

4. Sicherheitsmechanismen in Netzen

4.1. Einführung

Um die eigene Sicherheitssituation zu bewerten, ist die Beantwortung der folgenden Fragen ratsam:

1. Welche Objekte müssen geschützt werden?
2. Wovor müssen die Objekte geschützt werden?
3. Wer sind die potentiellen Angreifer?
4. Mit welchen Mitteln erfolgen die Angriffe?
5. Wie groß ist der Aufwand für den Angriff?
6. Wie hoch ist das Risiko des Erkanntwerdens für den Angreifer?
7. Wie groß ist der Nutzen für den Angreifer?
8. Wie hoch ist der mögliche Schaden?
9. Gibt es spezielle Bedrohungen?

Bild 4-1 [RUL93] gibt Auskunft über die Bedrohungsvielfalt.

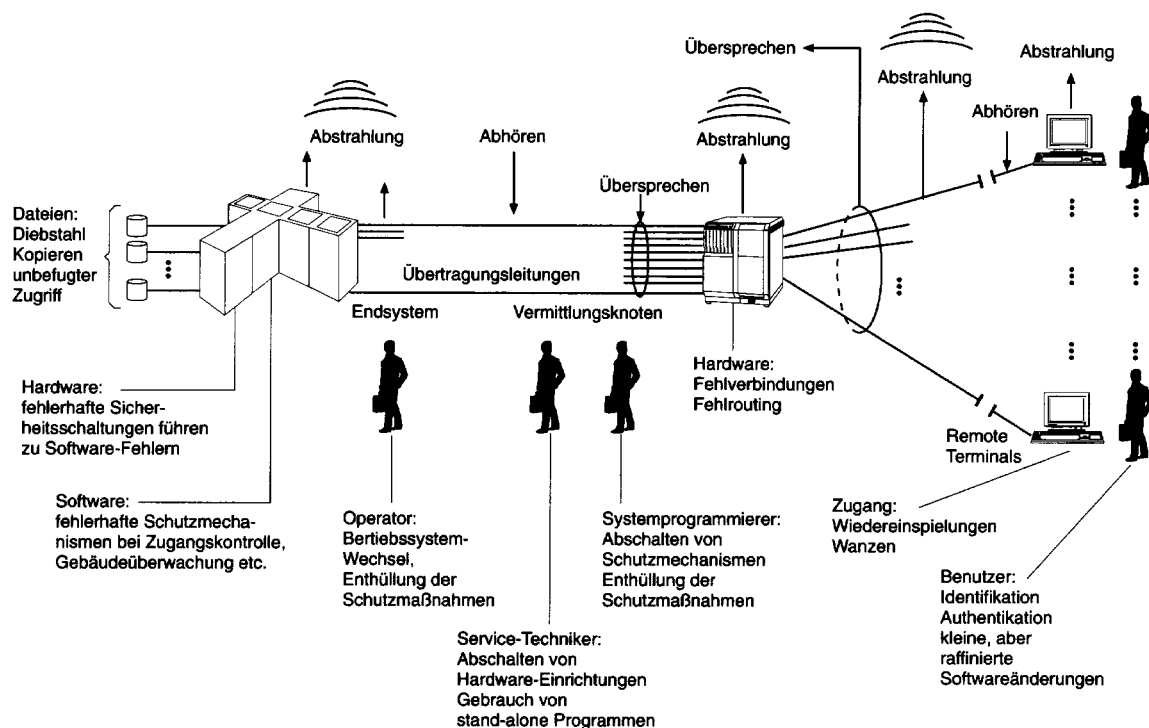


Bild 4-1 : Bedrohungsvielfalt

Klassifizierung der Sicherheit von Informationssystemen

Um die Sicherheit von Informationssystemen objektiv und nach einheitlichen Kriterien beurteilen zu können, wurden nationale und internationale Richtlinien geschaffen.

Der erste bedeutende Klassifizierungskatalog war das „Orange Book“, auch TCSEC (Trusted Computer System Evaluation Criteria) genannt, herausgegeben vom amerikanischen Verteidigungssystem im Jahre 1983 [DOD85]. Darin werden IT-Systeme in sieben Sicherheitsstufen eingeteilt.

Der für Europa relevante Klassifizierungskatalog ist das 1991 veröffentlichte Dokument „Kriterien für die Sicherheit von Systemen der Informationstechnik“, auch ITSEC (Information Technology Security Evaluation Criteria) genannt [BSI92]. ITSEC ist ursprünglich durch Vereinheitlichung der nationalen Richtlinien von Frankreich, Deutschland, Niederlande und Großbritannien entstanden. Heute ist ITSEC im gesamten EG-Raum als einheitliche Klassifikationsrichtlinie anerkannt. Auch der ITSEC-Kriterienkatalog teilt IT-Systeme in 7 Sicherheitsklassen ein.

Systeme, die einer Sicherheitsklasse des einen Kriterienkataloges entsprechen, erfüllen zumeist auch die Vorgaben der korrespondierenden Klasse des anderen Kataloges. Nachfolgend sind die wesentlichen Forderungen und die Korrespondenz von TCSEC- und ITSEC-Sicherheitsklassen dargestellt.

TCSEC-Klasse	ITSEC-Klasse	wesentliche Forderungen
E0	D	- geringster Sicherheitsstandard - alle Systeme, die nicht die Anforderungen der höheren Klassen erfüllen

E1	C1	<ul style="list-style-type: none"> - alle Benutzergruppen befinden sich auf demselben Sicherheitsniveau - Trennung zwischen Benutzern und Daten
E2	C2	<ul style="list-style-type: none"> - Überwachung und Speicherung der Operationen der einzelnen Benutzer - individuelle Identifizierung der einzelnen Benutzer - Schutz der Überwachungsdaten vor nicht autorisierten Zugriffen
E3	B1	<ul style="list-style-type: none"> - Forderungen von E2/C2 - Beseitigung aller bekannten Einbruchsmöglichkeiten in das System - verbindliche Zugangskontrollen - formelle Beschreibung des Sicherheitsmodells - vollständige Dokumentation der Funktionen des Systemverwalters - Markierung aller Objekte durch Geheimhaltungsstufen - Kenntlichmachung von vertraulichen Daten
E4	B2	<ul style="list-style-type: none"> - Forderungen von E3/B1 - Zugangskontrollen zu allen vom IT-System erreichbaren Komponenten - gesicherter Kommunikationspfad zwischen Benutzer und IT-System - elektromagnetische Abschirmung des IT-Systems nach außen
E5	B3	<ul style="list-style-type: none"> - Forderungen von E4/B2 - Eintragung aller nicht zugriffsberechtigten Benutzer in Zugangslisten - detaillierte Beschreibung des Sicherheitsmodells - automatische Erfassung von sicherheitsrelevanten Ereignissen - modularer Aufbau des IT-Systems - Verlagerung bestimmter Funktionen in Hardware des IT-Systems - gesicherte Wiederherstellung des Systemzustands nach Fehlern
E6	A1	<ul style="list-style-type: none"> - Forderungen von E5/B3 - keinerlei Systemerweiterungen gegenüber E5/B3 - formelle Beschreibung des Software-Designs - mathematische Eindeutigkeit des Sicherheitsmodells - Nachweis der fehlerfreien Implementierung der Software - Garantie der spezifischen Auslieferung von Hard- und Software

Tabelle 4-1 : Forderungen und Korrespondenz von TCSEC- und ITSEC-Sicherheitsklassen

Die Konformitätsprüfung und offizielle Klassifizierung nach dem ITSEC-Katalog (Orange-Book) wird vom National Computer Security Center in den USA durchgeführt. Zu beachten ist, daß eine Evaluierung von Sicherheitssystemen erst ab Klasse B1 aufwärts durchgeführt wird und daß diese für eine Dauer von ein bis zwei Jahren veranschlagt wird.

Die meisten Firmen, die für ihre Produkte eine ITSEC-Klassifizierung ausweisen, geben hierfür meist keinerlei Erläuterungen. Hierbei ist davon auszugehen, daß es sich um einen geringen Sicherheitsstandard handelt. Auch gibt es Firmen, die in den technischen Datenblättern ihrer Produkte die „Mechanismenstärke hoch“ ausweisen, bei einem Produkt der Firma KryptoKom verbarg sich jedoch dahinter die Klasse E2, entsprechend Tabelle 4-1 die zweitniedrigste Schutzklasse [KRY96].

4.2. Encryption

Die Encryption oder Kryptografie umfaßt alle Verschlüsselungsmechanismen, mit deren Hilfe Daten in eine für jeden unverständliche Form transformiert werden können. Diejenigen Personen, die Zugang

zu den Daten erhalten sollen, erhalten einen geheimen Entschlüsselungscode, mit dessen Hilfe es möglich ist, die unleserlichen Daten wieder in eine verständliche Form zurückzutransformieren.

Neben der Vertraulichkeit durch die Verschlüsselung von Klartext kann mittels Encryption auch die Authentizität einer Nachricht sowie die Integrität einer Datei sichergestellt werden. Authentizität heißt, Gewißheit über die Identität des Verfassers zu haben, und kann mittels Digitaler Signaturen, d.h. Digitale Unterschriften des Urhebers einer Nachricht, realisiert werden. Integrität heißt, Gewißheit über den Empfang der Datei in unveränderter Form zu haben, und kann mittels Message Digests (MD), d.h. Quersummenbildung über die Datei, erzielt werden.

Hauptanwendungen für die Encryption sind die Übertragung von sensiblen Daten über unsichere Netzwerke und die Unleserlichmachung von sensiblen Daten auf Speichermedien für unbefugte Personen.

Bei der Encryption gibt es zwei grundsätzlich verschiedene Methoden: die symmetrische und die asymmetrische Verschlüsselung. Bei symmetrischen Verfahren wird ein einziger Schlüssel benutzt, der sowohl dem Sender als auch dem Empfänger der codierten Nachricht bekannt sein muß. Der Schlüssel ist daher unbedingt geheimzuhalten. Symmetrische Verfahren heißen daher auch Private-Key-Verfahren. Der Schlüssel muß vor der Kommunikation über einen sicheren Kanal zwischen den Partnern ausgetauscht oder von einer dritten Stelle an die Kommunikationspartner verteilt werden (siehe Bild 4-2 [RUL93]).

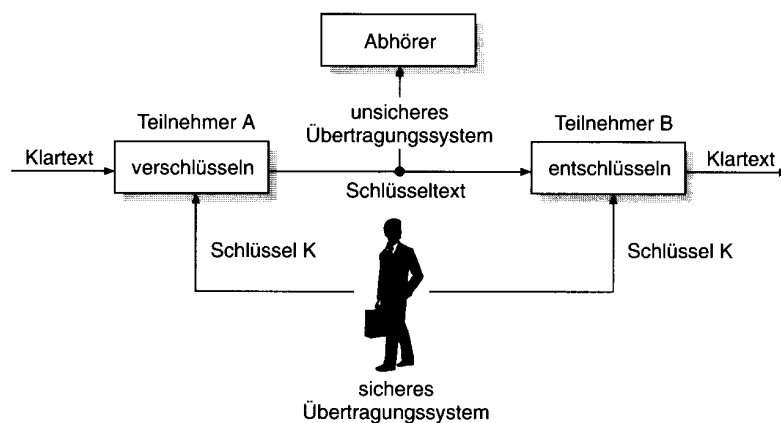


Bild 4-2 : Symmetrische Verschlüsselung

Bei asymmetrischen Verfahren werden dagegen zwei verschiedene Schlüssel benutzt, wobei einer bewußt veröffentlicht wird. Daher heißen diese Verfahren auch Public-Key-Verfahren. Jeder Teilnehmer erhält ein persönliches Schlüsselsystem. Der Schlüssel des Systems, der öffentlich bekannt gegeben werden kann, heißt öffentlicher Schlüssel (public key), der andere ist der geheime Schlüssel (secret key). Bild 4-3 [RUL93] veranschaulicht das Prinzip der asymmetrischen Verschlüsselung,

wobei der öffentliche Schlüssel zur Verschlüsselung und der geheime Schlüssel zur Entschlüsselung verwendet wird.

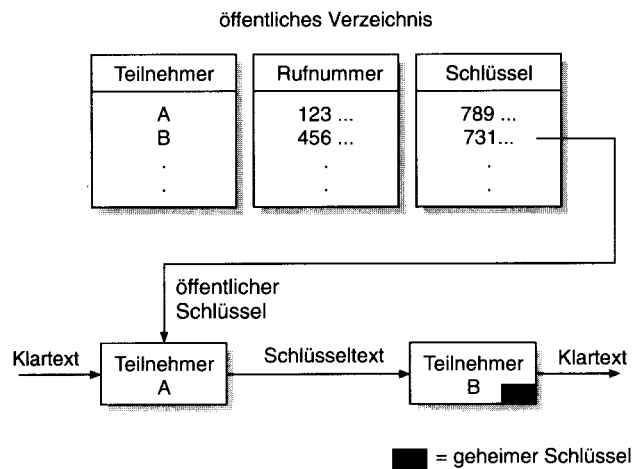


Bild 4-3 : Asymmetrische Verschlüsselung

Nachfolgend sind die wichtigsten, derzeit gängigsten Verfahren für Encryption angeführt. Für eine vollständigere Behandlung sei der Leser an folgende Literatur verwiesen: [DEU82], [RUL93], [SCH94].

4.2.1. Data Encryption Standard (DES)

Der Data Encryption Standard ist das bekannteste Beispiel für ein symmetrisches Verschlüsselungsverfahren. Der DES, von IBM entwickelt, wurde bereits 1974 veröffentlicht und in den USA als ANSI-Standard normiert. 1978 wurde DES zum nicht-sicherheitsrelevanten Einsatz für US-Bundesbehörden freigegeben. Alle fünf Jahre findet eine Überprüfung statt, wobei die letzte, 1993, DES für den Einsatz im Bankwesen und zur Authentifikation bestätigte [CHE96]. DES kann als internationaler Quasi-Standard bezeichnet werden.

DES ist ein Blockalgorithmus, der 64 Bit-Klartextblöcke in 64 Bit-Schlüsselblöcke konvertiert. Zur Verschlüsselung benutzt DES einen 64 Bit langen Schlüssel, wovon 8 Bits die Funktion von Paritätsbits haben. Der Ablauf einer DES-Verschlüsselung eines Klartextblocks ist in Bild 4-4 [RUL93] erläutert. Dabei wird der Ausgangstext zunächst einer Reihe von Permutationen und Substitutionen unterworfen. Das Resultat wird im Anschluß durch ein logisches Exklusiv-Oder mit dem ursprünglichen Klartext verknüpft. Diese Verschlüsselungssequenz wird sechzehn Mal mit einer jeweils unterschiedlichen Anordnung der Schlüsselbits wiederholt.

