EIN SICHERHEITSKONZEPT

Seminararbeit im Rahmen des
Wirtschaftsinformatik-Seminars Sommersemester 1998

Thema Nr. 3

vorgelegt am Betriebswirtschaftlichen Institut der Universität Stuttgart,
Abteilung VII,
Allgemeine Betriebswirtschaftslehre und Wirtschaftsinformatik

Inhaltsverzeichnis Seite

Abkürzungsverzeichnis

ATM	Asynchronous Transfer Mode
DFÜ	Datenfernübertragung
FDDI	Fiber Distributed Data Interface
FTP	File Transfer Protocol
i.d.R.	in der Regel
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPX	Internet Package Exchange
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
IT	Informationstechnik
IV	Informationsverarbeitung
LAN	Local Area Network
OSI	Open Systems Interconnection
SMTP	Simple Mail Transport Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WAN	Wide Area Network
WWW	World Wide Web

Abbildungsverzeichnis ..... Seite

1. Einleitung

IV-Sicherheit ist ein wichtiges und trotzdem oft unterbewertetes Thema vieler Unternehmen. Optimale Sicherheit erfordert ständig neue Planungen und Änderungen, die die Finanzmittel und das Know-how stark beanspruchen. In dieser Arbeit sollen nach einer Themen- und Begriffseinführung in die Thematik der IV-Sicherheit verschiedene Sicherheitskonzepte vorgestellt werden. Anschließend wird auf spezielle Sicherheitsbedürfnisse eingegangen, die Schwerpunkte liegen hierbei auf der Identifikation und Beseitigung von Schwachstellen der bisherigen IV-Landschaft, auf der Einrichtung und Konfiguration von innerbetrieblichen Firewalls und den Chancen und Risiken einer Internet-Anbindung. Dabei soll die finanzielle Seite keinesfalls außer Acht gelassen werden.
Da eine detaillierte Analyse aller der hier zu berücksichtigenden Faktoren den zur Verfügung stehenden Rahmen sprengen würde, wird zur weiteren Vertiefung auf die einschlägige Fachliteratur verwiesen.

2. Sicherheit in der netzwerkunterstützten Informationsverarbeitung[1]

2.1 Grundbegriffe

Sicherheit in der Informationsverarbeitung läßt sich zum Einen als 'Ordnungsmäßigkeit' definieren[2], worunter man allerdings noch mehrere verschiedene Teilbereiche versteht:

- Funktionsgarantie (Vorsorge vor technischem Ausfall),
- Kontroll- und Revisionsmöglichkeiten (Erkennen von Bedienungs- und Systemfehlern, um diese Fehler nachvollziehen zu können),
- Qualitätssicherung und
- Rechtssicherheit (vor allem zur (Produkt-) Haftung).

Im Gegensatz zur verfahrensbezogenen Ordnungsmäßigkeit befaßt sich die 'IT-Sicherheit' mit dem Schutz gegenüber Manipulationsversuchen in einem IT-System, betrachtet also Daten oder Dateien und ist damit objektbezogen. Die Summe dieser beiden Eigenschaften faßt man schließlich unter dem Begriff der 'IV-Sicherheit' zusammen, deren oberstes Ziel es ist, die Qualität der Informationsverarbeitung zu verbessern.

---

1 anschaulich und detailliert erklärt vom BSI (1997), http://www.bsi.bund.de/gshb/deutsch/menue.htm
2 s. Kersten (1995), S. 72ff

Die Grundziele der Informationsverarbeitung sind[3]:

- die Verfügbarkeit von Daten, Dienstleistungen und Maschinen, sobald ein autorisierter Benutzer Zugriff auf sie haben will. Der kontinuierliche Zugriff auf Daten und Ressourcen muß gewährleistet sein.
- die Unversehrtheit (Integrität) von Daten und Systemen, damit Manipulationen ausgeschlossen werden können. Daten dürfen nur auf vorherbestimmte Art und Weise von autorisierten Personen abgeändert werden können.
- die Verbindlichkeit von Daten und Dienstleistungen, um eine juristische Akzeptanz in den elektronischen Verfahren zu gewährleisten.
- die Vertraulichkeit von Informationen – kein Unberechtigter darf Zugriff auf Informationen bekommen können, dies wird nur befugten Personen gestattet.

Der Zeitraum, innerhalb dem eine Verletzung dieser Ziele bemerkt wird, ist hier von großer Bedeutung[4]. Ein Verlust der Verfügbarkeit wird i.d.R. sofort bemerkt, eine Verletzung der Integrität dagegen erst mit zeitlicher Verzögerung – nämlich sobald sich auffällig falsche Ergebnisse oder ein abnormales Systemverhalten einstellen. Bei der Verbindlichkeit wird ein Verlust erst im Streitfall relevant, bei der Vertraulichkeit wird eine Verletzung vielleicht gar nie bemerkt.

Es ist also wichtig, Bedrohungen, Risiken und Schäden zu kennen, zu analysieren und zu dokumentieren, um sie klassifizieren zu können. Bedrohungen führen zu Schwachstellen, diese Schwachstellen bedeuten Risiken, die wiederum Schäden verursachen können. Gibt es z.B. für jemanden eine Möglichkeit, ein System unerlaubt zu benutzen, so hat dieses System eine Schwachstelle. Leider wird hier immer ein Restrisiko bleiben, eine absolute Sicherheit wird es in dem sehr dynamischen IT-Bereich wohl nie geben. Dieses Restrisiko gilt es also auf ein erträgliches Maß zu minimieren, so daß es als unwahrscheinlich angesehen werden kann, daß jemand innerhalb einer kritischen Zeit die Sicherheit des Systems oder Teilen davon bedrohen kann. Auch die Fragen, was ein neues Türschloß oder eine neue Alarmanlage kosten, werden der Überlegung gegenübergestellt, wie groß das Risiko ist, daß diese auch notwendig werden.

