine hohe Flexibilität, die vom Anwender nicht immer vollständig ausgenutzt werden kann. Einige wesentliche Kritikpunkte am derzeitigen IPsec-Standard sollen nachfolgend kurz genannt werden. Eine ausführliche Beschreibung liefert [Ferg99].

Komplexität

IPsec wurde entwickelt, um verschiedene Kommunikationssituationen mit einer Vielzahl verschiedener Optionen zu unterstützen. Das daraus resultierende System hat einen Grad an Komplexität erreicht, der mit den vorhandenen Methoden nur aufwendig analysiert und implementiert werden kann.

Dokumentation

Die Dokumentation zu IPsec ist nur für einen vollständig informierten Leser verständlich; sie beinhaltet weder eine Einführung noch einen Überblick.

Auch sind die Ziele, die durch den Einsatz von IPsec erreicht werden sollen, nicht definiert. Dadurch wird der Einsatz von IPsec sowohl bei der Implementierung als auch bei der Konfiguration erschwert.

Tunnel- und Transport-Mode

Der Tunnel-Mode stellt eine Erweiterung des Transport-Mode dar. Der einzige Vorteil des Transport-Mode ist die geringere benötigte Bandbreite und der geringere Overhead. Durch den Einsatz eines Kompressionsalgorithmus für die Header-Daten können auch im Tunnel-Mode die gleichen Performancewerte erreicht werden wie im Transport-Mode. Dadurch entfällt die Notwendigkeit, einen zweiten Mode einzusetzen, der keine funktionale Erweiterung bei der Implementierung und Konfiguration bringt.

AH-Protokoll

Die Funktionalitäten des AH- und des ESP-Protokolls überlappen sich teilweise. AH unterstützt die Authentifikation des Payload und des IP-Paket-Header. Da sich aber einige Teile des IP-Header während des Routing ändern, müssen diese Felder ausgespart bleiben. Es ist also notwendig, dass das AH-Protokoll die komplexe Definition des IP-Header kennt und entsprechend einbindet. Diese Komplexität könnte sicherheitsrelevante Probleme aufwerfen und verstößt gegen den modularen Aufbau des Protokoll-Stack.

Durch einen alleinigen Einsatz des Tunnel-Mode kann das ESP-Protokoll eine gleich starke Authentifizierung wie das AH-Protokoll leisten. Die vollständig authentifizierte Payload eines ESP-Tunnel-Pakets enthält sowohl den Original-IP-Header als auch die Nutzdaten und bietet damit die gleiche Leistung wie das AH-Protokoll im Transport-Mode. Ein Einsatz des AH-Protokolls ist daher nicht notwendig.

Anpassung ESP-Protokoll

Im ESP-Protokoll sind Verschlüsselung und Authentifizierung optional. Ohne die Funktionalität von IPsec zu verringern, könnte durch den Einsatz des mit integrierter Authentifizierung versehenen ESP-Protokolls im Tunnel-Mode eine Vereinfachung erreicht werden. Die Nutzung des AH-Protokolls, welches aufgrund der notwendigen Kenntnis des IP-Header-Aufbaus eine hohe Implementierungskomplexität aufweist, könnte dadurch vermieden werden.

Fragmentierung

IPsec interagiert mit dem Fragmentierungssystem des IP-Protokolls. Fragmentierung ist ein Teil der Internetschicht und sollte für IPsec transparent sein. Aus Kompatibilitätsgründen mit existierenden Protokollen (TCP) ist diese Interaktion jedoch notwendig. Durch die zusätzliche Funktionalität wird Komplexität des Programms erhöht und damit sowohl die Implementierung als auch die Überprüfung des Programms erschwert – das Sicherheitsniveau sinkt.

Reihenfolge der Operationen

Wenn sowohl Authentifizierung als auch Verschlüsselung unterstützt werden, führt IPsec zuerst die Verschlüsselung und danach die Authentifikation des Schlüsseltextes durch.

Nach dem „Horton Prinzip“ [Wag96] soll das Protokoll authentifizieren, was gemeint ist. Das bedeutet, daß die Authentifikation für den Klartext erfolgen sollte, nicht für den Schlüsseltext. Diese Vorgehensweise wäre einfacher und robuster. Dadurch wäre es z.B. möglich, die Auswirkungen spezieller Angriffe auf die SA´s während des IKE-Protokolls zu erkennen.