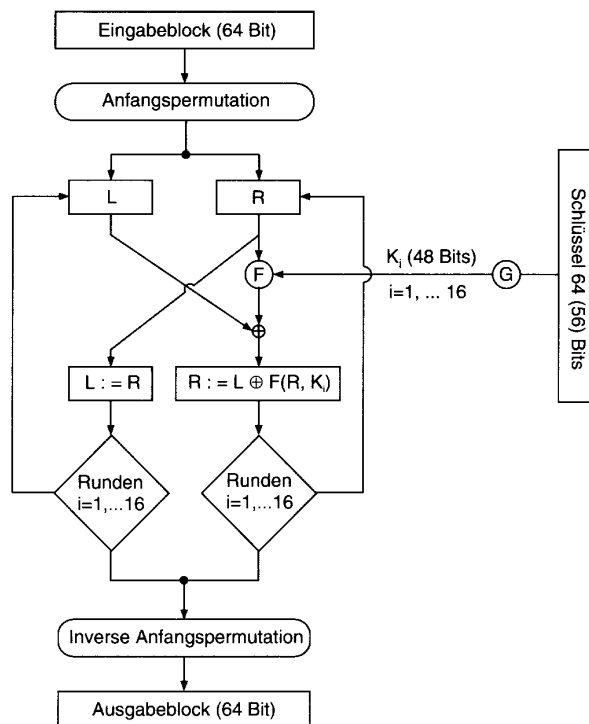


Bild 4-4 : Prinzipieller Aufbau des DES

Nach heutigen Standards ist die resultierende Verschlüsselung als einigermaßen sicher anzusehen [KYS96]. Michael J. Wiener stellte 1994 [WIE94] einen effizienten DES-Cracker vor. Nach seinen Schätzungen könnte für 1 Million Dollar eine Maschine gebaut werden, die binnen 7 Stunden jeden der 2^{56} möglichen Schlüssel findet. Im Mittel benötigt sie die halbe Zeit. Dieser Entwurf ist skalierbar, d.h. für ein Zehntel der Investitionssumme ist die benötigte Zeit zu verzehnfachen..

Um die Sicherheit von DES weiter zu erhöhen, wurde eine Variante von DES, das Triple DES, entwickelt. Es wurde 1981 von Merkle und Hellmann veröffentlicht und ist u.a. Bestandteil der „Common Cryptographic Architecture“ der Firma IBM. Durch die Vergrößerung der Schlüssellänge von DES auf das Zwei- bis Dreifache wird allerdings auch die Rechenzeit für die Ver- und Entschlüsselung im gleichen Maße vergrößert.

In der Tabelle 4-2 wird auf heute erreichbare Werte des Datendurchsatzes mit verschiedenen DES-Verschlüsselungs-Implementationen eingegangen [KYS96], [RUL93].

Krypto-Hardware	Datendurchsatz
DEC VLSI Chip	1 Gbit/s
CE SuperCrypt 99C003 Chip	96 Mbit/s
AMD Chip	14 Mbit/s
PC-Assembler 486/25 MHz	840 kbit/s
PC-Assembler 386/25 MHz	250 kbit/s
Smart Cards	2 kbit/s

Tabelle 4-2 : Durchsatz von DES-Verschlüsselungs-Implementationen

Weitere bedeutende symmetrische Block-Verschlüsselungsverfahren heißen RC2 und RC4. Sie benötigen etwa dieselbe Verschlüsselungszeit wie DES, können aber je nach Sicherheitsanforderungen mit variabler Schlüssellänge arbeiten.

4.2.2. Kerberos

Im Rahmen des Internet und besonders der Sicherung von Weitverkehrsnetzen ist die Geheimhaltung, das Haupteinsatzgebiet der Encryption, häufig zweitrangig. Häufig ist man mehr an der durch die Verschlüsselung implizierten Authentifikation interessiert : ein Paket, welches nicht mit dem richtigen Schlüssel chiffriert wurde, ergibt entschlüsselt keinen Sinn. Dies schränkt die Möglichkeiten eines möglichen Angreifers, z.B. gefälschte Nachrichten einzuschleusen, erheblich ein.

Ein auf dem DES-Verfahren beruhendes Netzwerk-Authentifikationsverfahren ist das Kerberos-System [RFC1510]. Kerberos wurde am Massachusetts Institute of Technology (MIT) entwickelt und dient der Authentifikation von Zugriffen auf die verschiedenen Netzwerkdienste (sog. Logins) in Echtzeit [KYS96].

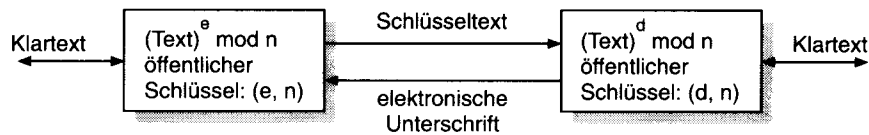
Kern des Systems ist ein sog. Kerberos-Server, der in einer Datenbank die Schlüssel aller registrierten Benutzer enthält. Dazu muß dieser Server vollständig abgeschrimmt und gesichert installiert sein. Möchte ein Benutzer einen bestimmten Dienst nutzen oder eine gesicherte Kommunikationsbeziehung aufbauen, überprüft der Kerberos-Server anhand des DES-Schlüssels dessen Identität und generiert einen sog. Session Key, der nur während der Nutzung des betreffenden Dienstes gültig ist.

Nachteil des Kerberos-Systems ist, wie bei allen symmetrischen Verschlüsselungsverfahren, daß eine externe Instanz wie der Kerberos-Server benötigt wird. Gelingt es einem Angreifer, diesen Server auszuschalten, so ist die Sicherheit des gesamten Netzwerkes gefährdet.

4.2.3. RSA-Verfahren

Das bekannteste und verbreitetste asymmetrische Verfahren ist das nach seinen Erfindern Rivest, Shamir und Adleman benannte RSA-Verfahren. Das RSA-Verfahren wurde 1978 veröffentlicht und kann als Quasi-Standard bei den asymmetrischen Verfahren angesehen werden (ähnlich dem DES bei den symmetrischen Verfahren).

Den Ablauf des RSA-Verfahrens demonstriert Bild 4-5 [RUL93].

**Bild 4-5 : Prinzip des RSA-Verfahrens**

Der öffentliche Schlüssel besteht aus dem Zahlenpaar (e, n) , wobei e der öffentliche Exponent und n der Modulus ist. Der geheime Schlüssel entspricht der Zahl d , auch als geheimer Exponent bezeichnet. Der geheime Exponent d kann aus dem öffentlichen Schlüssel (e, n) nur errechnet werden, wenn es gelingt, n in seine Primfaktoren, d.h. in zwei Primzahlen, die miteinander multipliziert wieder die Ausgangszahl n ergeben, zu zerlegen.

Die Schlüssellänge beträgt meist 512 Bit, in manchen Anwendungen werden auch bereits 768 Bit lange Schlüssel vorgezogen. Ist die numerische Länge des Nachrichtentextes größer als die Schlüssellänge, muß der Text in Blöcke aufgeteilt werden. Daher wird der RSA-Algorithmus auch als Blockalgorithmus bezeichnet.

In der Tabelle 4-3 wird auf heute erreichbare Werte des Datendurchsatzes mit verschiedenen RSA-Verschlüsselungs-Implementationen eingegangen [KYS96], [RUL93]. Dabei wird eine Schlüssellänge von 512 Bit verwendet.

Krypto-Hardware	Datendurchsatz
schnellster RSA-Chip	600 kbit/s
Vught PCC200 VLSI Chip	40 kbit/s
Cryptech PC Crypto Toolkit	20 kbit/s
KryptoKom KryptoServer	16 kbit/s

Tabelle 4-3 : Durchsatz von RSA-Verschlüsselungs-Implementationen

Der Vorteil des RSA-Verfahrens ist die hohe Sicherheit. Diese basiert auf der Schwierigkeit, die großen Zahlen n (512-Bit-Zahlen, entsprechen dezimal etwa 155 Ziffern) in Primfaktoren zu zerlegen. Die derzeit effizientesten Algorithmen sind in lediglich in der Lage, Zahlen mit bis zu 120 Ziffern in Primfaktoren zu zerlegen [KYS96]. Derzeitige Schätzungen ergeben, daß ein System mit einer Rechenleistung von 1 MIPS (1 Million Operationen je Sekunde) 420000 Jahre rechnen müßte, um die entsprechenden Primfaktoren zu finden [KYS96].

Ein Nachteil gegenüber symmetrischen Verfahren ist jedoch die deutlich höhere benötigte Rechenleistung (vgl. Tabellen 4-2 und 4-3). DES-Hardware-Implementationen sind um den Faktor 1000 bis 10000, DES-Software-Implementationen um den Faktor 100 schneller als vergleichbare RSA-Implementationen [KYS96].

4.2.4. Angriffsmöglichkeiten gegen Encryptionsysteme

Encryption bietet keinesfalls eine hundertprozentige Sicherheit gegen Angriffe. Nachfolgende Tabelle 4-4 faßt die wichtigsten Angriffsformen gegen Encryptionsysteme zusammen.

Bezeichnung	Erläuterung
Abhören	Abhören der Kommunikation durch einen Lauscher (passiver Angreifer)
Birthday Attack	Angriff auf die Hash-Funktionen (zusätzl. String mit Informationen), bei dem zwei Nachrichten mit der gleichen Signatur (Hash-Wert) gesucht werden
Chosen Plaintext Attack	Senden eines vom Angreifer gewählten Klartextes zum Angriffsziel und anschließende Beobachtung der Zustellung der verschlüsselten Kopie
Cut and Paste	Empfang von mehreren Nachrichten derselben Codierung, Zusammenstellung einer neuen Nachricht von Stücken aus diesen, Absendung dieser neuen Nachricht an das Angriffsziel und Manipulation von Reaktionen
Man in the Middle Attack	Zwischenschaltung des Gegners zwischen zwei Kommunikationspartner und Vortäuschung des jeweiligen Partners
Known Plaintext Attack	Kryptoanalyse von Crips (Paare von bekanntem Klartext und zugehörigem Chifftrat), die in Besitz des Angreifers gelangen
Kryptoanalyse	Entzifferung von chiffrierten Nachrichten ohne Kenntnis des Schlüssels
Pragmatische Kryptoanalyse	Diebstahl des Schlüssels (Gegenteil der Kryptoanalyse)
Replay	Wiederholung einer legitimen Nachricht zu einem späteren Zeitpunkt
Täuschen	Einfügen von Nachrichten oder Löschung bzw. Modifizierung von legitimen Nachrichten durch den Gegner (aktiver Angreifer)
Vollständiges Durchsuchen	Ausprobieren aller Schlüssel (auch Brute Force oder Exhaustive Search genannt)
Zeit-Manipulation	Verwirrung der Zeitvorstellung des Angriffsziels durch den Angreifer bei Protokollen, die die aktuelle Zeit verwenden

Tabelle 4-4 : Angriffsformen gegen Encryptionsysteme

4.2.5. Anwendungsbeispiele

Während vor wenigen Jahrzehnten die Encryption ausschließlich auf militärischem Gebiet zum Einsatz kam, gibt es heute Einsatzbeispiele für Encryption auf allen Gebieten der Datenkommunikation.

So verwenden die meisten Firewall-Systeme, die ein entferntes Management unterstützen, Encryption zur geschützten Übertragung ihrer Konfigurationsdaten zwischen den Firewall-Modulen und der entfernten Managementstation.

Im Betriebssystem UNIX, dem weitverbreitetsten Server-Betriebssystem, werden die Paßwort-Daten verschlüsselt nach dem DES-Algorithmus in einer Datei (passwd) abgelegt.

In Kryptoboxen der deutschen Firma KryptoKom werden die symmetrischen Verfahren (DES) zur schnellen Datenverschlüsselung und die Public-Key-Verfahren (RSA) zur Authentifikation und zum Key-Management eingesetzt.

Das Cisco-Betriebssystem IOS unterstützt Layer3-Encryption auf Routern, die so als Endgeräte für Encryption einsetzbar sind (RSA (Public Key) für Authentifikation des Routers, DES (Secret Key) für fortlaufende Datenübertragung).

Auch der Cisco-PIX-Firewall kann mit einem Zusatzmodul zu einem Cisco PIX Private Link umgerüstet werden, das es ihm ermöglicht, als DES-Encryption-System zu arbeiten.

Ein aktuelles Anwendungsgebiet für Encryption ist die Bildung von Virtual Private Networks (VPN): mehrere räumlich getrennte Standorte eines Unternehmens kommunizieren verschlüsselt über das Internet miteinander, dies spart kostenintensive Standleitungen. Durch die Encryption wird ein sog. Tunneling durch das unsichere Netz realisiert, d.h. die sensitiven Daten, die zwischen verschiedenen Standorten ausgetauscht werden, bleiben den übrigen Internetbenutzern verborgen.

4.3. Access Control

Die häufigste Ursache für erfolgreiche Einbrüche in Computer-Systeme liegt im Versagen von Mechanismen, die der Zugangskontrolle bzw. Access Control dienen. Die Schlüsselrolle spielt dabei die Benutzer-Authentifikation, mit der die Identität eines Nutzers und damit verbundene Nutzungsrechte, für die er autorisiert ist, überprüft werden.

Der Gewährleistung von Authentifikation (und weiteren Sicherheitsmechanismen) sowie der Übermittlung von diesbezüglichen Daten dienen speziell zugeschnittene Protokolle, nachfolgend auch Security-Protokolle genannt.

4.3.1. Benutzer-Authentifikation

Paßworte

Paßwörter sind das einfachste und älteste Mittel persönlicher Authentifikation. Der Vorteil liegt darin, daß ihr Einsatz keine besondere Ausrüstung erfordert, der Nachteil darin, daß diese im einfachsten Fall weitergegeben oder erraten werden können.

Für letzteres gibt es eine Reihe frei verfügbarer Rateprogramme, die den Prozeß automatisieren. Dabei ist es sogar möglich, DES-verschlüsselte Paßwörter (z.B. UNIX-Paßwörter) zu erraten, indem man die eigene Wortliste mit demselben Algorithmus kodiert und die Sequenzen vergleicht.

Anspruchsvollere Formen des Paßwort-Angriffes sind Sniffing (Protokollanalyse mit Paßwortfilterung), TSR-Monitoring (Aufzeichnen von Logins über längere Zeiträume) und Trojanische Pferde (getarnte Login-Programme mit E-Mail-Funktion).