2.2 Sicherheitsfunktionen und Sicherheitsmechanismen

Eine Sicherheitsfunktion macht die Bedrohung eines IT-Systems unwirksam oder kann zumindest die Auswirkungen im Schadensfall begrenzen. Das dahinter stehende Verfahren oder den mathematischen Algorithmus nennt man Sicherheitsmechanismus. Unbefugte Benutzer müssen ferngehalten werden, Anmeldeversuche und die (versuchte) Ausübung von Rechten müssen mittels Protokollie-

[3] vgl. Stallings (1995), S. 24ff
[4] s. Kersten (1995), S. 74

rung[5] festgehalten werden. Es müssen Zugriffsrechte vergeben und diese Vergaben geprüft werden, die Speicher müssen wiederaufbereitet werden, die Betriebsystemintegrität und die Übertragungssicherheit auf dem Transportsystem müssen gewahrt werden.

Eine Funktion gibt also an, *was* gemacht werden soll und der dazugehörige Mechanismus beschreibt, *wie* es geleistet werden soll. Ein Mechanismus ist um so sicherer, je nachdem, welche Kenntnisse, welcher zeitliche, finanzielle und personelle Aufwand und welche Hilfsmittel notwendig sind, um den Mechanismus zu "brechen". Das schwächste Glied in der Kette muß verbessert werden, oder durch andere Mechanismen kompensiert werden. An dieser Stelle sollen verschiedene Sicherheitsfunktionen[6] vorgestellt werden:

- Identifizierung (Bestimmung der Identität eines Subjekts): Die Identität wird durch das Subjekt selbst verifiziert oder durch ein technisch-administratives Verfahren ermittelt. Die Identifizierung des Benutzers gegenüber dem System ist insofern sinnvoll, indem sie es dem System ermöglicht, dem Benutzer auf bestimmte Information Zugriff zu gestatten oder zu verweigern. Außerdem ermöglicht sie eine Aufzeichnung der Datenzugriffe eines Benutzers.
- Authentisierung (Nachweis einer Identität): Hier muß – im Rahmen der Möglichkeiten – der Nachweis erbracht werden, ob das Subjekt tatsächlich genau dasjenige ist, für das es sich ausgegeben hat. Zur Überprüfung der Benutzeridentität wird ein Merkmal abgefragt, von dem der Benutzer Kenntnis hat (Paßwort), das er besitzt (Magnetkarte) oder das eine Eigenschaft des Benutzers eindeutig zuordnet (Fingerabdruck, Netzhaut). Die so gewonnenen Authentisierungsinformationen sollen vor unberechtigten Zugriffen und unbefugter Kenntnisnahme geschützt sein. Der Benutzer seinerseits muß allerdings sicher sein können, daß die Aufforderung zur Identifizierung auch wirklich direkt vom gewünschten System stammt und nicht etwa von einem anderen, welches in betrügerischer Absicht Kennwörter aufzeichnet, um sie für spätere Manipulationen zu verwenden[7]. Kerberos[8] hat sich als Authentifizierungssystem in der Praxis bewährt[9]. Eine sehr einfache und wirkungsvolle Möglichkeit, das Abhören und Aufzeichnen von Paßwörtern sinnlos zu machen, ist die Verwendung von Einmalpaßwörtern[10]: Die Benutzer bekommen eine Liste mit Paßwörtern, die sie jeweils nur einmal verwenden können. Wenn das System entsprechend so konfiguriert ist, daß sich ein Benutzer grundsätzlich nur einmal anmelden kann und die Paßwort-

---

5 sog. "Audit"

6 vgl. Kersten (1995), S. 87ff, ergänzend Reiser (1998), S. 159ff

7 diese Programme werden als "Sniffer" bezeichnet, vgl. Cheswick / Bellovin (1996), S. 192

8 Kerberos ist ein netzweites Authentifizierungssystem des MIT für physikalisch unsichere Netze. Mit ihm können mehrere Parteien über ein Netz kommunizieren und gegenseitig ihre Identität beweisen, ohne daß Angriffe über Abhören des Netzes oder Wiederholung von Datenpaketen möglich wären. Außerdem werden die Integrität des Datenstroms und Geheimhaltung mit kryptographischen Verfahren garantiert.

9 s. Siyan / Hare (1995), S. 105ff

10 vgl. Cheswick / Bellovin (1996), S. 142

listen ausschließlich persönlich an die berechtigten Personen vergeben werden, kann ein Mißbrauch nahezu vollständig ausgeschlossen werden. Die potentielle Bedrohung dieses Systems liegt hierbei vor allem wieder beim Benutzer, wenn z.B. die Paßwortlisten ungesichert auf dem Schreibtisch oder in einer der zuletzt geöffneten unverschlüsselten Tabellendateien liegen.

- Zugriffskontrolle (Überprüfung, ob ein bestimmtes Subjekt berechtigt ist, eine bestimmte Aktion mit einem Objekt durchzuführen): Verhinderung von unbefugten Aktionen, darunter fallen neben Lese- und Schreibzugriffen, der Erzeugung oder Löschung von Objekten und Weitergabe von Zugriffsrechten auch die Anforderungen von Betriebsmitteln (Speicherplatz und Prozessorzeiten dürfen nicht überbeansprucht werden). Diese Rechte können nur der Besitzer (Erzeuger) und der Systemverwalter vergeben. Es müssen Regeln für die Kontrolle von Zugriffen aufgestellt werden, an die sich sowohl Benutzer als auch Administrator halten müssen, damit kein Wildwuchs entsteht. Eine unkomprimierte Zugriffskontrollmatrix ist dabei nur für sehr kleine und überschaubare IV-Landschaften geeignet, da sie sehr groß werden kann und unnötig Ressourcen beansprucht. Eine Vereinfachung durch die Aufteilung der Matrix in Benutzergruppen (User-Level) und Objektgruppen (Laufwerke / Verzeichnisse, Zugriffsprofile) schafft hier Übersichtlichkeit und Performancevorteile. Eine weitergehendere Möglichkeit der Zugriffskontrolle ist das Schutzklassen-Konzept[11], bei dem nur Benutzer mit derselben oder einer höheren Schutzklasse auf eine Datei einer bestimmten Schutzklasse zugreifen dürfen. Eine (notwendigerweise lineare) Skala würde z.B. von 'offen' über 'nur für den Dienstgebrauch', 'vertraulich' und 'geheim' bis hin zu 'streng geheim' gehen.
- Beweissicherung und Protokollauswertung (Protokollierung der (versuchten) Ausübung von Rechten und Entdeckung sicherheitsrelevanter Ereignisse): Benutzeraktionen werden in Protokollen aufgezeichnet, um die Benutzer für ihre Handlungen verantwortlich machen zu können. Durch die Auswertung der Protokolle werden Sicherheitsverstöße aufgezeigt, insbesondere die versuchte Ausübung nicht zugestandener Rechte.
- Wiederaufbereitung (Aufbereitung wiederverwendbarer Speicher vor dem nächsten Gebrauch): Ein unerlaubter Informationsfluß durch nicht ordnungsgemäß gelöschte Daten auf Speichermedien muß verhindert werden.
- Unverfälschtheit (Gewährleistung der Korrektheit und Konsistenz von Daten und Relationen): Die Sicherheit und Integrität der Datenübertragung müssen gewährleistet sein.
- Verfügbarkeit, Verläßlichkeit, Zuverlässigkeit: Ein definiertes Verfahren wird inhaltlich und zeitlich wie geplant ablaufen. Dabei muß die Funktionalität zu jedem gewünschten Zeitpunkt verfügbar