Security Association

Der Einsatz von zwei Protokollen (AH und ESP) und zwei Modi (Transport- und Tunnel-Mode) macht die SA komplexer. Selten wird eine uni-direktionale Kommunikation zwischen Rechnern stattfinden. Eine Zusammenfassung der einzelnen SA zu einer SA für eine bi-direktionale Kommunikation wäre möglich. Auch ist eine asymmetrische Sicherheitskonfiguration[4] im realen Einsatz eher unerwünscht, da sie das Sicherheitsniveau nicht erhöhen, sondern nur verringern kann.

Security Policy Database

Jedes Paket kann anhand einer Vielzahl von Parametern speziell verarbeitet werden. Die Viel-

---

[4] Für die Kommunikation von A nach B werden andere Algorithmen eingesetzt als für die Kommunikation von B nach A.

zahl an Entscheidungsmöglichkeiten kann den Anwender bzw. Administrator überfordern und Sicherheitslöcher entstehen lassen.

Die SPD sollte ausschließlich angeben, welche Pakete authentifiziert, sowohl authentifiziert als auch verschlüsselt oder gar nicht von IPsec behandelt werden. Die Implementierung muss gewährleisten, dass für *alle* eingesetzten Algorithmen in jeder Situation ein adäquates Sicherheitsniveau erreicht wird. Dies ist durch eine Beschränkung auf wenige gute kryptographische Algorithmen möglich; es ist nicht erforderlich, unsichere oder schlechte Algorithmen zu verwenden [Ferg99].

4. Produkttest VPN-Software

Von November 1999 bis Januar 2000 wurde ein Produkttest von 8 VPN-Softwareprodukten in Kooperation mit einem industriellen Anwender und einer Unternehmensberatung für EDV-Sicherheit durch-geführt. Der Test wurde reproduzierbar dokumentiert mit den Testverfahren, den benutzten Testdaten, den eingesetzten Tools, der benutzte Konfiguration und allen Abläufen, so dass er jederzeit wiederholbar ist.

Zugrunde liegt ein kooperatives Vorgehensmodell [Les00b]. Darin werden in der ersten sog. Test- und Evaluierungsphase ausgewählte Produkte eines Typs anhand von an der Hochschule entwickelter und mit den Partnern abgestimmter Bewertungsparameter unabhängig bewertet. In der zweiten Phase – der sog. Referenzierungsphase – wurden die priorisierten Produkte in der Hochschule anhand unternehmensspezifischer Parameter und hinsichtlich ihrer Einpassbarkeit in die Arbeitsumgebung des Unternehmens einer zweiten Bewertung unterzogen. In der dritten sog. Roll-out-Phase wird das anwendende Unternehmen bei dem flächendeckenden Roll-out nur noch in grundsätzlicher Weise bei der Aufbereitung von Betriebshandbüchern und Schulungsunterlagen sowie ggf. der Schulung von Ausbildern (Multiplikatoren) unterstützt.

Der Gesamtaufwand für die Testphase sowie die Verifizierung der Testergebnisse in der Evaluierungsphase durch eine zweite Gruppe betrug 200 Manntage.

4.1 Verfahrensfestlegung

Der VPN-Produkttest gliederte sich in drei Hauptteile.

4.1.1 Vorauswahl

In dieser ersten Phase wurden verfügbare Informationen über Produkte des Typs Virtual Private Network gesammelt.

Die folgenden Kriterien wurden in der Vorauswahl als wesentlich für die **Produktabgrenzung** angesehen [Schl00a]:

- Selbständiges Produkt ohne Einbindung in anderweitige Funktionen wie z.B. Firewall etc, die die Komplexität erhöhen und damit das Sicherheitsniveau senken würde.
- Verschlüsselung auf IP-Ebene.
- Unterstützung mindestens des Transport-, möglichst des Tunnel-Modus.
- Unterstützung eines Site-to-Site[5] VPN.
- Transparenter Einsatz für den Endanwender.

Diese Produktabgrenzung wurde anhand öffentlich zugänglicher Quellen (überwiegend Internet) durchgeführt. Da in diesen Quellen häufig keine (bzw. nur im geringen Umfang) technische Details genannt werden, war eine eingehende Beurteilung schwierig.

Eine ganze Reihe von Produkten erfüllten die o.g. Kriterien nicht und wurden daher bei den weiteren Untersuchungen nicht berücksichtigt.