Einmal-Paßworte

Durch die Verwendung von Einmal-Paßwörtern kann eine deutliche Steigerung der Sicherheit gegenüber herkömmlichen Paßwörtern erzielt werden. Einmal-Paßworte werden genau einmal verwendet und sind danach ungültig. Es gibt verschiedene Möglichkeiten, Einmal-Paßwort-Konzepte zu implementieren.

Das bekannteste Konzept beruht auf einer Art Taschenauthenticator, auch Token oder Dongle genannt. Eine verbreitete Form enthält eine interne Uhr, einen geheimen Schlüssel und eine Anzeige. Die aktuelle Zeit und der geheime Schlüssel werden durch eine Funktion verknüpft und das Ergebnis angezeigt. Dieser Wert, der sich alle 30 oder 60 Sekunden ändert, dient zur Authentifikation, er wiederholt sich nie [CHE96].

Der Server überprüft die Authentizität des Benutzers, indem er mit Hilfe seiner eigenen Uhr und einer Kopie des geheimen Schlüssels das erwartete Ergebnis berechnet. Stimmen beide überein, wird der Login gestattet.

In der Praxis können Gangfehler zwischen Server und Token zum Problem werden. Als Gegenmaßnahme werden Ergebnisse für ein gewisses Zeitfenster berechnet und das Paßwort des Benutzers mit all diesen Werten verglichen. Das hat jedoch den Nachteil, daß Paßworte innerhalb des Zeitfensters wiederverwendet werden können. Daher sollten Implementierungen kurze Zeitfenster verwenden und sich alle bereits verwendeten Paßwörter merken sowie eine versuchte Wiederverwendung abweisen und protokollieren.

Ein anderes Einmal-Paßwort-Konzept verwendet statt einer Uhr einen Challenge, der vom Server bestimmt und nicht wiederholt wird. Auch hier hat der Benutzer ein Gerät mit gespeichertem, geheimen Schlüssel. Der Challenge wird in das Gerät eingegeben, wobei dieser aus Challenge und Schlüssel ein Paßwort berechnet.

Da keine Uhr beteiligt ist, gibt es auch keine Gangunterschiede und daher keine Notwendigkeit, Paßworte zu merken. Andererseits muß das Gerät eine Tastatur besitzen, und der Benutzer muß den Challenge eingeben.

Beide Konzepte beruhen auf Geräten, die gestohlen werden können. Abhilfe schaffen persönliche Identifikationsnummern (PIN). Ein Angreifer benötigt dann sowohl die PIN als auch das Gerät, um den Benutzer zu verkörpern, ähnlich dem Bankautomaten-Geschäft.

Smart Cards

Eine Chipkarte oder Smart Card ist ein tragbares, scheckkartengroßes Gerät mit einer CPU, mehreren I/O-Kanälen und einem einigen Kbyte großen ROM-Speicher, der nur von der CPU der Karte zugreifbar ist. Das Gegenstück ist ein Lesegerät, das im jeweiligen Terminal, Workstation etc. des Benutzers integriert ist. Chipkarten werden oft durch eine PIN ergänzt

Mit dieser Art von Authentifikation werden die Schwachstellen der Einmal-Paßwort-Konzepte, die angreifbaren Schlüsseltabellen der Server, beseitigt.

Biometrik

Diese Methode der Benutzerauthentifikation versucht, benutzerspezifische Eigenschaften zu messen. Hierzu zählen etwa Fingerabdruck, Stimmuster oder Unterschrift. Dazu wird spezielle Hardware benötigt, wodurch die Einsatzmöglichkeit biometrischer Verfahren stark eingeschränkt wird. Attraktiv sind diese Verfahren, weil biometrische Kennzeichen weder weitergegeben noch gestohlen werden können.

In der Praxis gibt es einige Grenzen. Traditionelle Sicherheitsregeln fordern, daß Authentifikationsdaten regelmäßig geändert werden, dies ist jedoch z.B. bei Fingerabdrücken nicht möglich. Außerdem stoßen einige Methoden auf Widerstand bei den Benutzern, wie z.B. bei Lippenabdrücken [DAV89]. Außerdem gibt es Toleranzen bei der Identitätsprüfung (z.B. durch Krankheit, Stimmungsschwankungen), die eine Entscheidung unsicher machen.

Zur Zeit ist kein routinemäßiger Einsatz biometrischer Daten im Internet bekannt [CHE96], was sich jedoch z.B. mit der Verbreitung mikrofonbestückter Computer ändern kann.

4.3.2. Security-Protokolle

RADIUS

RADIUS bedeutet Remote Authentication Dial In User Service und wurde von Livingston Enterprise entwickelt. Es ist ein Client-Server-basierendes Security-Protokoll, das auf einem vom IETF empfohlenen Modell für verteilte Sicherheitssysteme basiert und bei Zugriffen von Remote-Systemen die Sicherheit im Netz gewährleistet. Dabei werden die Authentifikation, die Benutzerberechtigung (Authorisierung) und die Konfigurationsparameter der sich einwählenden Komponenten überprüft.

Dies erfolgt auf Basis einer vom Network Access Server (NAS) abgesetzten zentralen Datenbank, dem RADIUS-Server.

Zu den wichtigsten Funktionen, die RADIUS bietet, zählen die Verwaltung eingehender und ausgehender Anrufe, der Wiederaufbau von unterbrochenen Verbindungen, die Protokollierung und die Bereitstellung von QoS-Diensten.

RADIUS hat den Vorteil, daß dieser Mechanismus sowohl in lokalen als auch in Weitverkehrsnetzen einsetzbar ist. Außerdem können mehrere Benutzer gleichzeitig auf ihre Zugangsberechtigung hin überprüft werden. Als Nachteil gilt, daß bei der Authentifikation lediglich das übermittelte Paßwort verschlüsselt wird, die anderen Informationen wie Benutzername sowie Autorisierung und Accounting erfolgen unverschlüsselt. Außerdem ist es dem Benutzer nicht möglich, ggf. sein Paßwort zu ändern.

TACACS

TACACS bedeutet Terminal Access Controller Access Control System und ist in RFC 927 und RFC 1492 vom IETF definiert.

TACACS+ ist die Weiterentwicklung von TACACS und unterstützt wie RADIUS den sicheren Zugang in Netzwerke (siehe [Anlage 7]). Es werden Authentifikation, Autorisierung und Accounting (AAA) unterstützt. Authentifikation bestimmt die Identität des Benutzers und prüft, ob dieser Berechtigung zur Einwahl besitzt. Autorisierung berechtigt den ausgewählten Benutzer zu bestimmten Handlungen. Accounting ist eine Protokollierung aller Handlungen des Benutzers inklusive der zugehörigen Zeit. Dabei ist die Architektur ähnlich dem RADIUS: Wiederum erfolgt der Transfer zwischen Network Access Server (NAS) und zentraler Datenbank (TACACS-Server).

Der Vorteil von TACACS gegenüber RADIUS liegt darin, daß hier die gesamte AAA-Übertragung verschlüsselt erfolgt. Außerdem wird eine zwischenzeitliche Änderung des jeweiligen Paßwortes unterstützt. Ein dritter Vorteil ist, daß durch eine Trennung von Authentifikation, Autorisierung und Accounting das Sicherheitssystem mit anderen Komponenten verknüpft werden kann. Eine verbreitete Architektur ist der parallele Einsatz eines TACACS-Servers (für Autorisierung und Accounting) und eines Kerberos-Servers (für Authentifikation).

TACACS unterstützt die Token Card-Systeme verschiedener Hersteller (z.B. der Firma Security Dynamics), dabei kann die erforderliche Token-Software entweder auf dem TACACS-Server oder auf einem eigenen Token-Server implementiert werden (siehe [Anlage 10]).

SecureSNMP / SNMP 2

Das Simple Network Management Protocol (SNMP) gilt seit seiner Einführung 1989 als Standard für die Netzwerkmanagementwelt, und dies trotz fast gänzlich fehlender Sicherheitsmechanismen. SNMP wird in den RFCs 1155-1157 sowie in RFC 1213 spezifiziert. Sämtliche Hardware-Komponenten wie Switches, Hubs und Router werden mit dem auf IP basierenden SNMP-Protokoll gemanagt.

SNMP verfügt nur über ein triviales Authentifikationsschema. Community-Strings für Lese- und Schreibvorgänge, die im Klartext auf dem Netz übertragen werden, sind als einziger Schutzmechanismus implementiert. Als Mangel gelten dagegen folgende Punkte:

- Es ist keine Datenintegrität gewährleistet (Daten können manipuliert sein).
- Es erfolgt keine Überprüfung der Quelle (Origin Authentication).
- Es erfolgt keine Geheimhaltung der Daten (Confidentiality).

Trotzdem wird SNMP wegen seiner sonstigen Vorteile selbst bei Banken verwendet [Datko].

Seit 1992 ist ein wesentlich verbesserter SNMP-Standard (SNMP 2) im Gespräch.

SNMP 2 bietet folgende drei Sicherheitsmechanismen: Authentifikation, Verschlüsselung der Daten und Zugriffskontrolle auf einen bestimmten Dienst. Die Verschlüsselung der Daten erfolgt vorwiegend mit dem DES-Algorithmus.

Alle Cisco-Komponenten unterstützen bereits SNMP 2. Das Problem ist jedoch die noch nicht vollzogene Integration von SNMP 2 in die Netzmanagement-Plattformen von Fremdfirmen wie HP und Sun.

Von einigen Seiten wird sogar nur die Zwischenstufe SecureSNMP für die weiterführende Standardisierung favorisiert. SecureSNMP macht gegenüber SNMP den Einsatz des DES-Algorithmus zwingend.

4.3.3. Anwendungsbeispiele

Das RADIUS-Protokoll wird von Access Servern der Firmen Ascend, Livingston, Xylogics und zukünftig auch Cisco unterstützt.

TACACS+ unterstützen Cisco-Router und Access Server, TACACS darüberhinaus auch die Firmen Ascend und Shiva (siehe Anlage 4, 5 u. 7)).

TACACS-kompatible Token Cards werden von der Firma Security Dynamics angeboten. Dabei handelt es sich um SecurID-Karten, deren Schlüssel aus 4 bis 8 Ziffern besteht und sich im Intervall von 30, 60 oder 120 Sekunden ändert. Das Zeitfenster ist 3 Intervalle breit. Die Laufzeit der SecurID-Karten beträgt 3 Jahre, diese gibt es auch mit integrierter PIN-Tastatur (siehe [Anlage 10]).

Beispiele für PIN-geschützte Smart Cards sind die Chipkarten der Firma KryptoKom in Kombination mit geeigneten Chipkartenlesern für die Authentifikation an Netzzugängen (siehe [Anlage 10]).

4.4. Firewalls

„Ein Firewall ist eine Schwelle zwischen zwei Netzen, die überwunden werden muß, um Systeme im jeweils anderen Netz zu erreichen. Durch technische und administrative Maßnahmen wird dafür gesorgt, daß jede Kommunikation zwischen den beiden Netzen über den Firewall geführt werden muß. Auf dem Firewall sorgen Zugriffskontrolle und Audit dafür, daß das Prinzip der geringsten Berechtigung durchgesetzt wird und potentielle Angreifer schnellstmöglich erkannt werden.“ [DFN76]

In den meisten Fällen werden heute Firewalls zwischen dem internen, privaten Netz und dem öffentlichen Datennetz wie dem Internet errichtet. Dabei ist es deren Aufgabe, einen freien Zugriff der Benutzer des privaten Netzes auf das öffentliche Netzwerk zu ermöglichen und gleichzeitig das eigene Datennetz vor externen Zugriffen zu schützen.

Man unterscheidet drei Hauptkategorien von Firewalls: Packet Filter, Circuit Level Gateways und Application Level Gateways. Diese können allein oder in Kombination eingesetzt werden.

Bild 4-6 zeigt die Funktion von Firewalls anhand des OSI-Referenzmodells.

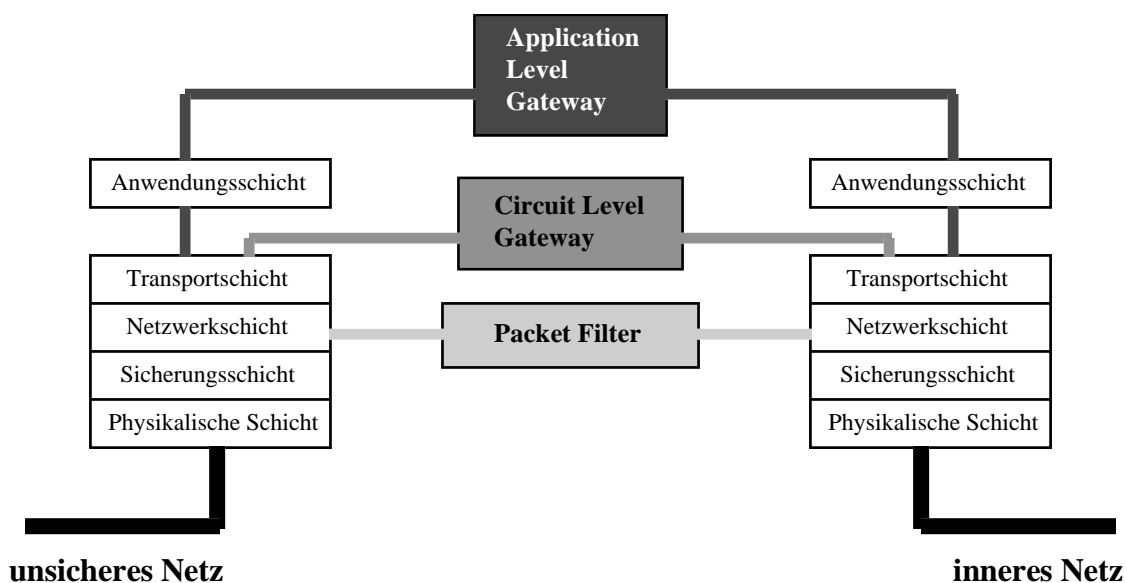


Bild 4-6 : Firewalls und das OSI-Referenzmodell

4.4.1. Packet Filter

Das einfachste und preiswerteste Sicherheitssystem ist der Packet Filter, auch Packet Screen oder Screening Router genannt. Packet Filter sind in der Lage, Datenpakete nach bestimmten Kriterien zu filtern, diese sind: Sende- und Zieladresse, Sende- und Ziel-Port, benutzte Protokolle. Erfüllen Datenpakete die Kriterien nicht, werden sie verworfen.