[11] vgl. Kersten (1995), S. 111ff

sein, Dienstleistungen müssen zu einem gewünschten Zeitpunkt oder innerhalb gewünschter Zeit erbracht werden. Fehler werden an der Quelle oder zu einem möglichst frühen Zeitpunkt an ihren Auswirkungen erkannt, weiteres Fehlverhalten wird vermieden oder begrenzt und der Fehler wird an der Quelle behoben, um eine weitere verlustfreie Verarbeitung gewährleisten zu können.

- Übertragungssicherung (Sicherung von Daten beim Transport auf Übertragungswegen): Hier wird besonderer Wert auf Vertraulichkeit und Integrität bei einer Datenübertragung gelegt. Es muß verhindert werden, daß Unbefugte Einsicht in oder Zugriff auf Daten erhalten und diese unter Umständen sogar ändern können. Für eine verbindliche Datenübertragung muß gewährleistet sein, daß ausschließlich die gewünschten Partner die während der Übertragung geheimgehaltenen Daten zweifelsfrei über nachvollziehbare und unverfälschbare Wege erhalten.

Die Sicherheitsfunktionen und Sicherheitsmechanismen werden in sog. Sicherheitsklassen[12] eingestuft, in der die Qualität der Sicherheit beurteilt wird. Um die Sicherheit auf Hardwareseite gewährleisten zu können, muß als Grundvoraussetzung der physikalische Zugriff auf Netzwerkkomponenten (Kabel, Hubs, Switches, Verteilerschränke u.a.) verhindert werden[13], da hier leicht identifizierbare Daten ohne große technische Schwierigkeiten abgehört werden können.

2.3 Kryptographie und Verschlüsselungsverfahren[14]

Vertrauliche Daten, besonders die des Managements, sollten sowohl auf lokalen Datenträgern als auch auf Netzwerklaufwerken verschlüsselt abgelegt werden. Eine verschlüsselte Paßwortübertragung wäre auf jeden Fall angebracht, vor allem bei der Datenübertragung via Modem oder ISDN über ansonsten ungeschützte Telefonleitungen[15].

Durch den Einsatz von Verschlüsselungsverfahren kann die Integrität der Daten, deren Vertraulichkeit bei der Übermittlung und die Authentizität des Absenders sichergestellt werden. Früher wurden meist symmetrische Verfahren eingesetzt, dabei müssen alle Teilnehmer paarweise Schlüssel miteinander vereinbaren. Der Bedarf an Schlüsseln steigt aber hier mit der Zahl der Teilnehmer überproportional an, n Teilnehmer benötigen (n*(n-1)/2) Schlüssel. Schon bei 50 Teilnehmern müssen 1225 verschiedene Schlüssel generiert und zu jedem Teilnehmer 49 Schlüssel übertragen werden. Außerdem muß hier jedesmal eine absolut sichere Übertragung der Schlüssel gewählt werden und natürlich müssen die Schlüssel absolut geheim verwaltet werden. Es wird schnell klar, daß dieses Verfahren schon bei wenigen Teilnehmern einen untragbaren Aufwand bedeutet und eine unverhältnismäßig große Administration notwendig macht. Mittlerweile geht der Trend zu asymmetrischen Verschlüsse-

---

[12] nationale und internationale Funktionalitätsklassen können im Detail nachgelesen werden bei Kersten (1995), S. 120ff, siehe auch die Anwendung dieser Klassen ebenda auf S. 137ff, weitere Standards s. Kyas (1998), S. 311ff

[13] vgl. Kyas (1998), S. 237f

[14] s. Stallings (1995), S. 37ff

[15] s. Kyas (1998), S. 285ff und Reiser (1998), S. 98ff

lungsverfahren (*public key*-Verfahren), dafür ist allerdings eine Schlüsselzentrale notwendig, die an jeden Benutzer ein Schlüsselpaar ausgibt und verwaltet. Der eine Schlüssel wird als privater Schlüssel bezeichnet, dieser wird vom Besitzer geheimgehalten, während der andere, der sog. öffentliche Schlüssel, bekanntgegeben werden darf. Damit entfällt die Notwendigkeit für die Kommunikationspartner, einen geheimen privaten Schlüssel außer dem eigenen zu kennen und unter Verschluß zu halten. Das Verfahren dient zum einen der Verschlüsselung von Informationen[16] bei der Übertragung zwischen Sender und Empfänger. Der Sender verwendet den öffentlichen Schlüssel des Empfängers, nur er kann mit seinem privaten Schlüssel die Nachricht lesen:

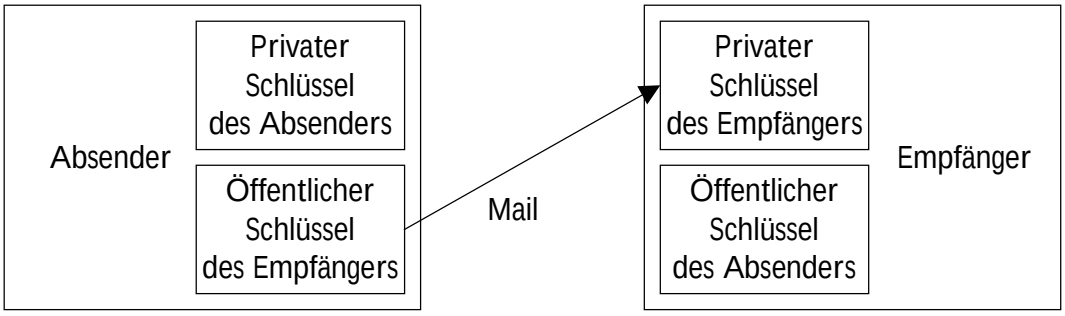

Abbildung 1: Codierung von Nachrichten[17]