Für den Test haben sich folgende 8 Produkte qualifiziert[6]:

---

[5] VPN-Verbindung zweier Intranets. Die VPN-Funktionen werden allein durch VPN-Gateways an den Schnittstellen der Intranets erbracht. Innerhalb der Intranets ist keine VPN-Funktionalität vorhanden.

Hersteller [7]	Produkt	Version
Cisco	Cisco 2600 (Hardware-Router)	IK2S-N - 12.0(7)T
Genua	GenuCrypt	1.0
Linux	FreeS/WAN	1.2
NAI	GVPN	5.x
Norman Data Defense	Security Server	3.2
Novell	Bordermanager VPN Service	3.00
Siemens	TranSON	1.x
Utimaco	SafeGuard VPN	2.3

Tabelle 1: Getestete VPN-Produkte und Hersteller

An die Vorauswahl schloß sich die Beschaffung der Testprodukte an. Es wurden nur reguläre Verkaufsversionen beschafft (Produkte - keine Beta-Versionen o.ä.). Von zwei Herstellern wurde auch Hardware bereitgestellt.

4.1.2 Dokumentenanalyse

Nach der Beschaffung der Testprodukte erfolgte die Dokumentenanalyse. Diese bezieht sich auf die mitgelieferte Produktdokumentation.

Für die Analyse wurde ein vorgegebener Produktbogen ausgefüllt, in dem alle relevanten Daten erfaßt werden konnten. Dieser Produktbogen ermöglicht einen direkten Vergleich zwischen den verschiedenen Produkten.

Auszugsweise sind die Hauptparameter[8] [Pohl99b] in der nachfolgenden Tabelle aufgeführt:

Produktbeschreibung
Systemanforderungen
Qualität der Mechanismen
Verschlüsselung
Digitale Signatur
Zertifikate
Qualität der Implementierung
Klartextverarbeitung
Schlüsseltextverarbeitung
Trennung der Datenströme
Selbstschutz
Key Management
Schlüsselgenerierung
Zufallszahlengenerator
Schlüsselversorgung
Schlüsselwechsel

---

6 Die Zahl der Produkte wurde wegen der begrenzten Ressourcen und in Abstimmung mit dem industriellen Partner begrenzt.

7 Die Liste ist in alphabetischer Reihenfolge der Herstellernamen aufgeführt.

8 Insgesamt wurden 98 Parameter je Produkt ausgewertet.

Backup, Archivierung, Recovery
Funktionalitäten
Normenkonformität
Benutzerfreundlichkeit
Investitionssicherheit
Aufwand

Tabelle 2: Bewertungsparameter für VPN-Produkte (Auszug)

Nach Abschluss der Dokumentenanalyse wurde ein Abgleich mit den vorher definierten **KO-Kriterien** [Pohl99b] vorgenommen:

- Ansprechpartner in physischer Nähe (Deutschland/Europa): Pflege, Wartung, Beratung.
- Veröffentlichte Algorithmen zur Konzelation und für die digitale Signatur.
- Schlüssellänge = 128 Bit symmetrisch, =1024 Bit asymmetrisch.
- Konformität mit IPsec-Standard.

Der Test eines Produktes wurde nur weitergeführt, sofern es **alle** KO-Kriterien erfüllt. Falls zu einem KO-Kriterium durch alleinige Dokumentenanalyse keine abschließende Aussage getroffen werden konnte, wurde gleichwohl ein Maschinentest durchgeführt.

Im Rahmen des Produkttests wurden folgende Betrachtungen **nicht** durchgeführt :

- Sicherheit des zugrundeliegenden Betriebssystems.
- Netzwerksicherheit der Schnittstellen zum Betriebssystem.
- Integration der Produkte in das Betriebssystemumfeld.
- Source-Code-Analyse.

4.1.3 Maschinentest

Alle Produkte, die sich nach der Dokumentenanalyse für den praktischen Test qualifiziert hatten, wurden dem nachfolgend dargestellten Testverfahren [Schl00b] unterzogen. Dazu wurde ein – ein Site-to-Site VPN simulierendes – Testszenario formuliert und installiert.