Als Packet Filter können Netzkomponenten wie Router oder Computer-Systeme mit entsprechender Software eingesetzt werden. Packet Filter sind meist bereits als Software in Routern implementiert. Dabei werden die verschiedenen Kriterien in Form von Routing-Tabellen (Access Lists) angelegt. Je nach Typ des Routers erfolgt die Filterung entweder bei eingehenden oder abgehenden Paketen oder bei beiden. Filtern am Router-Ausgang kann effizienter sein, da sich die Anwendung der Selektionskriterien meist mit Wegwahloperationen kombinieren läßt. Andererseits gehen Informationen verloren, etwa über welche Leitung das Paket empfangen wurde, was z.B. die Abwehr von Adreßfälschungen (IP-Spoofing) schwächt. Filtern am Router-Eingang bietet auch dem Router selbst Schutz vor Angriffen.

Bild 4-6 zeigt die Funktion von Packet Filtern anhand des OSI-Referenzmodells. Die Wirkungsweise beschränkt sich demnach im wesentlichen auf die Filterung des Datenstromes der Netzwerkschicht. Die Problematik der Access Lists besteht darin, daß ein Angreifer z.B. mit Kenntnissen über gültige, zugelassene IP-Adressen in der Lage ist, die auf Access Lists der Router basierenden Security-Mechanismen zu umgehen. Ein weiteres Problem stellt sich im Zusammenhang mit der Performance von Routern: umfangreiche Access Lists wirken sich negativ auf die Geschwindigkeit aus, mit der Pakete von Routern verarbeitet werden können. Außerdem kommt ein beträchtlicher Verwaltungsaufwand für den Administrator bei der Betreuung der Access Lists hinzu: neben physikalischen Umzügen verursachen nämlich auch neue Anforderungen nach Diensten (Beispiel: bisher Telnet, nun auch FTP) einen Betreuungsaufwand. Bei komplexen Netzwerken werden die Filtertabellen zudem rasch unübersichtlich und fehlerhaft.

Bei korrekter Konfiguration der Packet Filter kann ein erster Schutz des Netzwerkes erzielt werden. Packet Filter werden daher vielfach als Vorfilter für weitere Firewall-Komponenten wie Circuit Level Gateways oder Application Level Gateways benutzt.

4.4.2. Circuit Level Gateways

Durch Circuit Level Gateways, auch Circuit Relays genannt, wird eine deutliche Erhöhung der Netzwerksicherheit gegenüber den Packet Filtern erreicht. Circuit Level Gateways ermöglichen den Betrieb von auf den Kommunikationsprotokollen TCP und UDP aufsetzenden Applikationen wie FTP, Telnet, World Wide Web, Gopher usw., ohne eine durchgehende Kommunikationsverbindung auf Protokollebene zuzulassen. Dabei fungiert das Circuit Level Gateway als Vermittlungsstelle für das betreffende Protokoll. Alle eingehenden Verbindungen enden hier und werden am Ausgang neu aufgebaut.

Bild 4-6 zeigt die Funktion von Circuit Level Gateways anhand des OSI-Referenzmodells.

Vorteil der Circuit Level Gateways ist die geringe erforderliche Rechenleistung für das System. Ein Nachteil dieser Systeme besteht darin, daß die Client-Applikationen angepaßt werden müssen, um mit dem jeweiligen Circuit Level Gateway zusammenarbeiten zu können. Außerdem werden nur begrenzt Logging-Funktionalität und Benutzer-Authentifikation unterstützt.

4.4.3. Application Level Gateways

Auch Application Level Gateways ermöglichen wie die Circuit Level Gateways die Nutzung von Anwendungen, ohne eine das Firewall-System durchbrechende darunterliegende Kommunikationsverbindung auf Protokollebene zulassen zu müssen. Sie gehen jedoch noch einen Schritt weiter: während die auf die Protokolle zugeschnittenen Schnittstellenprogramme der Circuit Level Gateways nicht auf die Eigenheiten der Anwendungen eingehen, sind die auch als Proxies bezeichneten Application Level Gateways auf diese zugeschnitten. So haben sie eine wesentlich höhere Kontrolle über die versandten Daten. Allerdings ist für jede Anwendung ein eigenes Proxy-Programm zur Weiterschaltung erforderlich, so daß durch einen Application Level Gateway meist nur wenige Applikationen unterstützt werden.

Bild 4-6 zeigt die Funktion von Application Level Gateways anhand des OSI-Referenzmodells. Diese durchtrennen mit Hilfe der Proxies den Datenfluß auf Anwendungsebene.

Praktisch verhalten sich die Application Level Gateways aus Sicht der Client-Programme wie ein Server-System des jeweiligen Dienstes. Der Vorteil ist, daß die Client-Systeme dabei keinerlei Modifikation unterworfen werden müssen. Außerdem sind eine detaillierte Überwachung der Kommunikationsbeziehungen (Audit) und umfangreiche Logging-Funktionalitäten implementiert. Nicht zuletzt sind eine Reihe von kommerziellen Produkten auf Basis der Application Level Gateways verfügbar.

Nachteilig wirken sich die höhere erforderliche Rechenleistung und die vergleichsweise schwierigere Installation aus.

4.4.4. Network Address Translation (NAT)

Mit Hilfe der in RFC 1631 standardisierten Network Address Translation (NAT) wird eine IP-Adreß-Übersetzung von Netz zu Netz realisiert. Dies hat zweierlei Vorteile. Zum einen kann ein privates an das Internet angeschlossenes Netz in seiner Architektur vor Angreifern aus dem Internet verborgen werden: die internen Subnetze können nicht mehr direkt von außen adressiert werden. Zum anderen kann eine Institution die internen, nicht global gültigen IP-Subnetzadressen trotz Zugang zum Internet beibehalten. Dies beschränkt den Administrationsaufwand auf die Inbetriebnahme der NAT-Hardware.

Bild 4-7 zeigt die Funktionsweise der Network Address Translation anhand des ersten kommerziellen Produkts „Cisco PIX“. Hierzu verfügt der PIX über einen einstellbaren Pool von globalen IP-Adressen, auf die er bei Austausch des IP-Paket-Headers zugreift (siehe [Anlage 8]).

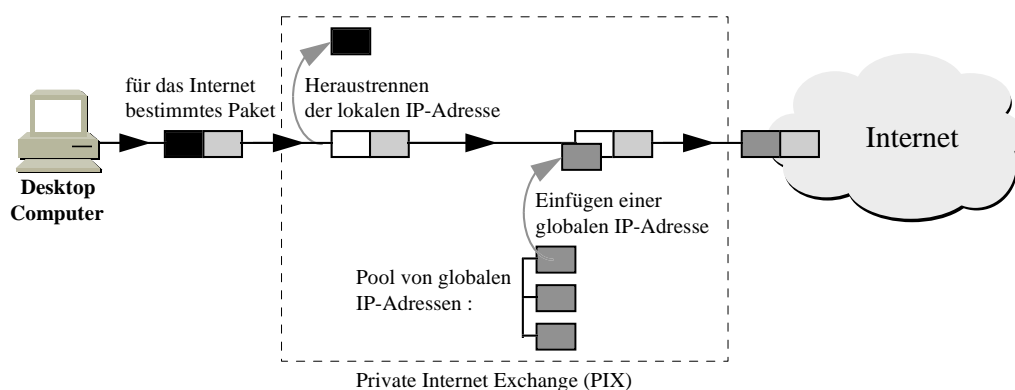


Bild 4-7 : Prinzip der Network Address Translation

4.4.5. Architekturen von Firewalls

Werden die bisher genannten Hauptkategorien von Firewalls in Kombination eingesetzt, ergeben sich eine Vielzahl von möglichen Firewall-Architekturen, auch als Mischtechniken bezeichnet. Die wichtigsten Architekturen sind die nachfolgend beschriebenen:

Screening Router mit abgesichertem Zwischennetz (Screened Subnet)

Hier werden einige wenige dedizierte und gut gesicherte interne Computersysteme zu einem abgesicherten Zwischennetz zusammengefaßt. Der Screening Router wird dabei so konfiguriert, daß lediglich Verbindungen vom bzw. zum Screened Subnet möglich sind.

Der Vorteil hierbei ist, daß dem Angreifer trotz Überwindung des Routers nicht das gesamte innere Netz zugänglich ist (Bild 4-8).

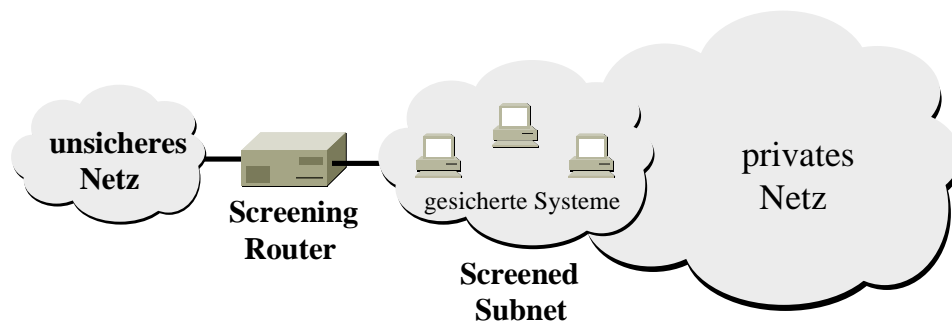


Bild 4-8 : Screening Router mit abgesichertem Zwischennetz (Screened Subnet)

Dual Homed Bastion Hosts

Ein Dual Homed Bastion Host oder Dual Homed Gateway ist ein Computer-System, das physikalisch zwischen dem internen Netzwerk und dem unsicheren Netzwerk platziert ist und zwei Netzwerkanschlüsse (einen Eingang und einen Ausgang) besitzt. Bastion Hosts können als Packet Filter, als Circuit Layer Gateway oder als Application Layer Gateway konfiguriert sein. Wird der Bastion Host mit Circuit Layer Gateways oder Application Layer Gateways ausgestattet, so wird der Aufbau von Verbindungen auf der Ebene der Kommunikationsprotokolle (TCP, UDP) durch das Firewall-System hindurch unterbunden. Von entscheidender Bedeutung für den Einsatz eines Dual Homed Host als Bastion Host ist die Deaktivierung der im UNIX-Kern realisierten Routing-Funktion, da sonst trotz auf höherer Ebene realisierter Firewall-Mechanismen die Daten-Pakete auf unterster Ebene weitergeleitet werden, dieser Fakt wird von vielen Herstellern nachlässig behandelt [Freiss].

Dual Homed Bastion Host mit Demilitarisierter Zone (DMZ)

Der Einsatz einer Demilitarisierten Zone hat den Vorteil, daß angreifbare, weil von beiden Seiten zugängliche Informations-Server (z.B. FTP- und WWW-Server) nicht auf dem Bastion Host installiert werden, sondern ihren Platz in diesem isolierten Netz erhalten. Die Platzierung der Demilitarisierten Zone erfolgt zwischen Screening Router und Dual Homed Bastion Host. Die Server-Systeme in der DMZ (Sacrificial Hosts) werden vom Bastion Host als unsicher eingestuft und behandelt (Bild 4-9).

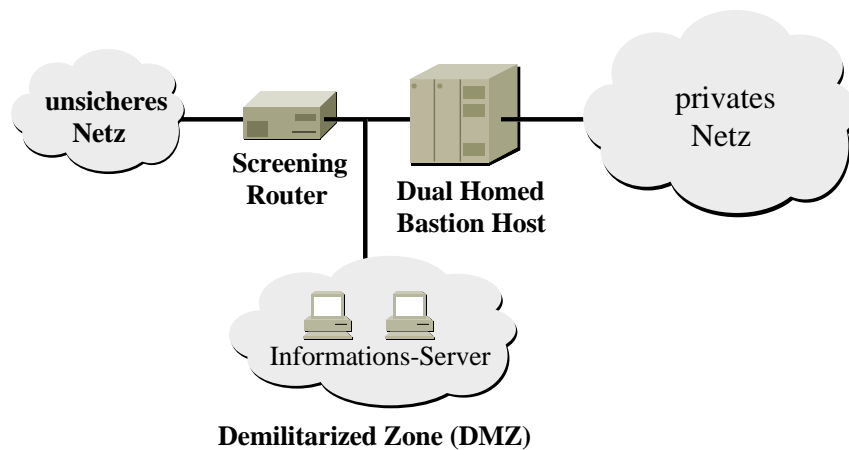


Bild 4-9 : Dual Homed Bastion Host mit Demilitarisierter Zone

Kaskadierte Dual Homed Bastion Hosts

Hiermit wird die größtmögliche Sicherheit erreicht. Dem Screening Router werden dabei zwei oder mehrere Bastion Hosts nachgeordnet. Der Vorteil ist, daß selbst, wenn ein Angreifer in der Lage sein sollte, in den äußeren Bastion Host einzubrechen, das Netzwerk noch durch die nachfolgenden Bastion Hosts geschützt wird.

Bild 4-10 zeigt die Kaskadierung von zwei Dual Homed Bastion Hosts und den davon eingeschlossenen Demilitarisierten Zonen. In der externen DMZ können öffentliche Informationsserver wie FTP- oder WWW-Server angeordnet werden, in der internen nichtöffentliche wie Kunden-FTP- oder Telnet-Server.

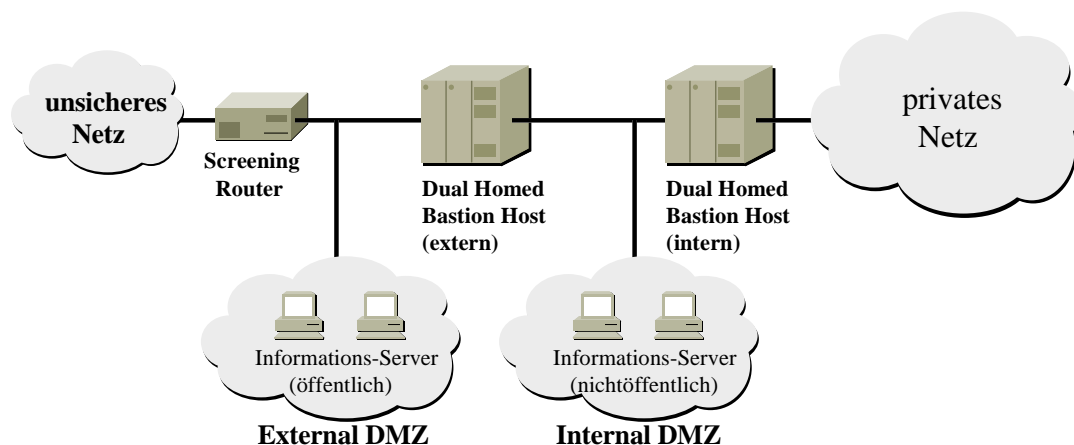


Bild 4-10 : Kaskadierte Dual Homed Bastion Hosts

4.4.6. Plazierung von Firewalls

Traditionell werden Firewalls zwischen dem internen Netz der Organisation und dem öffentlichen Netz errichtet. Große Organisationen können aber durchaus interne Firewalls benötigen, um administrative oder Sicherheitsbereiche (Security Domains) zu isolieren. Unter einem Sicherheitsbereich versteht man einen Rechnerverbund unter einheitlicher Administration, mit einheitlichem Sicherheitskonzept und einheitlicher Geheimhaltungsstufe.