Man kann damit aber auch Nachrichten digital signieren[18], also mit einer eindeutigen Unterschrift versehen. Die Nachricht wird vom Absender mit seinem privaten Schlüssel kodiert und kann nur mit seinem öffentlichen Schlüssel dekodiert werden. Damit wird dem Empfänger die Möglichkeit gegeben, sicherzustellen, daß der Absender wirklich der vorgegebene ist:

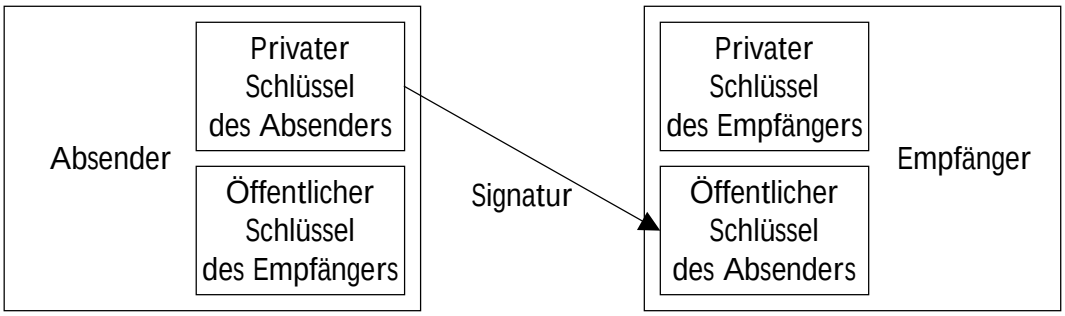

Abbildung 2: Signatur von Nachrichten[19]

Öffentliche Schlüssel sind also einfacher zu handhaben und mit weniger Aufwand zu nutzen. Außerdem ermöglichen sie nicht nur eine Codierung, sondern auch eine Signatur, was bei symmetrischen Verfahren prinzipiell nicht möglich ist. Dabei leidet aber die Geschwindigkeit - auch die besten Algorithmen für öffentliche Schlüssel sind aufgrund der relativ komplexen mathematischen Konzepte we-

[16] vgl. Heuser (1996), S. 12
[17] s. Kuppinger (1998), S. 118
[18] vgl. Heuser (1996), S. 12
[19] s. Kuppinger (1998), S. 119

sentlich langsamer als gängige Methoden, die auf privaten Schlüsseln aufsetzen. Aufgrund des CCITT-Standards X.509 ist ein unternehmensübergreifender, weltweiter sicherer Datentransfer gewährleistet. Durch ein Zertifikat des Servers, von dem der öffentliche Schlüssel kommt (das wiederum mit dem privaten Schlüssel der Zertifizierungsstelle verschlüsselt ist und nur mit deren öffentlichen Schlüssel lesbar ist), wird die Echtheit der öffentlichen Schlüssel von diesem Server gewährleistet. X.509 wird mittlerweile von allen gängigen Browsern, Internet-Servern und auch von verschiedenen Sicherheitsprotokollen genutzt[20].

Bei häufigem Datenaustausch zwischen zwei oder nur nur wenigen Partnern sollte aber aus Performancegründen ein symmetrisches Verfahren eingesetzt werden.

2.4 Systementwicklung und Evaluierung

Schon bei der Entwicklung eines Systems und seiner Komponenten wird der Grundstein für Sicherheit gelegt, das zentrale Anliegen bei allen Qualitätsaspekten ist die korrekte Funktionsweise von Hard- und Software. Wenn aber keine korrekt ablaufenden Sicherheitsfunktionen gegeben sind, kann Sicherheit nicht eintreten und wenn die Systeme inkorrekt arbeiten, kann keine Ordnungsmäßigkeit eintreten. Und es sind meist Kleinigkeiten, die eklatante Sicherheitslücken darstellen, weil sie erst zuletzt bemerkt und beseitigt werden. Aber auch ein ordnungsgemäßer Entwicklungsprozeß, wie z.B. nach ISO 9000, kann zu einem unsicheren Produkt führen, hier sei Microsoft mit seinen zahlreichen nachgereichten Hotfixes und Service Releases nur am Rande erwähnt[21].

Zur Prüfung von IT-Produkten und IT-Systemen gibt es neben der Qualitätssicherung die sog. Evaluierung[22], sie dient gegenüber der Konformitätsprüfung[23] dem Ausschluß von Sicherheitslücken gegenüber den potentiellen Bedrohungen. Die Evaluierung prüft, ob die erforderliche Systemsicherheit beim vorliegenden Produkt gegeben ist, sie ist aber ausschließlich für die getestete Release[24] gültig. Beim fertigen Produkt wird nur stichprobenartig geprüft, da bereits bei einfachen PC-Produkten, aber erst recht bei großen Betriebssystemen, wegen der Komplexität und des Umfangs eine vollständige und detaillierte Prüfung i.d.R. nicht möglich ist. Prinzipiell ist eine dermaßen umfangreiche Prüfung auch nicht notwendig, eine Beschränkung auf einzelne sicherheitsrelevante Programmteile genügt völlig. Da diese meist untrennbar mit dem Rest verbunden sind, sind sie als Ganzes kaum identifizierbar - eine Vielzahl von Schnittstellen erschwert das Ganze noch erheblich. Im Zuge der Evaluierung wird ein Modell erstellt: In der Mitte ist der Sicherheitskern (sicherheitsspezifische Funktionen), umgeben von den ergänzenden Diensten (sicherheitsrelevante Funktionen), die den Kern (=sicher) von

---

[20] vgl. Kuppinger (1998), S. 122f
[21] Eine Lücke in der Systemsicherheit eines Microsoft-Produkts stellt mittlerweile ein globales Problem dar!
[22] vgl. Kersten (1995), S. 181ff
[23] Das Produkt erfüllt die geforderten Produkteigenschaften.
[24] Version des Produkts

der restlichen Welt (=unsicher) abgrenzen. Damit muß nur der Kern evaluiert werden, die ergänzenden Dienste nehmen die Korrektheits- und Authentizitätsprüfung vor. Abschließend muß noch die Wirksamkeit der Abgrenzung zum Rest der Welt analysiert werden. Grundsätzlich gilt: Je kleiner der Sicherheitskern und der ihn umgebende Graubereich sind, desto leichter und schneller ist eine Prüfung des Produktes möglich. Bei neu zu entwickelnden Produkten kann die Spezifikation bereits auf diese Merkmale ausgelegt werden - bei bereits existierenden Produkten, bei deren Design seinerzeit Sicherheitsfragen kaum eine Rolle gespielt haben (weil sie z.B. für den Stand-alone-Bereich entwickelt wurden), wird es allerdings problematisch.