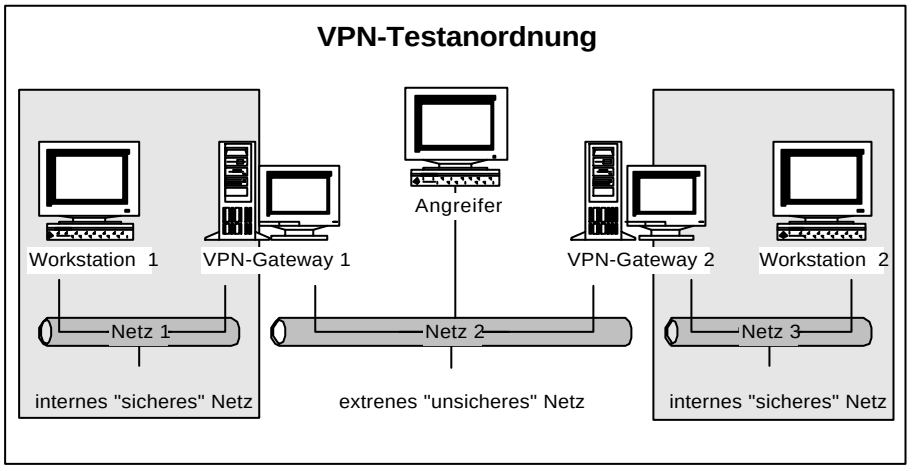

Abbildung 2: Testszenario VPN-Test

Der Datenverkehr zwischen den Netzen 1 und 3 erfolgt verschlüsselt. Das gesamte VPN-Aufgabenspektrum, welches dabei zu leisten war (Identifizierung, Authentifizierung, Verschlüsselung), war allein durch die Gateway-Rechner zu bewältigen.

Installations- und Konfigurationstest

Mit diesem Test wurden der personelle und zeitliche Aufwand für die Installation und die Konfiguration eines jeden Produkts überprüft.

Die Qualität des angebotenen Supports (wie Hilfedateien, Produktdokumentation und Hotline)

wurde anhand von real auftretenden Problemen bestimmt.

Sicherheitstest
Dieser Test liefert Aussagen über die Qualität der sicherheitsrelevanten Funktionen der Produkte:

- Unumgehbarkeit der sicherheitsrelevanten Funktionen.
- Kenntlichmachung von Änderungen wie Manipulationen an empfangenen Daten.
- Kenntlichmachung von Änderungen wie Manipulationen am Produkt.
- Visualisierung des Verschlüsselungsstatus.

Test-Angriffe
Hierbei wurde durch bekannte Angriffe [Rusc99] überprüft, ob die Funktion der Software durch Einwirkungen von außen gestört oder verhindert werden kann.

Performance-Test
Der Durchsatz des Systems in unterschiedlichen Konfigurationen (Einsatz verschiedener Verschlüsselungs- und Authentifizierungsverfahren) wurde bei diesem Test untersucht. Dazu wurden zum einen verschiedene, vorgegebene Dateisets [9] über eine FTP-Verbindung übertragen; zum anderen wurde die erreichbare Netzwerk-Performance mit einem Testtool ('Netperf') gemessen.

4.2 Ergebnisbeschreibung

4.2.1 Vorauswahl

Eine Vorauswahl anhand der definierten Mindestfunktionalitäten qualifizierte 8 Produkte für den Test. Aufgrund der begrenzten Ressourcen (Zahl der Mitarbeiter und Gesamtzeit) konnten keine weiteren Produkte, die gleichfalls den Produktabgrenzungskriterien entsprachen, in das Testfeld aufgenommen werden.

Die 8 Produkte wurden von den Herstellern/Lieferanten bereitgestellt. Mit der Begründung der im Testzeitraum geltenden US-amerikanischen Exportrestriktionen wurden 2 Produkte mit starker Verschlüsselung (>= 128 Bit symmetrisch) bis zum Testende nicht geliefert.

4.2.2 Dokumentenanalyse

Die Dokumentenanalyse qualifizierte 4 der 8 betrachteten Produkte für den Maschinentest. Zwei Produkte erfüllten ein bzw. mehrere KO-Kriterien nicht.

Das verdichtete Ergebnis der Dokumentenanalyse ist in der Tabelle 1 dargestellt [Les00a].

Produkt[10]	**KO-Kriterien**	**Max. Schlüssellänge**	**Maschinentest erfolgt**
A [11]	Unveröffentlicht	Unveröffentlicht	nein
B	Unveröffentlicht	Unveröffentlicht	nein

[9] 2 Dateisets mit einer Gesamtgröße von je 3 MB. Das Set „kleine Dateien“ enthielt 1059 Dateien, das Set „große Dateien“ 3 Dateien.