Als Beispiel ist Bild 4-11 angeführt. Die verschiedenen Sicherheitsbereiche sind durch Grautöne angedeutet, die Firewalls durch Symbole in Form von Dioden.

Die Firewalls sollten, wie im Bild dargestellt, an den Grenzen der Sicherheitsbereiche angeordnet werden. Der Pfeil im Symbol zeigt nach außen, in Richtung der Bedrohung.

Beispielsweise traut Netz 1 keinem anderen Netz. Selbst Netz 2, ein internes Datennetz, welches mit Netz 1 zusammenhängt, wird mißtraut. Hingegen traut Netz 5 dem Netz 6. Die Netze 3, 4 und 7 unterliegen derselben Geheimhaltungsstufe und müssen daher nicht durch Firewalls voneinander abgeschirmt werden.

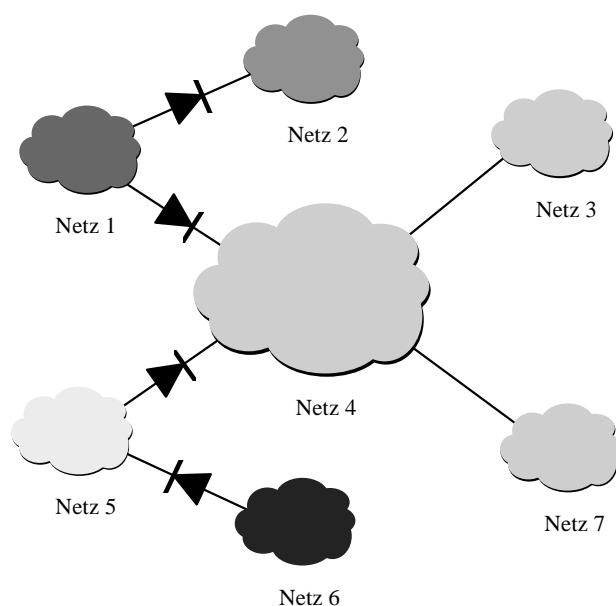


Bild 4-11 : Anordnung von Firewalls

Es gibt viele Gründe zur Errichtung interner Firewalls. In vielen größeren Unternehmen sollen den meisten Angestellten nicht alle Informationen zugänglich sein. Bei anderen muß der produktive Bereich (wie etwa eine Montagestraße oder die Telefonvermittlung) für Entwickler oder Wartungstechniker, nicht aber für sonstige Mitarbeiter zugänglich sein. Selbst befugte Nutzer sollten beim Passieren einer Firewall durch ein Sicherheitsgateway durchgeschleust werden.

4.4.7. Forderungen an Firewalls

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in Zusammenarbeit mit Anwendern und Herstellern einen Kriterienkatalog für den Einsatz von Firewalls in Sicherheitsbereichen (z.B. Behörden) erarbeitet. Diese Forderungen an Firewalls werden wie folgt unterteilt [BSI96]:

a) Forderungen zur Abwehr von Angriffen auf die Firewall-Anordnung

b) Forderungen zur Abwehr von Angriffen auf das zu sichernde Netz

Nachfolgend werden die Schwerpunkte dieser Abhandlung in Stichpunkten zusammengefaßt:

a) Forderungen zur Abwehr von Angriffen auf die Firewall-Anordnung

- Identifikation und Authentisierung für Administrator und Revisor nur über einen vertrauenswürdigen Pfad, z.B. die Konsole, eine verschlüsselte Verbindung oder ein separates Netz
- Die Defaulteinstellung der Rechte muß sicherstellen, daß die Rollen Administrator und Revisor realisiert sind.
- Bei einem Ausfall der Protokollierungskomponente muß eine Warnung ausgegeben werden, die ein unverzügliches Eingreifen des Administrators ermöglicht. Es muß möglich sein, die Firewall so zu konfigurieren, daß bei einem Ausfall der Protokollierungskomponenten jegliche nicht administrative Nutzung der Firewall unterbunden wird.
- Integritätstests der eingesetzten Programme und Dateien mindestens einmal täglich. Es muß möglich sein, die Firewall so zu konfigurieren, daß bei einer Integritätsverletzung jegliche nicht administrative Nutzung der Firewall unterbunden wird. Die für den Integritätstest notwendigen Programme und Dateien müssen auf einem Medium speicherbar sein, welches hardwaremäßig gegen Schreibzugriffe gesichert werden kann. Es muß protokolliert werden, welche Änderungen (mit Datum und Uhrzeit) an der Konfiguration der Firewall vorgenommen wurden.
- Es muß möglich sein, die Firewall so zu konfigurieren, daß bei einem Systemabsturz jegliche nicht administrative Nutzung der Firewall unterbunden wird.
- Auf den eingesetzten Komponenten darf nur Software vorhanden sein, die für die Funktionsfähigkeit der Firewall nötig ist. Die benutzte Software (inkl. aller Konfigurationsdateien) muß ausführlich dokumentiert und begründet werden.

b) Forderungen zur Abwehr von Angriffen auf das zu sichernde Netz

- Die Firewall-Anordnung muß für den Fall des hohen und sehr hohen Schutzbedarfs (ITSEC-Klassen E3 bis E6) aus mindestens zwei getrennten Filtern (z.B. ein Paketfilter und ein Dual-homed

Application-Gateway) bestehen. Die Filter müssen hintereinander angeordnet sein, so daß für eine Verbindung zwischen den beiden beteiligten Netzen beide Filter passiert werden müssen. Die Filter müssen mit unterschiedlicher Hard- und Software (Betriebssystem) arbeiten und unterschiedliche Formate für die Beschreibung der Filterregeln benutzen.

- Die Einstellung der Filterregeln bei einer Erstinstallation und die Anordnung der Komponenten muß sicherstellen, daß alle Verbindungen, die nicht explizit erlaubt sind, blockiert werden. Auch bei einem völligen Ausfall der Firewall-Komponenten dürfen nur Verbindungen durchgelassen werden, die explizit erlaubt worden sind.
- Die Struktur des zu schützenden Netzes muß verdeckt werden können, d.h. daß keine internen Informationen wie Benutzernamen, Rechnernummern, -namen und Mailadressen nach außen gelangen können.
- Die Verwaltung der Komponenten muß zentral über einen vertrauenswürdigen Pfad (z.B. ein separates Netz oder eine verschlüsselte Verbindung) erfolgen und übersichtlich sein (grafisches Interface).
- Der Aufbau von Verbindungen auf der Anwendungsschicht durch die Firewall muß benutzerabhängig und zeitabhängig erlaubt oder verboten werden können.
- Zur Benutzer-Identifikation müssen starke Authentisierungsmethoden benutzt werden.
- Es muß möglich sein, mehrere Benutzer zu einer Gruppe zusammenzufassen, um z.B. Fehler bei Einstellung der Access-Listen infolge einer unübersichtlichen Anzahl von Benutzern zu vermeiden.
- Die Filterregeln müssen auf ihre Widerspruchsfreiheit überprüft werden.
- Es müssen mindestens die Protokolle Telnet, FTP, SMTP, DNS, NNTP und HTTP unterstützt werden. Für Telnet-Verbindungen vom Internet zur Firewall (kommende Verbindungen) muß durch zusätzliche Prozesse eine Verschlüsselung der übertragenen Nutzinformationen durchgeführt werden.
- Für Verbindungen auf der Anwendungsschicht müssen zusätzlich alle Befehle, die den Import von Daten in das zu schützende Netz oder den Export von lokalen Daten ins Internet bewirken, benutzerabhängig und zeitabhängig erlaubt oder verboten werden können.
- Für jede aufgebaute und abgewiesene Verbindung auf der Anwendungsschicht muß eine Protokollierung von Benutzer-Identifikation, IP-Adresse des Quell- und Zielrechners, Portnummer, Zeit und Datum durchgeführt werden, wobei auch Einschränkungen auf bestimmte Verbindungen möglich sind.
- Spezielle, einstellbare Protokollmeldungen müssen zu einer unverzüglichen Warnung führen.
- Die Protokollinformationen von allen Komponenten müssen über einen vertrauenswürdigen Pfad an eine zentrale Stelle geschickt werden können.
- Bei der Benutzung von FTP muß es möglich sein, den Verbindungsaufbau für die Datenverbindung von der Firewall ins Internet durchführen zu lassen (Benutzung des PASV-Kommandos).

Zusätzliche Forderungen bei Verwendung von Packet Filtern:

- Die Weiterleitung von Paketen muß abhängig von
 - a) IP-Quell- und IP-Zieladresse einzelner Rechner oder kompletter Teilnetze und
 - b) Quell- und Zielport für TCP und UDPerlaubt oder verboten werden können. Dies wird in Filterregeln festgelegt.
- Die Filterung gemäß vorherigem Punkt muß getrennt für jedes Interface möglich sein.
- Die Reihenfolge der Filterregeln darf nicht automatisch vom Packet Filter verändert werden.
- Wenn mehr als zwei Interfaces vorhanden sind, muß eine Filterung getrennt für kommende und gehende Pakete möglich sein.
- Bei TCP-Paketen muß eine Unterscheidung, ob ein Verbindungsaufbau stattfindet oder eine bestehende Verbindung benutzt wird, d.h. eine Unterscheidung zwischen ACK und ACK-losen Paketen, möglich sein. Nur so läßt sich sicherstellen, daß ein Verbindungsaufbau nur vom zu schützenden Netz ins unsichere Netz erfolgt.
- Die Filterregeln müssen auf ihre Widerspruchsfreiheit geprüft werden.
- Protokollierung von IP-Nummer, Dienst, Zeit und Datum für jedes Paket, wobei auch Einschränkungen auf bestimmte Pakete (z.B. nur Pakete mit einer speziellen Quell-Adresse) möglich sind.
- Spezielle, einstellbare Protokollmeldungen müssen zu einer unverzüglichen Warnung führen.
- Die Protokollinformationen müssen über einen vertrauenswürdigen Pfad an eine zentrale Stelle geschickt werden können.
- Im Falle der Kombination des Packet Filters mit einem Router darf die Sicherheit der Firewall nicht durch eine Veränderung der Routing-Einträge gefährdet werden. Es muß statisches Routing benutzt werden.
- Source-Routing-Informationen müssen standardmäßig ignoriert werden.

4.4.8. Grenzen von Firewalls

Firewall-Systeme sind lediglich in der Lage, Netzwerkaktivitäten zwischen den OSI-Schichten 2 bis 7 zu überwachen. Sie sind jedoch machtlos gegen:

- Daten, die innerhalb von Applikationen transportiert werden (z.B. Viren)
- verkapselte (getunnelte) Nachrichten (z.B. Protokoll-Tunneling)
- unauthorisierte physikalische Zugriffe auf das interne Datennetzwerk (z.B. Abhören)

Gegen Angriffe dieser Art müssen weitere Maßnahmen ergriffen werden, wie:

- verschlüsselte Übertragung von sensiblen Daten
- umfassende Zugangskontrollen
- Abschließen von Hardware-Komponenten

- Einsatz von LWL-Fasern anstatt von Kupferkabeln

4.4.9. Beispiele für Firewalls

Cisco-Router

Cisco-Router beinhalten Access-Listen, deren Syntax zwischenzeitlich auch von anderen Herstellern übernommen wurde. Diese Access-Listen ermöglichen die Nutzung des Routers als Packet Filter und zeichnen sich durch eine einfache, aber leistungsfähige Struktur aus.

Im Standard-Filterformat (Standard Access List) besteht ein Access-Listen-Eintrag aus vier Komponenten: einer Access-Listen-Nummer, einem Permit/Deny-Operator sowie der Internet-Adresse und optional einer Adreßmaske [Bild 4-12].

Access-Liste (1-99)	permit/deny	Adresse	(Maske)
---------------------	-------------	---------	---------

Bild 4-12 : Standardmäßiges Filterformat im Cisco-Router

Daneben gibt es noch das Erweiterte Filterformat (Extended Access List), in dem zusätzlich das Protokoll, Sendeadresse mit Maske, Empfangsadresse mit Maske, ein logischer Vergleichsoperator (gt = größer als; lt = kleiner als; eq = gleich; neq = ungleich) sowie die Portnummer angegeben werden müssen [Bild 4-13].

Access-Liste (100-199)			
permit/deny	ip/icmp/tcp/udp	Sendeadresse	Sendeadressmaske
Empfangsadresse	Empfangsadressmaske	gt/lt/eq/neq	Portnummer

Bild 4-13 : Erweitertes Filterformat im Cisco-Router

Die Access-Listen-Nummer dient zur Strukturierung der unterschiedlichen Filtereinträge, so daß jedem Router-Interface seine eigenen Bedingungen zugeordnet werden können. Der Permit/Deny-Operator bestimmt, ob ein Paket, das die nachfolgende Filterbedingung erfüllt, weitergeleitet (permit) oder verworfen (deny) werden soll. Mit den Adreßmasken können ganze Adreßbereiche zusammengefaßt werden.

UNIX

Die meisten Firewall-Lösungen setzen auf das UNIX-Betriebssystem auf.

UNIX hat sich heutzutage vor allem in Bereichen der Hochleistungsrechner etabliert. Das Betriebssystem UNIX hat eine Vielzahl von Varianten: ULTRIX, SunOS, OSF/1, HP-UX, AIX, Solaris, IRIX, Linux etc..

Trotz vieler Stärken hat UNIX auch einige Schwächen: zum einen sind die Netzkomponenten zu nennen, die Ursache vieler Sicherheitslücken sind, zum anderen die komplizierte Syntax von Kommandos und die häufig fehlenden grafischen Oberflächen.