Die Evaluierungszeiten sind von der Art und Komplexität, der Qualität der Abgrenzung und von der angestrebten Sicherheitsstufe des Produktes abhängig. Manchmal ist die Lebenszeit eines Produktes kürzer als der Evaluierungsvorgang, weshalb es sowohl aus Zeit- als auch aus Kostengründen Sinn macht, die Evaluierung bereits in der Entwicklungsphase einzuleiten. Ein sauberes Design und eine vernünftige Implementierung mit entsprechender Qualitätssicherung nehmen natürlich viel Zeit in Anspruch - die schnellen Release-Wechsel im PC-Bereich im Gegensatz zu Großrechnersystemen lassen durchaus berechtigte Rückschlüsse auf das Qualitätsniveau zu.

2.5 Sicherheit in Netzwerken

Die Entwicklung dezentraler Datenverarbeitung und der zunehmende Einsatz von Mehrbenutzersystemen veränderte die vormals relativ einfache Einzelplatz-Situation. Nun ist es grundsätzlich möglich, sogar während des Betriebs Zugang zu Daten fremder Personen zu erhalten, ohne daß diese es überhaupt bemerken können. Zu den Grundforderungen von Einzelplatzsystemen kommen bei Netzwerken noch weitergehendere Forderungen bezüglich der Sicherheit hinzu, sie müssen also dahingehend entwickelt werden, um den Benutzern einerseits eine sichere Datenübertragung als auch eine sichere Datenlagerung zu gewährleisten. Der Trend geht durch die sich abzeichnende Dezentralisierung der IV-Welt weg von Großrechnern hin zu lokalen Netzwerken[25]. Deren Komplexität hat stark zugenommen, war anfangs lediglich eine gemeinsame Datenverwaltung angestrebt, so wurde diese im Lauf der Zeit angereichert durch bis ins Detail ausgefeilte Druckerdienste, Analysewerkzeuge, komfortable Administrationsmöglichkeiten, Überwachungseinrichtungen und schließlich umfassende Sicherheitsdienste. Die Kosten der Netzwerkverwaltung sind daher an und für sich schon hoch genug, für griffige und wirksame Datenschutzmaßnahmen reichen sie leider allzu oft nicht mehr. Wenn man diesem durchaus berechtigten Eindruck, daß Sicherheit viel Geld kostet, die Kosten, die beim Ausfall eines zentralen Rechners oder sogar des ganzen Netzwerks entstehen, gegenüberstellt, relativiert sich diese anfängliche Sichtweise zugunsten von Sicherheitsvorkehrungen. Hardware-

[25] Dieser Vorgang wird als "Downsizing" bezeichnet.

Sicherheitsmechanismen[26] können z.B. durch Spiegelung von Plattenbereichen, Einrichtung kompletter Spiegelplatten oder Verdopplung des kompletten Plattensubsystems erreicht werden. Durch die Verdopplung des ganzen Servers kann eine maximale Steigerung der Sicherheit erreicht werden.
Will man einen Teil des Netzwerks nicht allen Netzwerkteilnehmern zur Verfügung stellen, so müssen Zugriffsschutzmechanismen eingeführt werden, diese Mechanismen wurden bereits im Kapitel 2.2 vorgestellt. Man kann aber auch nicht nur nach Teilnehmern, sondern auch nach den zur Verfügung zu stellenden Diensten selektieren. Dazu braucht man kontrollierende Übertragungsschnittstellen zwischen zwei Netzwerkbereichen (LAN / LAN, LAN / WAN, etc.), die diese entsprechenden Dienste (u.U. in Abhängigkeit vom Teilnehmer) zulassen, kontrollieren oder verhindern. Zugriffskontrollierende Schnittstellen, die diese Funktionen realisieren können, nennt man Firewalls, Übertragungsschnittstellen ohne aufwendige Filterfunktionen nennt man Router.

2.6 Router

Router haben die Aufgabe, anhand der IP-Adressen von Quell- und Zielrechner und unter Zuhilfenahme von Routingtabellen Pakete gezielt in andere Netze weiterzuleiten. Neben dem eigentlichen Routing[27] kann zusätzlich schon eine selektive Kontrolle durchgeführt werden. Die Header der einzelnen Pakete werden gelesen, je nach Quell- und Zieladresse sowie nach Zielport wird entschieden, welche Pakete geroutet und welche Pakete verworfen werden, um Wege durch die verbundenen Netze zu schalten. Router arbeiten auf den unteren drei Schichten des ISO / OSI-Referenzmodells[28], den Netzwerkschichten. Durch sie wird die Gesamtzuverlässigkeit der Systemumgebung erhöht, weil sie adaptive Routing-Algorithmen, intensive Filter und einige zusätzliche Sicherheitsmerkmale besitzen[29]. Durch ihre hohe Speicherfähigkeit werden Router fast völlig zeitentkoppelt, damit können LANs unkritisch miteinander verbunden werden, auch wenn unterschiedliche Transmissionsmedien[30] und Netzwerkprotokolle[31] verwendet werden, nachteilig ist, daß Router globalen Namens- und Adressierungskonventionen unterliegen. Der Trend geht bei den Netzwerkprotokollen hin zu TCP / IP[32], dem Internet-Standardprotokoll, was bei Routern eine Vereinheitlichung der Struktur und damit eine Vereinfachung der Administration bedeutet.