[10] Aufgrund der für den Anwender spezifischen Situation und den darauf abgestellten Bewertungsparametern können die Test- und Evaluierungsergebnisse nicht allgemeingültig sein. Vielmehr müssen die Bewertungsparameter auf die jeweilige spezifische Anwender-Situation angepasst werden. Aus diesem Grunde werden hier auch keine zusammenfassenden Bewertungen genannt.

[11] Das Produkt wurde vom Hersteller nicht bereitgestellt mit der Begründung US-amerikanischer Exportrestriktionen für starke Verschlüsselung

Produkt[10]	KO-Kriterien	Max. Schlüssellänge	Maschinentest erfolgt
C [12]	Min. Schlüssellängen	56 Bit	nein
D	Fehlende IPsec-Konformität	128 Bit	nein
E	Erfüllt	168 Bit	ja
F	Erfüllt	168 Bit	ja
G	Erfüllt	168 Bit	ja
H	Erfüllt	168 Bit	ja

Tabelle 3: Verdichtetes Ergebnis der Dokumentenanalyse

4.2.3 Maschinentest

Installation / Konfiguration

Der Zeitaufwand und das notwendige Vorwissen für die Installation und Konfiguration der VPN-Produkte war produktabhängig sehr unterschiedlich. Ein Produkt mit vorbildlicher Installationsroutine und klarer Konfiguration ermöglichte z.B. die Installation eines voll funktionsfähigen VPN innerhalb von etwa 45 Minuten.

Bei einem anderen Produkt mußten schwer verständliche Konfigurationsdateien manuell angepaßt werden. Dabei wurde durch das Produkt keine Unterstützung für die Überprüfung der gewählten Einstellungen (Korrektheit, Funktionsfähigkeit) gewährt. Durch eine unerkannte Fehlkonfiguration könnte das angestrebte Sicherheitsniveau (z.B. Verschlüsselung mit 128 Bit Schlüsselstärke) stark gesenkt werden.

Performance-Test

Die Ergebnisse der Performance-Tests sind in den Abbildungen 2 - 5 dargestellt. Die Performance-Unterschiede sind z.T. erheblich.

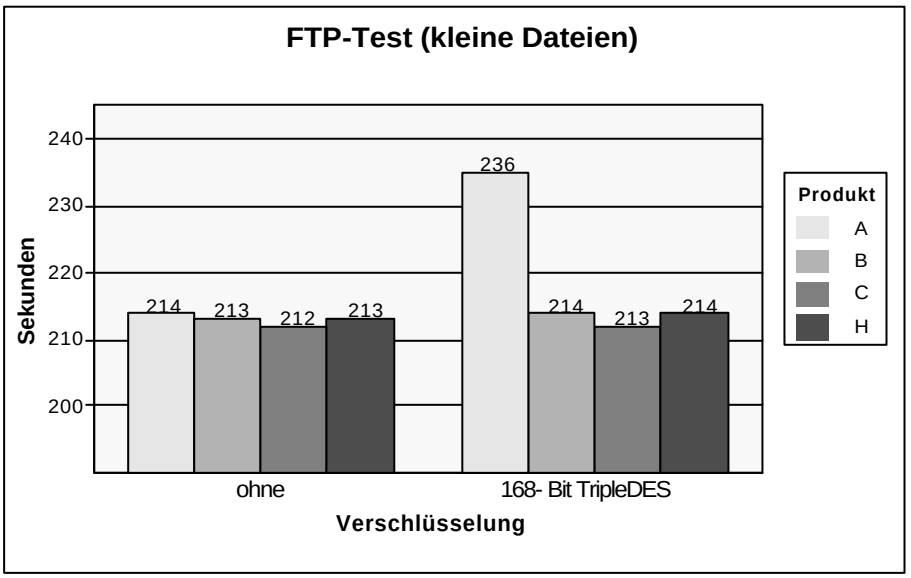

Abbildung 3: Ergebnisse FTP-Test (kleine Dateien)

[12] Das Produkt wurde vom Hersteller nicht bereitgestellt mit der Begründung US-amerikanischer Exportrestriktionen für starke Verschlüsselung. Für die Dokumentenanalyse stand eine Version mit 56 Bit Verschlüsselungsstärke zur Verfügung.