Die Netzanbindung von UNIX wurde vor etwa zehn Jahren in das Betriebssystem implementiert, als nur einige hundert Rechner im Internet angeschlossen waren. Entsprechend wenig wurde deshalb in sicherheitsrelevante Implementierungen investiert. Ein grobes Beispiel dieser Art stellt die unverschlüsselte Übertragung von Paßwörtern dar, die ganz einfach abgehört werden kann. Bei neuen Betriebssystemen, wie beispielsweise der Novell Netware, sind kryptographische Elemente von Grund auf implementiert und beseitigen diesen und andere Mängel. Im UNIX-Bereich gibt es auch Produkte wie Kerberos, jedoch gehören diese nicht zum Standard.

Ein weiteres Problem der UNIX-Rechner liegt in deren komplizierter Verwaltung. Noch vor wenigen Jahren gab es keinerlei Tools, diese zu bewältigen. Heutzutage ist diese Situation leicht verändert, jedoch bietet nur AIX ein Tool, das alle Verwaltungsaufgaben ermöglicht. Und selbst zur Bedienung dieses Tools ist einiges Hintergrundwissen erforderlich.

Das Paßwort-File stellt das wesentliche Element zur Kontrolle des Benutzerzugangs auf einem Rechner dar. Es handelt sich hierbei um ein ASCII-File, das eine Liste aller Benutzer enthält, sowie Informationen über das Paßwort (in verschlüsselter Form), den User-Namen, persönliche Daten, das Home-Verzeichnis und die verwendete Shell.

Beim Einloggen wird die Paßworteingabe des Benutzers verschlüsselt und mit dem Eintrag im Paßwortfile verglichen. Stimmen beide überein, so darf sich der Benutzer in das System einloggen. Während es zur Zeit praktisch unmöglich ist, aus der verschlüsselten Form des Paßwortes auf das tatsächliche, unverschlüsselte rückzuschließen, so stellt doch die frei lesbare Form des verschlüsselten Paßwortes eine gewisse Gefahr dar. Sog. Crack-Programme verschlüsseln (nach dem auf allen UNIX-Systemen gleichen Mechanismus) typische Paßwörter und vergleichen diese mit dem Eintrag im Paßwort-File. Bei vielen schlecht gewählten Paßwörtern ist dieses Verfahren erfolgreich, dies gilt für alle Wörter die nur aus Buchstaben bestehen und im Wörterbuch zu finden sind.

Außer Acht gelassen wird häufig, daß die Firewall-Hersteller in der Regel sorglos mit der Konfiguration der zu ihrer Software vertriebenen UNIX-Plattformen umgehen [Freiss]. Glaubt der Anwender (zu Recht), daß eine Verbindung auf Anwendungsebene durch die Firewall-Software wirkungsvoll kontrolliert wird, werden unbemerkt auf Transportebene die Datenpakete durchgereicht

(IP-Forwarding). Bisher ist lediglich der Harris CyberGuard-Firewall ITSEC-klassifiziert worden, da dieses System eine Einheit aus Hardware, Betriebssystem, Firewall-Software bildet, unter Vermeidung von überflüssigen Programm-Codes. Eine ITSEC-Klassifizierung kann nur für das gesamte Sicherheitssystem erfolgen (siehe Kapitel 4.1.).

Firewall-Vergleich

In verschiedenen Anhandlungen der vergangenen zwei Jahre sind Vergleiche zwischen einer Reihe von am Markt verfügbaren Firewall-Systemen angestellt worden. Dabei ging es vor allem um Kriterien wie die Anzahl der unterstützten Dienste, Fernwartbarkeit, Encryption etc.. Da sich gerade in dieser Hinsicht in den letzten Monaten die gängigsten Produkte einander genähert haben, können diese Kriterien bei der Auswahl nicht mehr die entscheidende Rolle spielen.

Für den Anwender entscheidend sind vielmehr neben der grundsätzlichen Technologie und der Anzahl der möglichen User die Sicherheit des Systems als ganzes und die Bedienbarkeit bzw. der Administrationsaufwand.

Im nachfolgenden Vergleich werden daher lediglich diejenigen Produkte erwähnt, die bereits seit mehreren Jahren verfügbar sind und sich hinsichtlich der eingangs erwähnten Kriterien kaum noch unterscheiden. Dabei wurden durch den Verfasser nach umfassenden Recherchen Meinungen verschiedener Anwender verwertet, bzw. diese Produkte eigenhändig vor allem hinsichtlich ihrer Bedienbarkeit überprüft. Im Falle des Cisco PIX hatte der Verfasser gar Gelegenheit, eine Testgestellung bei einem privaten Unternehmen (DSR Rostock) mit diesem Gerät durchzuführen, mit erfolgreichem Ergebnis..

Der Borderware Firewall Server ist gezielt auf einfache Bedienbarkeit konzipiert. Die Konfiguration läßt sich über ein Menüsystem vornehmen. Borderware ist das bislang einzige Produkt, das bereits über fertige Anwendungsserver für die wichtigsten Internet-Dienste verfügt, diese liegen allerdings auf der Firewall.

Checkpoint Firewall-1 verfügt über mehr Flexibilität als der Borderware Firewall Server. Außerdem besitzt sie eine grafische Oberfläche (GUI), dennoch erweist sich die Konfiguration als kompliziert.

Raptor Eagle ist ein Application Level Gateway, es sichert also auf Anwendungsebene. Die Vorteile von Eagle liegen in der breiten Plattformunterstützung sowie in der umfangreichen Funktionalität. Wie Firewall-1 ist auch Raptor Eagle ein System, das bei der Konfiguration entsprechendes Fachwissen erfordert.

TIS Gauntlet bietet von allen Firewall-Produkten die größte Flexibilität, ist aber in Bezug auf Implementation und Auditing am schwersten zu handhaben. Die Firewall-Software basiert auf dem als Freeware erhältlichen TIS Toolkit, integriert somit einen geprüften Code.

SCC Sidewinder bietet nur begrenzte Authentifikation und keinerlei Encryption.

Harris CyberGuard setzt auf sein eigenes Betriebssystem Harris Nighthawk auf, es ist als bisher einziges Firewall-System mit der ITSEC-Klasse B1 evaluiert worden.

ANS InterLock automatisiert im Gegensatz zu anderen Firewalls die Beseitigung der Forwarding-Mechanismen auf UNIX-Systemen.

Der Cisco PIX implementiert die Technologie der Network Address Translation in ein kompaktes Gerät, das im Gegensatz zu den anderen Firewall-Systemen nicht auf das als unsicher geltende UNIX aufsetzt. Die Installation des Gerätes reduziert sich auf ein Setup von wenigen Minuten. Ist es bei allen anderen Firewall-Produkten nötig, sich durch Software-Updates an den jeweils aktuellen Stand der Internet-Dienste anzupassen, so entfällt diese aufwendige und fehleranfällige Prozedur beim PIX (siehe auch Kapitel 5.2.3.).

Tabelle 4-5 faßt die wichtigsten Eigenschaften der gängigsten Firewall-Systeme zusammen. Bei den Performance-Angaben handelt es sich um Testergebnisse der Zeitschriften Datamation (*) und Data Comm Magazine (**).

Produkt	Technologie	True NAT	max.Anz. der User (*)	max. Anz. d. Verbind. (**)	Betriebssystem	Administration	Authent./ Token Support	Einstiegs- Preis (U.S. \$)
Cisco PIX	Network-Adress- Translation, anf. Appl.-Level-Gw.	Ja	Hundert- tausende	> 16000	eingebetteter Echtzeit-Kernel	Minuten-Setup, keine weitere Verwaltung, GUI	Neu	9.000 (PIX-32, inkl. HW)
Checkpoint Firewall-1	Packet-Filtering, Application-Lev.- Gateway	Neu	Mehrere Tausend	> 1000	Solaris, HP-UX	fortlaufende Verwaltung	Ja	11.000 (50 User, nur SW)
BNT BorderWare	Packet-Filtering, Circuit- u. Appl.- Level-Gateway	Nein	Wenige Hundert	k. A.	BSDI UNIX	fortlaufende Verwaltung	Ja	8.000 (inkl. PC)
Raptor Eagle	Application- Level-Gateway	Nein	Wenige Hundert	Wenige Hundert	SunOS, AIX, HP-UX, NT	fortlaufende Verwaltung	Ja	13.000 (inkl. SPARC)
TIS Gauntlet	Application- Level-Gateway	Nein	Wenige Hundert	Viele Hundert	BSDI UNIX, SunOS	fortlaufende Verwaltung	Ja	19.000 (inkl. PC)
SCC Sidewinder	Circuit- und Application- Level-Gateway	Nein	Wenige Hundert	> 1000	Modifiziertes BSDI	muß off-line verwaltet werden	Ja	30.000 (inkl. PC)
Harris CyberGuard	Packet-Filtering, Circuit- u. Appl.- Level-Gateway	Ja, jedoch kein. stat. Übersetz.	Wenige Hundert	> 1000	B1-bewertetes CX/SX UNIX	GUI	Ja	25.000
Sun SunScreen	Packet-Filtering	Nein	k. A.	k. A.	Solaris	mittels Windows- basierter Verw.-Station	Ja	68.000 (inkl. PC u. SPARC)
ANS InterLock	Application- Level-Gateway	Nein	Wenige Zehn	ca. 1000	Solaris oder AIX	aktive Beratung und Support durch Hersteller	Ja	42.500 (inkl. SUN- Miete)

Tabelle 4-5 : Vergleich von ausgewählten Firewall-Produkten

Die Zeitschrift Datamation bescheinigte außerdem allen Produkten einen kontinuierlichen Datendurchsatz von bis zu 40 Mbit/s bei der jeweils maximalen Anzahl gleichzeitiger Verbindungen [Freiss].

Zu Aussagen von Herstellern und Testlaboren hinsichtlich der Sicherheit sind zwei Punkte erwähnenswert:

Erstens finden diese Tests in speziellen Laboren statt, wo die Hardware-Plattformen von Fachleuten optimal konfiguriert wurden. Ein Käufer wendet aber kaum die gleiche Sorgfalt bei der Konfiguration an (oft mangels Wissen), da er davon ausgeht, daß ein Einspielen der Software genügt. Die Hersteller, die einen Support bieten, schneiden meist auch nicht besser ab. Daher können Testurteile über die Sicherheit meist nur auf die Software bezogen werden.

Zweitens werden für Testzwecke oft sog. Angriffs-Tools verwendet (z.B. SATAN) und dies dann vom Hersteller gesondert erwähnt. Solche und ähnliche veraltete Tools sind selbst bei einfachen Firewall-Systemen mittlerweile völlig wirkungslos [Lehle]. Daher ist zu empfehlen, sich ggf. nach aktuellen Tools umzusehen.

4.5. Entwicklungsstand auf ATM-Ebene

Bei der Realisierung von Sicherheitssystemen auf ATM-Ebene gibt es prinzipiell zwei Ansätze [Kyas]:

Der erste Ansatz basiert auf der Verschlüsselung auf ATM-Zellenebene mit Hilfe von Public-Key-Verfahren. Obwohl in Versuchen bereits die Verschlüsselung von ATM-Datenströmen bis 622 Mbit/s nachgewiesen wurde, gestaltet sich die durchgehende Verschlüsselung aller Zellen als schwierig. Dies will man umgehen, indem man lediglich die Verbindungsphase der Authentifikation verschlüsselt.

Der zweite Ansatz basiert auf der Realisierung auf Anwendungsebene. Hierbei ergibt sich das Problem der Neudefinierung der Protokolle. Beispielsweise unterstützen FTP oder HTTP innerhalb einer Session die Eröffnung mehrerer Prozeß-Ports. Die Modifizierung könnte dahingehend erfolgen, daß für die Eröffnung jedes einzelnen Prozeß-Ports ein eigener ATM-Signalisierungsaufbau erfolgt.

Die Firma Cisco Systems arbeitet an einer Architektur, die es ermöglicht, die Filterung von einzelnen ATM-Adressen in Switches zu implementieren. Diese Firewalls stellen dann das ATM-Äquivalent zu den Router-basierten Paketfiltern dar.

Ein endgültiger Standard für ATM-Sicherheitsmechanismen wird derzeit vom ATM Forum in der Spezifikation „Security 1.0“ erarbeitet.

In der Spezifikation wird die Sicherheit für alle drei Ebenen, die Benutzer- die Kontroll- und die Management-Ebene des B-ISDN-Referenzmodells, beschrieben. Dabei werden folgende Sicherheitsbausteine behandelt [Sheth]:

<u>Ebene</u>	<u>End-zu-Ende</u>	<u>Switch-zu-Switch</u>	<u>Ende-zu Switch</u>
Benutzer-Ebene	Authentifikation	Authentifikation	nicht definiert
	Vertraulichkeit	Vertraulichkeit	
	Integrität		
Kontroll-Ebene	Authentifikation	Authentifikation	Authentifikation
Management-Ebene	Authentifikation	Authentifikation	Authentifikation

Davon werden folgende Aufgaben im Detail behandelt:

- Zugangskontrolle
- Bestätigungsalgorithmen
- Schlüsselaustausch
- Verhandlung der Sicherheitsparameter

Als primäres Ziel gilt dabei die Implementierung von Authentifikations-Mechanismen auf Benutzer- und Kontrollebene. Dafür gibt es verschiedene Gründe: Für die Initialisierung eines sicheren Kanals ist die Authentifikation der wichtigste Schritt, denn nur so können häufig vorkommende Angriffe wie Vortäuschen einer falschen Herkunft, Leugnen eines Dienstes usw. eliminiert werden. Außerdem ist die Authentifikation ein wesentlicher Bestandteil der meisten o.g. Aufgaben, wie Schlüsselaustausch, Parameterverhandlung usw.. Ein weiterer Grund für den Schwerpunkt der Authentifikation sind die hohen Anforderungen an die Verschlüsselungsalgorithmen im ATM bezüglich der Geschwindigkeit. So wird eine weitestgehende Verlagerung von Vertraulichkeit und Integrität in die Hardware befürwortet.

Mit der Fertigstellung und Bekanntgabe der Spezifikation ist im August 1997 zu rechnen.

4.6. Sicherheitskonzepte in Beispielen

Im Rahmen des Deutschen Forschungsnetzes werden eine Reihe von Projekten zum Aufbau und zum Test von Sicherheitsstrukturen in wissenschaftlichen Einrichtungen betrieben und gefördert. Das reicht von der Anbindung der Verwaltungsrechner an das Hochschulnetz über eine Zwei-PC-Karten-Lösung (FH Wilhelmshaven) bis zur Erprobung von asymmetrischen kryptographischen Verfahren mit dem Ziel der sicheren Anbindung von entfernten Arbeitsplätzen an das Hochschulnetz (Fern-Uni Hagen). Hier handelt es sich jedoch ausschließlich um Eigenentwicklungen bzw. als Freeware erhältliche Lösungen, die hier nicht weiter behandelt werden sollen, da sie einen enormen Umfang haben und

daher auch einen beträchtlichen Administrationsaufwand hervorrufen. Außerdem liegt hier die Verantwortung gänzlich beim Anwender und es wird auch keinerlei Unterstützung angeboten.