---

[26] s. Kauffels (1994), S. 520ff
[27] s. Cheswick / Bellovin (1996), S. 27ff
[28] s. Anhang
[29] vgl. Kauffels (1994), S. 482ff
[30] z.B. Ethernet - ISDN
[31] das wird durch sog. Gateways erreicht, zur Funktion von Gateways siehe Haun / Georgiadis (1992), S. 132
[32] s. Anhang

2.7 Firewalls

Firewalls[33] ("Brandschutzmauern") dienen zur Abschottung eines Netzwerks nach außen[34]. Durch die Installation einer Firewall werden die sensiblen Bereiche eingeengt und auf einen (oder wenige) Rechner konzentriert. Der gesamte Datenverkehr und damit auch alle Angriffe, werden durch ein einziges Tor geleitet. Dieser Rechner bildet dann eine Hürde oder Mauer gegen Eindringversuche. Eine solche Firewall, stellt nach außen nur eine kleine Anzahl gut gesicherter Dienste zur Verfügung. Jede Kommunikation zwischen innen und außen wird überwacht. Der Systemverwalter kann seine Aufmerksamkeit auf diesen Rechner konzentrieren, nur er darf einen Account auf dem Firewall-Rechner haben. Die Kommunikation der Rechner im LAN untereinander wird durch die Sicherheitsmechanismen jedoch nicht beeinträchtigt. Verstärkt findet der innerbetriebliche Einsatz zur Absicherung bestimmter Netzteile eines Unternehmens Einzug, damit kann von "normalen", allgemein zugänglichen Netzbereichen, nicht auf vertrauliche Daten der Unternehmensleitung zugegriffen werden kann, obwohl sich beide im gleichen Gebäude befinden und auch Clients aus beiden Seiten der Firewall auf gleiche Dienste, wie z.B. das Intranet, zugreifen können[35]. Firewalls bieten derzeit die beste Methode, ein Netz und die daran angeschlossenen Rechner vor Angriffen von außen zu sichern, eine Firewall beschränkt den Verkehr zwischen zwei Netzen auf die vordefinierten erlaubten Aktionen. Grundsätzlich gilt: Was nicht erlaubt ist, ist verboten. Böse Zungen behaupten, die einzig sichere Firewall sei ein Luftspalt zwischen zwei Kabelenden - bei manchen Installationen nicht ohne Grund.

Firewalls setzen sich aus verschiedenen Komponenten zusammen[36]. Ein oder mehrere Paketfilter überprüfen den Datenverkehr durch Access-Listen auf erlaubte Transaktionen. Alle Transaktionen, die nicht durch Access-Listen ausreichend geschützt werden können, werden über Transportschicht-Filter oder Applikationsfilter angeboten. Im folgenden wird auf die möglichen Komponenten einer Firewall eingegangen, wobei gezeigt werden soll, daß Sicherheit durchaus auch mit geringen finanziellen Mitteln machbar ist.

2.7.1 Paketfilter

Paketfilter[37] können Datenpakete nach Kriterien wie Sende- und Empfangsadresse, Protokolle, Ports und benutzerdefinierten Bitmasken filtern. Diese Filterung wird auf den Schichten 2 und 3 des ISO/OSI-Referenzmodells durchgeführt. Bei komplexen Netzwerken wird diese Filterung allerdings schnell unübersichtlich und fehlerhaft, weshalb Paketfilter meist nur als Vorfilter für weitere Firewall-

---

[33] s. Cheswick/Bellovin (1996), S. 61ff und news:comp.security.firewalls
[34] umfangreiches Konzept siehe BSI (1997), http://www.bsi.bund.de/gshb/deutsch/b/73.htm
[35] s. Kapitel 3.4
[36] vgl. Chapman/Zwicky (1996), S. 65ff
[37] s. Cheswick/Bellovin (1996), S. 64ff

Komponenten eingesetzt werden[38]. Der Paketfilter bietet nur eine geringe Sicherheit und kann wegen dem Fehlen eines zentralen Audits der Netzaktivitäten nicht als Firewall bezeichnet werden.

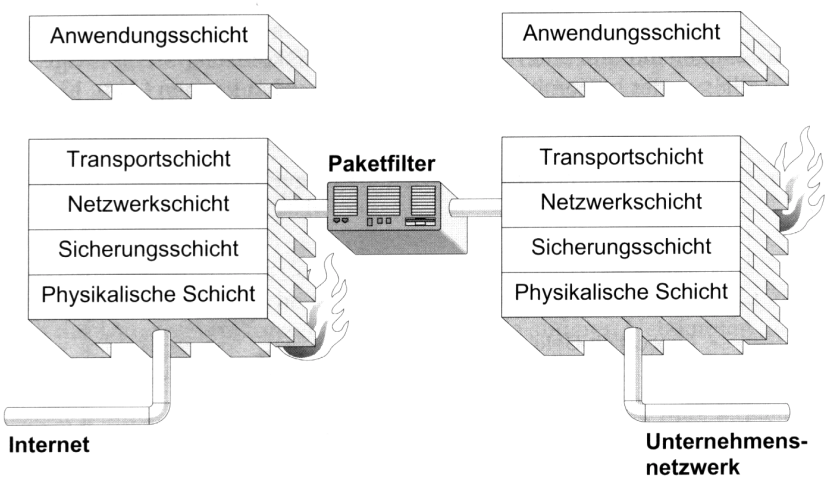

Abbildung 3: Paketfilter[39]

2.7.2 Transportschicht-Filter

Mit Transportschicht-Filtern[40], auch Circuit Relays genannt, kann die Netzwerksicherheit deutlich erhöht werden. Sie ermöglichen den Betrieb von Applikationen, die auf den Kommunikationsprotokollen wie z.B. TCP aufsetzen, ohne eine durchgehende Kommunikationsverbindung auf Netzwerkebene zuzulassen[41]. Die Client-Applikationen müssen allerdings angepaßt werden, um mit dem Circuit Relay zusammenarbeiten zu können.