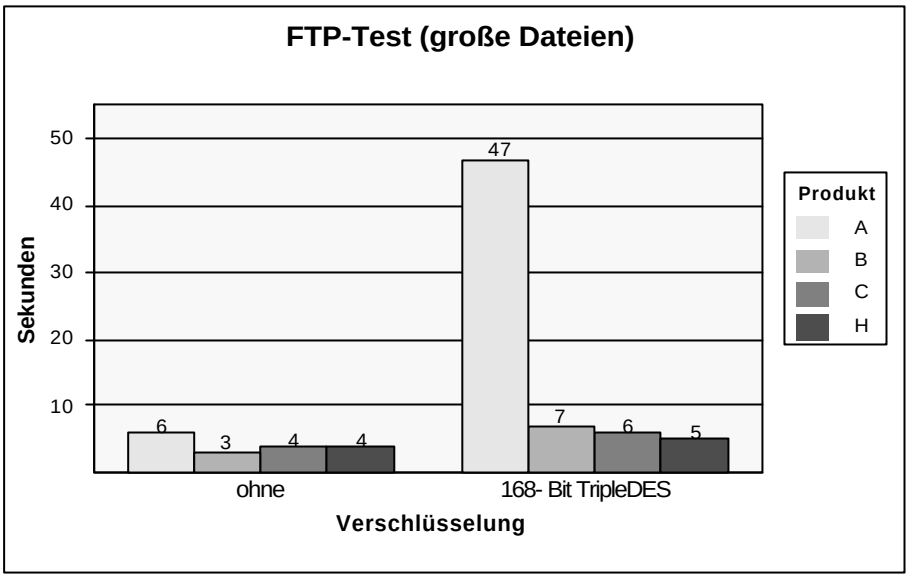

Abbildung 4: Ergebnisse FTP-Test (große Dateien)