Die Recherche über den kommerziellen Einsatz von Security-Systemen erwies sich für den Verfasser als schwieriger Weg. Dies hatte verschiedene Gründe:

1. Es ist kein konkretes Wissen auf dem Gebiet der IT-Sicherheit vorhanden.
2. Es gilt als nachteilig für die eigene Sicherheitssituation, konkrete Angaben über die eigene Netzstruktur zu machen.
3. Es ist aus wettbewerbstechnischen Gründen nicht sinnvoll, Wissen über dieses momentan aktuelle Thema preiszugeben.

Nachfolgende Auszüge aus Stellungnahmen auf den Messen „exponet“ und „Internet World“ Ende November 1996, die ganz im Zeichen von Sicherheit im Internet stand, belegen dies eindrucksvoll:

- „kein durchgängiges Firewallsystem, keine konkreten Angaben, kein Allgemeinrezept“ [Schäfers]
- „Sicherheit durch Trennung der Übertragungswege (ATM: PVCs; SDH: Zeitschlitz; andere Übertragungsleitungen)“ [Schul]
- „noch keine Entwicklung von ATM-Firewalls (noch keine Projekte; nicht sicher, ob IP für ATM verwendet)“ [Hansen]

Nachfolgend sind drei Beispiele für Sicherheitskonzepte in der Praxis erläutert. Das erste Beispiel befaßt sich mit der Anbindung eines Verwaltungsnetzes an ein Hochschulnetz mit dem Schwerpunkt der Paketfilterung. Hier hatte der Verfasser Gelegenheit, vor Ort zu recherchieren, mit freundlicher Unterstützung von [Vogel]. Daran anschließend wird ein Einsatz von vorwiegend auf der Applikationsebene operierenden Firewallsystemen in einem MAN gezeigt. Das dritte Beispiel beschreibt den Einsatz von Encryption-Systemen.

4.6.1. Datennetz der Technischen Hochschule Darmstadt

Einleitung

Die Technische Hochschule Darmstadt (THD) gehörte als Universität des Landes Hessen zu den ersten deutschen Einrichtungen, die einen direkten Anschluß an das weltweite Internet betrieben.

Die THD umfaßt als Mitglieder der Hochschule 330 Professoren, 1390 wissenschaftliche Mitarbeiter, 18000 Studenten sowie 1780 sonstige Mitarbeiter, diesen stehen derzeit ca. 4800 vernetzte Rechner zur Verfügung. Heute verfügt die THD über einen 34 Mbit/s-B-WIN-Anschluß mit dem Deutschen Forschungsnetz (DFN).

Innerhalb der THD, deren Institute über mehrere Standorte verteilt sind, wird vornehmlich Ethernet eingesetzt. Die einzelnen Ethernetsegmente sind durch Router abgetrennt. Die zentral gelegenen Router vom Typ Cisco 4000 bzw. 7000 sind untereinander über Glasfaser verbunden und bilden so einen FDDI- bzw. ATM-Backbone.

In der Verwaltung der THD besteht seit einiger Zeit ein eigenes Rechnernetz, an das die Arbeitsplätze der Verwaltungsmitarbeiter angeschlossen sind. Es hat sich sehr schnell der Bedarf herausgestellt, dieses Netz mit dem allgemeinen Hochschulnetz zu verbinden, um einerseits Kontakt mit den eigenen Instituten, Dekanaten zu ermöglichen und andererseits den Zugang zum Internet für die deutschland- und weltweite Tätigkeit der Hochschulverwaltung herzustellen.

Sicherheitsstrategie

Im folgenden soll die Art der Anbindung und der Aufbau des Verwaltungsnetzes kurz dargestellt werden [Vogel].

In der Verwaltung liegen zwei getrennte Netze vor, die über einen Router miteinander verbunden sind. Eines der beiden Netze ist über einen zweiten Router mit dem Hochschulnetz verbunden (siehe Bild 4-14).

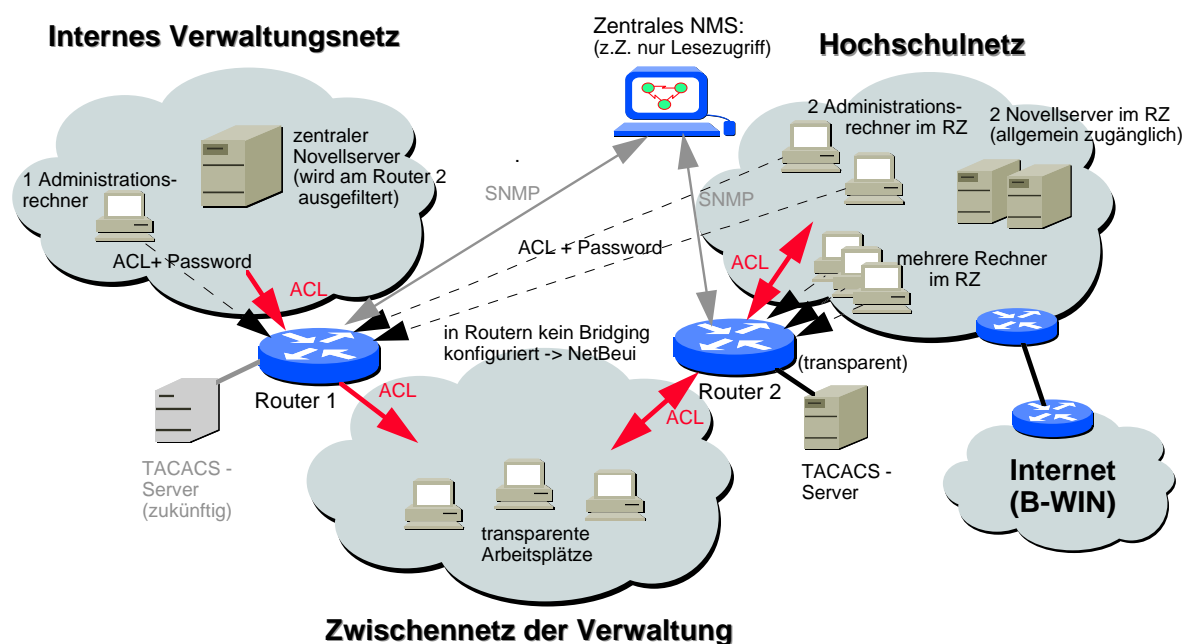


Bild 4-14 : Anbindung der Verwaltung an das Hochschulnetz der THD

Router 1 dient dediziert dem Abtrennen der internen Verwaltungsrechner vom restlichen Netz der Hochschule. Der Zugang auf diesen Rechner ist per Access-Liste nur von zwei Administrationsrechnern im Rechenzentrum und einem Rechner im internen Verwaltungsnetz aus möglich. Der Zugang selbst ist zusätzlich per Paßwort geschützt.

In Zukunft soll zusätzlich ein Dienst benutzt werden, der eine persönliche Identifikation über einen personenbezogenen Login-Mechanismus erlaubt. Dies soll mittels eines TACACS-Servers realisiert werden, der als externer Server auf einer UNIX-Maschine läuft. Die Einlog-Vorgänge werden dabei mitprotokolliert. Zusätzlich können dann über ein Log-File die Aktivitäten auf dem Router mitgeschrieben werden.

Der Zugang zum Router 2 erfolgt bereits über TACACS. Zusätzlich ist auch hier der Zugang nur von bestimmten Rechnern im HRZ möglich.

Beide Router sind in das zentrale Netzmanagement der TH Darmstadt integriert. Daher ist der Zugriff per SNMP für einige dedizierte Rechner freigegeben. Zur Zeit ist über diesen Weg nur lesender Zugriff erlaubt, so daß über diesen Weg keine Konfigurationsänderungen durchgeführt werden können.

Innerhalb des Verwaltungsnetzes werden an Protokollen TCP/IP, Novell IPX und NetBeui (Windows for Workgroups) verwendet.

Die beiden Verwaltungsnetze sind aus dem Gedanken heraus entstanden, daß eine Reihe von Arbeitsplätzen transparent im TH-Netz sein müssen. Von den restlichen Plätzen soll zwar prinzipiell ein Zugriff möglich sein, dieser wird jedoch auf bestimmte Dienste beschränkt.

Dementsprechend ist die Konfiguration auf Router 1 eingerichtet. Hingegen bindet Router 2 die Netze nur transparent in das Hochschulnetz ein. Damit ist vom Zwischennetz aus freier Zugriff auf alle Rechner innerhalb und außerhalb der Hochschule möglich.

Der Zugriff vom internen Verwaltungsnetz ist grundsätzlich nur gerichtet möglich: die Verbindung muß von einem Rechner aus dem internen Netz aufgebaut werden. Damit ist ein Zugriff seitens eines externen Rechners aus dem Hochschulnetz oder aus dem Internet verhindert, ausgenommen sind Zugänge zu zentralen Mail- und FTP-Servern.

Grundsätzlich ist der Zugang zu den UNIX-Servern der Verwaltung gesperrt.

Für alle Arbeitsplätze zugelassen sind folgende Dienste: Zugriff per Telnet auf Rechner innerhalb der Hochschule, Zugriff auf den NEWS- und Archie-Server der Hochschule und Zugang zum Gopher- und WWW-Service. Weiterhin ist der Zugriff auf die Time-Dienste und den Domain Name Service (DNS) zugelassen. Alle anderen Dienste sind per Access List verboten.

Im Verwaltungsnetz der TH Darmstadt wird für die Mitarbeiter ein zentraler Novellserver betrieben. Dieser ist sowohl vom Zwischennetz als auch vom internen Verwaltungsnetz erreichbar. Im restlichen Hochschulnetz ist er jedoch nicht sichtbar, da er am Router 2 herausgefiltert wird. Dagegen ist der Zugang zu den im Hochschulnetz angeschlossenen Novell-Servern seitens der Arbeitsplatzmaschinen

der Verwaltungsmitarbeiter gestattet (z.B. zur Softwarewartung). Damit ist zwar der Zugang zu den Daten und Informationen des Hochschulnetzes für die Verwaltung möglich, der Verwaltungsserver jedoch außerhalb des Verwaltungsnetzes nicht sichtbar und damit kann auf die dortigen Daten auch nicht zugegriffen werden.

Auf keinem der beiden Router ist Bridging konfiguriert. Damit wird das nicht routingfähige NetBeui-Protokoll lokal in den Segmenten gehalten, in denen es verwendet wird (internes Verwaltungsnetz). Die Daten sind daher nur innerhalb des Verwaltungsnetzes sichtbar. Ein Zugriff von außerhalb ist grundsätzlich nicht möglich.

Fazit

Diese effektive Lösung der Verwaltungsanbindung beruht auf dem vorteilhaften Umstand, daß sich innerhalb der Verwaltung zwei getrennte Netz befinden. Nennenswerte Angriffe sind bisher nicht zu verzeichnen gewesen. Lediglich Einlogversuche auf die zentralen Router wurden bisher registriert, diese konnten mittels des mitgeschriebenen Protokolls der Cisco-eigenen TACACS-Software nachgewiesen werden.

Dennoch hält man dieses Sicherheitskonzept keinesfalls für ausreichend. So wurde auf den Einsatz von Token Cards zur Administration bisher verzichtet. Das Konzept beruht derzeit lediglich auf Packet Filtering mittels Access Lists und Dauerpaßwörtern. Die momentane Beschränkung des SNMP-Zugriffs auf die Netzkomponenten kann auch keine dauerhafte Lösung darstellen.

Das Rechenzentrum muß die Beschaffung von Netzkomponenten vorwiegend in Eigeninitiative vornehmen. Weitere Beschaffungen müssen daher im Hochschulbereich gegenüber den Geldgebern sorgfältig begründet werden, was sich gerade auf dem Gebiet der Sicherheit als momentan wenig erfolgreich erweist. So ergab sich bei der Aufdeckung eines Angriffsversuches folgendes Bild: Die zuständigen Behörden fragten weder nach der Herkunft des Angriffs noch sahen sie sich genötigt, notwendige Konsequenzen einzuleiten - lediglich auf die exakte Einhaltung der Richtlinien bei der Bekanntgabe dieses Angriffes wurde besonderer Wert gelegt.

4.6.2. Berliner Landesnetz

Einleitung

Das Berliner Landesnetz umfaßt die Gesamtheit der Netzdienste im Sprach- und Datenbereich für die derzeit 75 Verwaltungsstandorte im Metropolitan Area Network (MAN) des Landes Berlin. In der Berliner Verwaltung werden auf 13 Großrechnern 20 Großverfahren betrieben, auf 199

Abteilungsrechnern laufen ca. 2800 Einzelverfahren. Über 300 LANs sind installiert, an über 20000 Endgeräten arbeiten ca. 24000 Mitarbeiter.

Für die ressortübergreifende IT-Koordinierung im Land Berlin und für damit verbundene Grundsatzfragen ist die Senatsverwaltung für Inneres zuständig. Eine ihr nachgeordnete Behörde ist das Landesamt für Informationstechnik (LIT), das für die technischen Belange im Berliner Landesnetz zuständig ist. Ein unter Führung des LIT gebildeter Arbeitskreis Netzsicherheit (AKS) ist hierbei für die Sicherheitsstrategie in der Berliner Verwaltung verantwortlich.

Sicherheitsstrategie

Das geplante Sicherheitskonzept des LIT sieht eine Teilung der Berliner Verwaltung in ein offenes (OVN) und ein geschlossenes Verwaltungsnetz (GVN) vor [Biedka]. Dabei sollen auch innerhalb dieser beiden Netze Firewall-Systeme errichtet werden, die wiederum verschiedene Subnetze mit unterschiedlicher Sicherheitsrelevanz trennen (siehe Bild 4-15 [Biedka]).