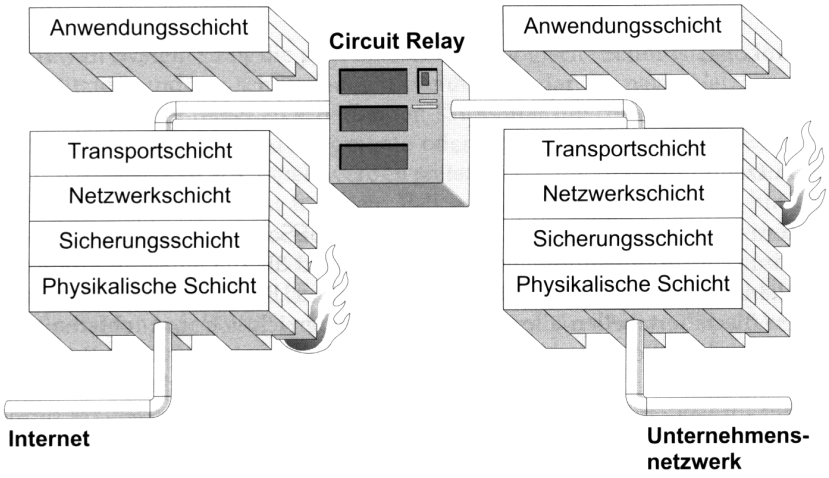

Abbildung 4: Transportschicht-Filter oder Circuit Relay[42]

---

[38] s. Abbildung 3
[39] aus Kyas (1998), S. 248
[40] vgl. Cheswick / Bellovin (1996), S. 91ff
[41] s. Abbildung 4
[42] aus Kyas (1998), S. 248

2.7.3 Applikationsfilter

Application Relays oder Applikationsfilter[43] funktionieren wie Circuit Relays, allerdings mit der Besonderheit, daß sie sich genauso verhalten wie ein Server des jeweiligen Dienstes. Es ist also keine Modifikation der Client-Systeme notwendig, weil aus ihrer Sicht kein Unterschied zur Kommunikation ohne Applikationsfilter besteht[44]. Da in einem Applikationsfilter die Pakete bis auf Anwendungsebene "hinaufgereicht" und erst dort analysiert werden, ist gegenüber einfachem Routing ein ziemlicher Mehraufwand an Rechenleistung zu erbringen, es kann zu Zeitproblemen kommen, falls man keine leistungsstarken Rechner einsetzt. Ein Applikationsfilter bietet gute Sicherheit bei relativ geringen Kosten, empfehlenswert ist eine Kombination mit Paketfiltermechanismen.

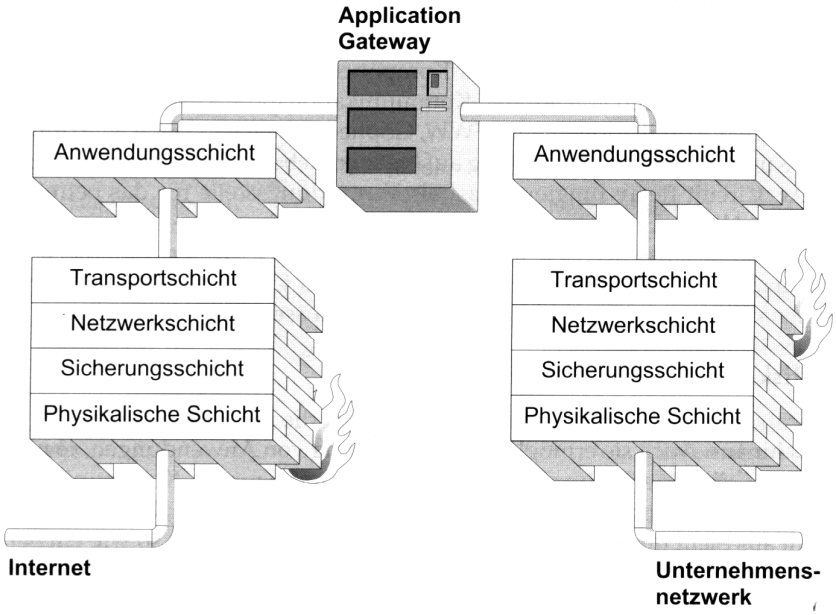

Abbildung 5: Applikationsfilter[45]

2.7.4 Proxy-Systeme[46]

Sowohl Circuit Relays als auch Application Relays werden allgemein als Proxy-Server[47] bezeichnet, ein Proxy hat den Auftrag, stellvertretend für den jeweiligen Client TCP bzw. UDP-Verbindungen auf- bzw. abzubauen. Um Dienste des Internet (Telnet, Mail, FTP, WWW, Gopher etc.) innerhalb des LANs zugänglich zu machen, müssen auf dem Firewall-Rechner sog. Proxy-Server oder Proxy-Gateways eingerichtet werden, die nach dem "store and forward" Prinzip arbeiten: Hereinkommende Daten werden gespeichert, geprüft und, falls die Prüfung positiv ist, weitergeleitet. Klienten im LAN

---

[43] auch Dual Homed Gateway genannt, vgl. Cheswick / Bellovin (1996), S. 89ff
[44] s. Abbildung 5
[45] aus Kyas (1998), S. 250
[46] vgl. Chapman / Zwicky (1996), S. 215ff
[47] vgl. Kuppinger (1998), S. 283ff am Beispiel des Microsoft Proxy-Servers

wenden sich also zunächst an den Proxy-Server, der dann - nachdem Quell- und Zieladresse überprüft wurden - den gewünschten Dienst im Internet startet und umgekehrt die Antworten an den Klienten durchreicht. Ruft ein Benutzer aus dem lokalen Netz die fremden Dienste über den Proxy-Server auf, so identifiziert sich der Kommunikationsrechner (entweder über Auflösung der IP-Adresse oder das Authentifizierungsprotokoll), während die IP-Adressen und symbolischen Namen der Rechner im LAN nach außen hin nicht bekannt gemacht werden müssen.