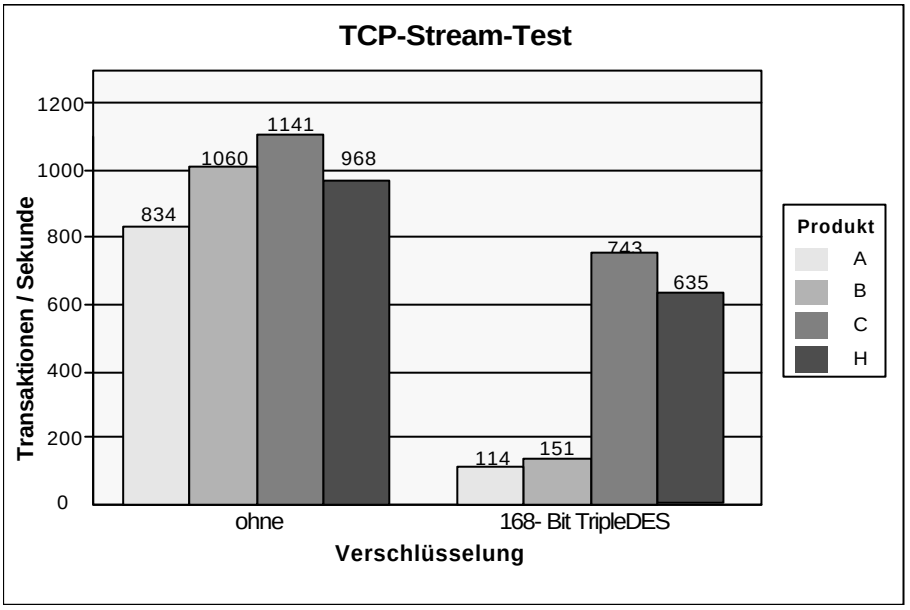

Abbildung 5: Ergebnisse TCP-Stream-Test

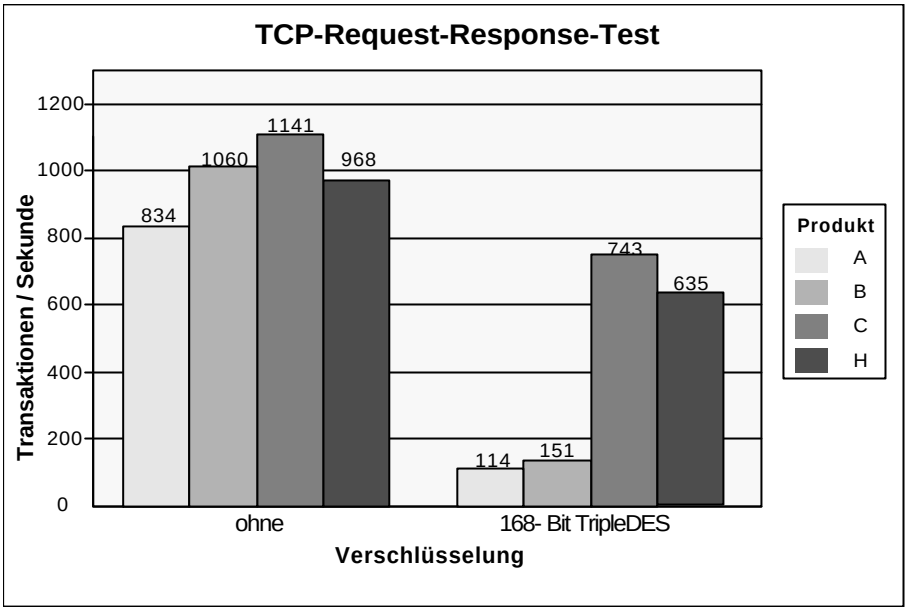

Abbildung 6: Ergebnisse TCP-Request-Response-Test

Sicherheitstest

Fehlender Selbstschutz: Keines der getesteten Produkte konnte Manipulationen an den eigenen Programmdateien erkennen. Die Möglichkeit und der Umfang der Protokollierung durch die Programme war sehr unterschiedlich.

Die Unumgehbarkeit ist bei allen Produkten bei einem korrekt konfigurierten VPN-Gateway und gleichfalls korrekt konfigurierten Netz weitgehend sichergestellt. Da die gesamte Funktionalität durch die VPN-Gateways übernommen wird, bemerkt der Endanwender nichts von deren Arbeit; das VPN ist für ihn vollständig transparent.

Testangriffe

Die durchgeführten Testangriffe waren bis auf eine Ausnahme erfolglos. Die VPN-Gateways ließen sich weder durch Replay-Angriffe während des Schlüsselaustauschs noch während der Datenübertragung stören. Auch die Manipulation von IPsec-Paketen und deren erneutes Senden zeigte keine negative Wirkung. Gleichfalls erfolglos waren Telnet-Angriffe auf die benutzten Ports. Die aufgezeichneten IPsec-Pakete waren verschlüsselt. Details waren nicht erkennbar.

Allein bei einem Produkt war ein Replay-Angriff erfolgreich. Es war möglich, den Schlüsselaustausch zwischen den beiden VPN-Gateways zu jedem beliebigen Zeitpunkt neu anzufordern. Dieser Angriff mit der Folge eines Denial-of-Service kann die VPN-Funktion für ein Zeitintervall [13] unterbinden. Es ist jedoch nicht möglich, die Inhalte der IPsec-Pakete im Klartext zu erkennen.

4.3 Produktempfehlung

Als bestes Produkt schnitt ein aus dem Internet entgeltfrei ladbares ab. Kein anderes der untersuchten Produkte kann uneingeschränkt empfohlen werden. Die Produkte weisen sowohl positive als auch negative Eigenschaften auf. Das zweitplazierte weist die geschilderte Schwäche gegenüber Replay-Angriffen auf, die allerdings mit einem Manpower-Aufwand von etwa 4 Mannwochen behoben werden kann. Das drittplazierte Produkt wies bei verschlüsseltem Betrieb eine Performance-Einbuße auf 1/10 auf, die sich durch die Beschaffung hochperformanter Hardware ausgleichen läßt.

Über die Unternehmensentscheidung und über Erfahrungen des Auftraggebers (Anwenders) sowie die Abschlußtests mit dem vom Anwender ausgewählten Produkt in der Arbeitsumgebung des Anwenders [Schl00c] wird berichtet [Nüh00].

---

[13] Die Zeitspanne ist abhängig von der Konfiguration des VPN-Gateways und der Frequenz, mit der die Replay-Pakete gesendet werden.

5. Literatur

[Bale00] Balenson, D.; Markham, T.: ISAKMP Key Recovery Extensions. Computers & Security. 19, 1, 91 - 99, 2000.