Die geringste Schutzbedürftigkeit besitzen demnach die offenen Verwaltungsnetze (hierin fällt auch der von außen zugängliche Public Server), diese sind trotzdem durch eine Firewall (OVN-FW) vom Internet getrennt, da sich z.B. auf den Public Servern nichtöffentliche Wahlergebnisse befinden. Die Schulen, Bibliotheken und Theater bilden ihrerseits ein Offenes Subnetz (OSN), dieses ist durch eine eigene Firewall vom OVN getrennt. Ein vom Internet kommender Angreifer müßte hierbei also bereits zwei Firewall-Systeme überwinden. Ähnlich verhält es sich mit dem internen Geschlossenen Verwaltungsnetz (GVN), mit dem Unterschied, daß hier eine wesentlich höhere Schutzbedürftigkeit vorliegt als beim OSN. So liegt es auf der Hand, daß der GVN-Firewall (GVN-FW) auf einem höheren Niveau kontrollieren muß als der OSN-Firewall (OSN-FW).

Die verschiedenen Behörden-Subnetze (BSN) werden wiederum durch eigene interne Firewalls (BSN-FW) vom allgemeinen GVN abgeschildert. So ist ein Behörden-Subnetz bereits durch drei verschiedene Barrieren vom Internet abgeschildert.

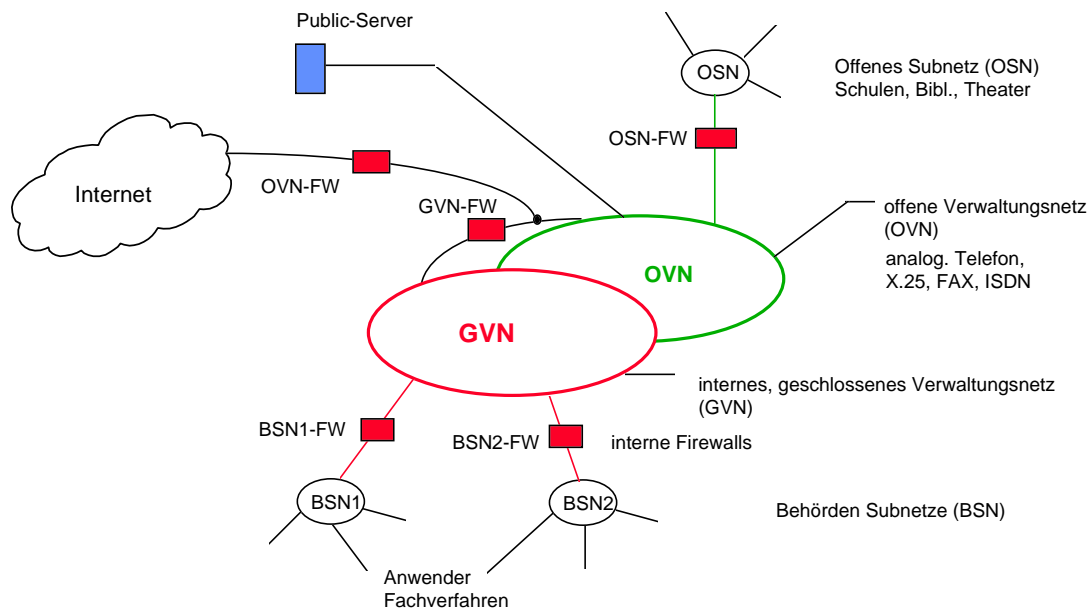


Bild 4-15 : Gestaffelte Firewall-Anordnung im Berliner Landesnetz

Bild 4-16 geht auf die Plazierung der verschiedenen Server ein [Biedka]. So wird der externe Domain Name Server (DNS) für die Domänen „berlin.de“ und „schule.de“ im öffentlichen Verwaltungsnetz angeordnet, dasselbe gilt für den Public Server (PS). Der interne DNS-Server für die Zuordnung der internen Komponenten (IP-Adressen) zur Domäne „verwalt-berlin.de“ befindet sich logischerweise im Strang des geschlossenen Verwaltungsnetzes. Durch einen Remote Access Server (RAS) wird die Einwahlmöglichkeit für physisch getrennte Standorte bzw. mobile Nutzer, sowohl auf analogem als auch auf digitalem Wege, ermöglicht. Hierzu zählen Schulen, einzelne Abgeordnete und Fremdfirmen. Die physische Anbindung des RAS im offenen Verwaltungsnetz stellt sicher, daß einem Nutzer bei erfolgreicher Einwahl, ob befugt oder unbefugt, zunächst nur das bezüglich Sicherheitsrelevanz geringer eingestufte OVN-Netz offensteht.

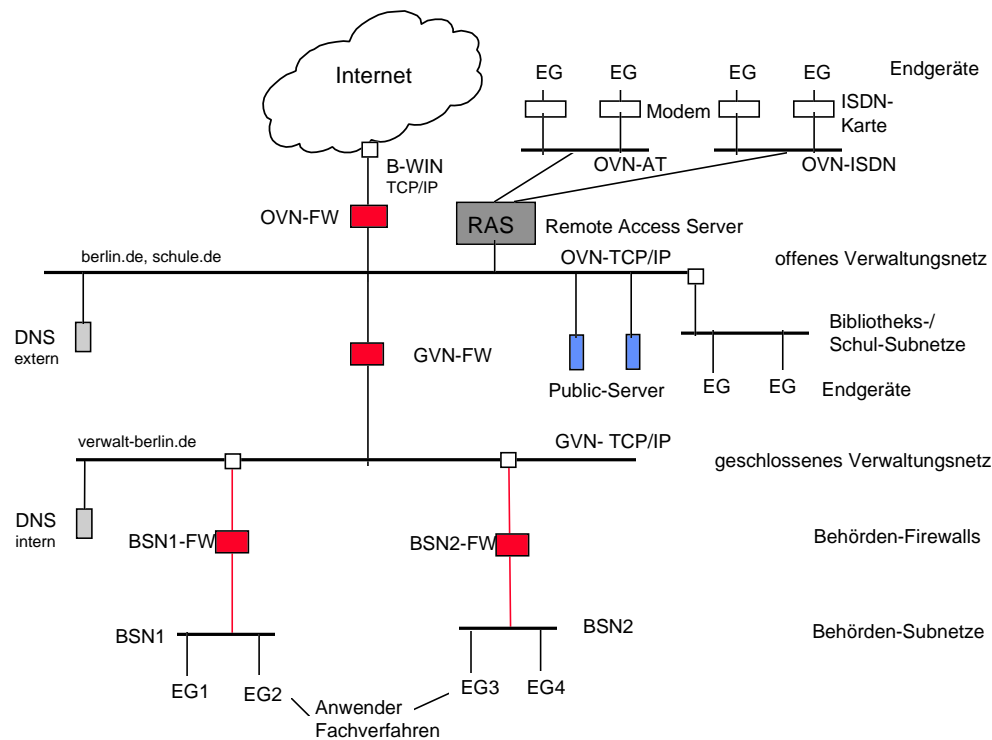


Bild 4-16 : Anordnung der Server im Berliner Landesnetz

Testnetz

Bevor das vorgestellte Sicherheitskonzept im Berliner Landesnetz zu Einsatz kommt, werden derzeit geeignete Firewall-Systeme für die speziellen Bedürfnisse des Landesnetzes getestet. In der Sicherheitsstruktur sollen verschiedene Firewall-Systeme gleichzeitig zum Einsatz kommen, da dies für Netze mit sehr hohem Schutzbedarf in den Anforderungen des BSI formuliert ist. Zur Erprobung der Firewall-Systeme wurde ein Testnetz entworfen, das die verschiedenen Netzebenen des Landesnetzes repräsentieren soll (Bild 4-17 [Biedka]). Neben den auf dem Markt verfügbaren und von der NCSA zertifizierten Produkten Borderware, Firewall-1 und Eagle kommt hier auch eine Eigenentwicklung BAS zum Einsatz, worauf jedoch nicht weiter eingegangen wird.

- Erprobung von ausgewählten Einzelfunktionen der Firewalls nach Szenario
- Überprüfung der Durchlässigkeit für spezielle Dienste
- Feststellen von Unterschieden der in den Firewalls implementierten Sicherheitspolitik
- Aufwandseinschätzung für Installation, Konfiguration, Überwachung und Auswertung
- Überprüfung der Verträglichkeit der kaskadierten Firewalls beim Durchgang zugelassener Dienste
- Erprobung der Authentifizierung und Verschlüsselung in gestaffelten Firewall-Systemen

Fazit

Da die Evaluierung noch nicht abgeschlossen ist, konnten noch keine konkreten Ergebnisse zu den einzelnen Firewall-Systemen übermittelt werden. Man ist sich jedoch einig, daß zu Aufbau und Konfiguration der Firewall-Systeme umfassende Netz- und UNIX-Kenntnisse erforderlich sind. Allerdings wurden bisher Performancefragen nicht berücksichtigt.

Das LIT sieht in dem Einsatz von verschiedenen Firewall-Systemen eine hohe Notwendigkeit, obwohl dies einen beträchtlichen Administrationsaufwand bedeutet. Den Vorteil hierbei sieht man in der hohen Flexibilität der einsetzbaren Sicherheitsregeln. Man ist der Ansicht, mittels Remote-Administration (Verwaltung aller Firewall-Systeme von einem Ort aus) den Administrationsaufwand in Grenzen halten zu können.

Das Durchschleusen authentisierter Dienste war jedoch nicht immer möglich, die Lösung sucht man in einer Authentisierung beim ersten Firewall und einem Durchreichen bei den nachfolgenden Firewalls. Auch die Auswertung von Log-Vorgängen war bei allen Produkten verbesserungswürdig, vielfach konnten die Log-Files nicht ausgedruckt werden.

Eine mit der jetzigen Firewall-Technologie nicht zu lösende Anforderung ist die Überwachung von RPC-basierten Client/Server-Anwendungen, bei denen nach Client-Anfrage vom Server dynamische Portnummern vergeben werden. Hierzu müßten noch speziell zugeschnittene Proxy-Programme implementiert werden.

Außerdem hatte man zunächst keinen Zugang zu einem DNS vorgesehen, so daß alle Adreßeinstellungen mit der Hand vorgenommen werden mußten.

Die Vorgehensweise des LIT ist beispielhaft für das schrittweise Vorgehen bei der Implementierung eines wirkungsvollen Sicherheitssystems und bildete bei den Recherche-Bemühungen des Verfassers bezüglich Entgegenkommen und Offenheit die Ausnahme.

4.6.3. Encryption-Systeme

Berliner Kliniken

Die Berliner Kliniken setzen im großen Maße Geräte der Firma GRETAG (AT&T) ein, die eine Ende-zu-Ende-Verschlüsselung gewährleisten [Renneberg]. So wird es vereinzelt Arbeitsgruppen, die sicherheitsrelevante Daten bearbeiten und verwalten, ermöglicht, über ein gemeinsames unsicheres Netz miteinander zu kommunizieren. Bild 4-18 zeigt einen Auszug daraus.

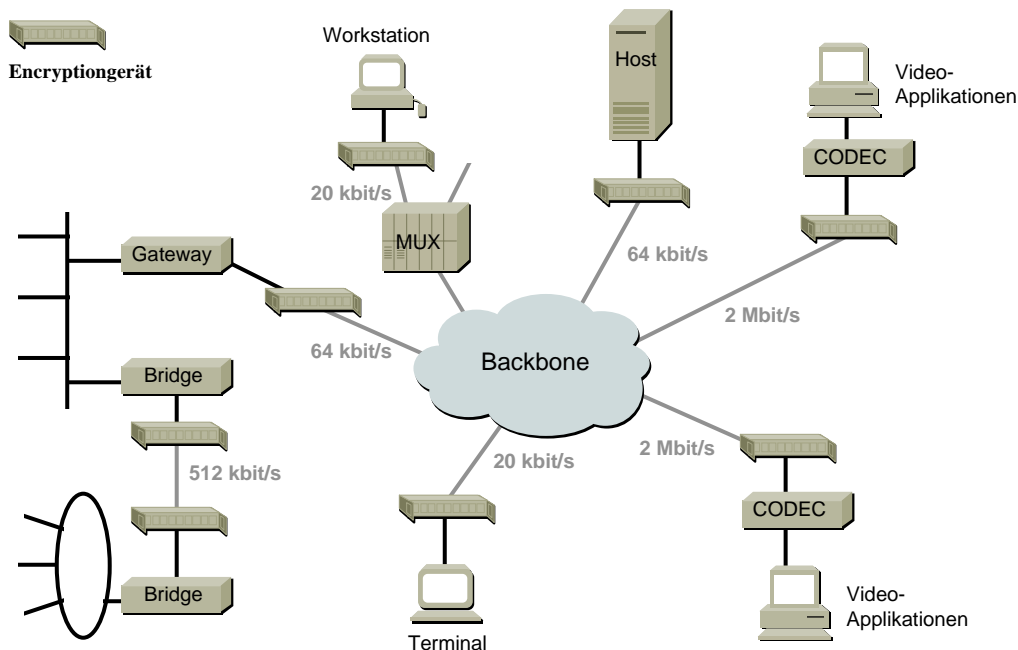


Bild 4-18 : Einsatz von Encryptiongeräten in den Berliner Kliniken

Dabei werden je nach Anwendung Chiffriergeräte mit unterschiedlichen Geschwindigkeiten eingesetzt, die jedoch miteinander kompatibel sind. Die verwendeten Geräte der Reihe GRETACODER bieten hierbei den Vorteil, daß der Einsatz ohne Änderung der bestehenden Software oder Protokolle geschieht. So konnten die bestehenden Netzkonfigurationen beibehalten werden.

Die Encryption erfolgt durch symmetrische Verfahren, entweder auf Basis des DES-Standards (56 Bit-Schlüssel) oder einer proprietären Block-Chiffrierung (128 Bit-Schlüssel). Der Austausch der Geheimschlüssel erfolgt automatisch über exponierte Kanäle, die Abspeicherung geschieht chiffriert in einem Sicherheitsmodul, das nur über ein manuelles Schloß oder Eingabe einer PIN zugänglich ist. Einstellung und Konfiguration können über eine menügesteuerte Anzeige vorgenommen werden, ein integrierter Selbsttest ermöglicht die Fehlereinkreisung.

Weitere Beispiele

Die Firma KryptoKom setzt in einigen Bundesbehörden sowie in den Universitäten in Jena, München, Nürnberg eigene Krypto-Boxen ein. Damit sollen lokale Netze vor unbefugtem Eindringen geschützt

werden sowie Daten verschlüsselt werden, die zwischen zwei voneinander getrennten LAN-Segmenten über den ungesicherten Backbone übertragen werden.

Weiterhin sollen sämtliche Hochschulen in Nordrhein-Westfalen bis Ende 1997 diese Produkte einsetzen, in Hamburg werden demnächst Testaufbauten installiert.

Der mit den KryptoKom-Produkten erreichbare Durchsatz beträgt bis zu 9,6 Mbit/s [Havers].