[Doro00] Doraswamy, N.; Harkins, D.: IPsec. Der neue Sicherheitsstandard für das Internet, Intranets und virtuelle private Netze. München 2000.

[Ferg99] Ferguson, N.; Schneier B.: A Cryptographic Evaluation of IPsec. www.counterpane.com. San Jose 1999.

[Hark98] Harkins, D.; Carrel D.: RFC 2409. The Internet Key Exchange (IKE). http://www.rfc-editor.org. 1998.

[Kent98a] Kent, S.; Atkinson, R.: RFC 2401. Security Architecture for the Internet Protocol. http://www.rfc-editor.org. 1998.

[Kent98b] Kent, S.; Atkinson, R.: RFC 2402. IP Authentication Header (AH). http://www.rfc-editor.org. 1998.

[Kent98c] Kent, S.; Atkinson, R.: RFC 2406 - IP Encapsulating Security Payload (ESP). http://www.rfc-editor.org. 1998.

[Kesd99] Kesdogan, D.; Schäffter, M.: Übersicht und Bewertung von VPN-Produktlösungen. In: DFN-CERT GmbH & DFN-PCA (Hrsg.): 7. Workshop Sicherheit in vernetzten Systemen. Hamburg 2000.

[Lab98] Labouret, G.; Schauer, H.: IPsec – a technical overview. http://www.hsc.fr/ressources/veille/ipsec/papier/papier.html.en. 1998.

[Les00a] Lessing & Partner (Hrsg.): Abschlußbericht Produkttest Virtual Private Networks. Jülich 2000 (unveröffentlichter Bericht).

[Les00b] Lessing, G.: Zum Kooperationsmodell Wissenschaft – Wirtschaft: Evaluierung und Referenzierung im Labor für Informationssicherheit, Roll-out im Unternehmen. In: Pohl, H.; Lessing, G.: Informationssicherheit mit Virtual Private Networks (VPN). Jülich/St. Augustin 2000 (unveröffentlichter Bericht).

[Mark00] Markham, T; Williams, C.: Key Recovery Header for IPsec. Computers & Security. 19, 1, 86 - 90, 2000.

[Nüh00] Nühnen, A.: Erfahrungen eines Anwenders mit der Produkt-Evaluierung und Referenzierung im Labor für Informationssicherheit. In: Pohl, H.; Lessing, G.: Informationssicherheit mit Virtual Private Networks (VPN). Jülich/St. Augustin 2000 (unveröffentlichter Bericht).

[Pohl98] Pohl, H.; Cerny, D.: Unternehmensinterne Schlüssel-Archive (Key Recovery Center). Wirtschaftsinformatik 40, 5, 443 – 446, 1998.

[Pohl99a] Pohl, H.; Cerny, D.: Enterprise Key Recovery – Vertrauenswürdige Server mit skalierbarer Sicherheit zur Archivierung von Konzelationsschlüsseln. Informatik Spektrum 22, 2, 110 – 121, 1999.

[Pohl99b] Pohl, H.: Auswahl von Virtual Private Networks (VPN). Köln/St. Augustin, 1999 (unveröffentlichter Bericht).

[Rusc99] Rusche, T.: Sichere Datenübertragung über das Internet mittels IPsec. Studienarbeit. Hamburg 1999

[Schl00a] Schlichting, J.; Hartmann, J.; Pohl, H.: Produkttest Virtual Private Networks. Sankt Augustin 2000 (unveröffentlichter Bericht).

[Schl00b] Schlichting, J.; Pohl, H.: Evaluierungsprojekt Virtual Private Networks (VPN). Standard-Konformität, Leistungen und Schwachstellen. In: Pohl, H.; Lessing, G.: Informationssicherheit mit Virtual Private Networks (VPN). Jülich/St. Augustin 2000 (unveröffentlichter Bericht).

[Schl00c] Schlichting, J.; Pohl, H.: Referenzmodell Virtual Private Networks. Sankt Augustin,

Jülich, Köln 2000 (unveröffentlichter Abschlußbericht).

[Schü99] Schüßler, I.; Ungerer, B.: Verschlußsache. Kosten sparen mit Virtual Private Networks. IX 2, 114 – 119, 1999

[Smit98] Smith, R. E.: Internet-Kryptographie. München 1998.

[Wag96] Wagner, D; Schneier, B.: Analysis of the SSL 3.0 Protocol, The Second USENIX Workshop on Electronic Commerce Proceedings. 1996.