3. Geeignete Sicherheitskonzepte

Bevor man sich mit der Frage beschäftigt, wie man sich schützt, muß man sich zunächst darüber klar werden, vor was und vor allem vor wem man sich schützen will. Auch wenn die Mitarbeiter keine Zweifel an der Loyalität zum Unternehmen lassen, bleibt ein gewisser Unsicherheitsfaktor, man sollte sich also nicht nur strikt nach außen, sondern unbedingt zuerst nach innen gut absichern. Eine Sicherheitspolitik auf Rechner-Ebene ist kaum durchsetzbar, da eine wirkungsvolle Kontrolle der angeschlossenen Systeme aufgrund der Zahl der installierten Rechner nur schwer durchführt werden kann. Ein Ansatz auf Rechner-Basis kann somit nur zusätzliche Sicherheit erbringen, es besteht also vorrangig die Notwendigkeit einer zentrale Sicherheitsschranke, die für alle Systeme gleichzeitig wirkt. Wenn diese innere Sicherheit gewährleistet ist, müssen die bestehenden Verbindungen zur Außenwelt untersucht werden. Unsichere Verbindungen dürfen gar nicht erst zugelassen werden, eine Systemhomogenisierung muß angestrebt werden. Des weiteren müssen alle Kontakte von und nach außen kontrolliert werden, wobei besonders auf die Modemzugänge geachtet werden sollte. Man sollte bedenken, daß die bisherigen Modemzugänge ohne Filtermechanismen oder Firewall im Vergleich zu einer durchdachten Internet-Anbindung, wie sie heutzutage bei zigtausenden Unternehmen bereits eingerichtet ist, auf jeden Fall weit unsicherer sind und bei einem gezielten Angriff ein hoffnungslos unterlegenes Opfer darstellen. Des weiteren sollten Subsysteme im IV-Bereich selektiv mit Firewalls getrennt werden, um (wenn auch unwahrscheinliche) ungewünschte "Übergriffe" schon im Ansatz zu unterbinden.

Einige einfache Firewalls würden hier genügen, aber schon der Gedanke an verstärkte Sicherheitsmechanismen und eine neue Sicherheitspolitik läßt Rufe nach den hohen Kosten laut werden. Aber zu den gängigen UNIX-Derivaten und der von Administratoren gefürchteten Microsoft-Welt gibt es seit geraumer Zeit eine ernstzunehmende und kostengünstige Alternative. Linux[48] ist eine UNIX-Implementierung, die unter anderem auf INTEL-Prozessoren läuft und als Public Domain gratis erhältlich ist. Von verschiedenen Firmen gibt es CDs, die das gesamte Linux-Paket sowie diverse andere allgemein zugängliche Source Codes enthalten, Linux steht auch in jeder gut sortierten Buchhandlung

[48] Linux wird in vielen Unternehmen erfolgreich eingesetzt.

im Regal. Probleme gibt es aus technischer Hinsicht keine, der Haken ist ein vergleichsweise hoher Administrationsaufwand, man kann dieses Problem aber von zwei Standpunkten sehen. Da der Sourcecode offen liegt und jeder Zugriff darauf haben kann, stellt sich dem Anwender ein völlig offenes System gegenüber, in das er selbst Verbesserungen und Restriktionen implementieren kann und auch darf. Einerseits kann man sicher sein, daß die Anwender in Newsgruppen und auf einschlägigen Homepages[49] Sicherheitslücken und Gefahren hinreichend erörtern und daß dementsprechend schnell auch Lösungsvorschläge und Hotfixes publiziert werden, wie diese Risiken eliminiert werden können. Andererseits fühlen sich vielleicht bösartige Hacker aufgefordert, zu versuchen, mit Hilfe dieser Veröffentlichungen und dem Hintergrundwissen über die Systemstruktur unerlaubt in fremde Systeme zu gelangen. Da Linux als Betriebssystem schon lange über den Experimentierstatus hinaus ist, es von den Beschreibungen her alle Fähigkeiten für die gewünschten Dienste als Router, Firewall und Server mitbringt und ein freies Betriebssystem viele Vorteile hat, von denen Microsoft- und Netware-Kunden nur träumen können, fällt die Wahl nicht schwer.

Nicht verschweigen sollte man aber, daß es unter Umständen bis zur Lauffähigkeit doch viel Zeit und starke Nerven kosten kann, Hilfe bekommt man in den passenden Newsgroups und vom Support der deutschen Firma S.u.S.E.[50], solange man deren Linux-Distribution besitzt.

Da das Linux-Betriebssystem vom Preis-/Leistungsverhältnis her unschlagbar ist, und als Hardware z.B. ein ausgedienter 486er mit 16 MB Arbeitsspeicher völlig ausreicht, könnte ein Linux-PC mit zwei Netzwerkkarten, auf dem IP-Forwarding installiert wurde, als Router dienen:

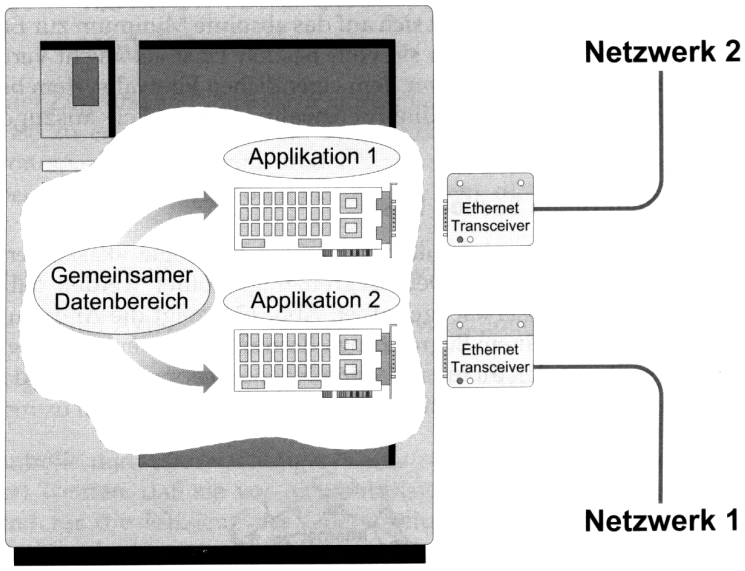

Abbildung 6: Einfacher Router auf PC-Basis[51]

[49] s. http://www.uni-tuebingen.de/zdv/projekte/linux/ und http://www.mnd.fh-wiesbaden.de/~dreymann/linux/
[50] http://www.suse.de/
[51] aus Kyas (1998), S. 253

Da diese "recyclefähige" Hardware im normalen Büroalltag nicht mehr verwendet wird, sollte die Beschaffung kein allzu großes Problem darstellen. Linux beinhaltet bereits im Kernel IP-Filterfunktionen, es stellt also schon von Haus aus einen schnellen und sicheren Filter[52]. Zwischen diesen Router und dem zu sichernden LAN wird ein Firewall-Rechner mit den gleichen Grundanforderungen eingerichtet, auf den z.B. das TIS Firewall-Toolkit[53], das ebenfalls frei zur Verfügung steht, installiert wird. Damit die Firewall ihre Schutzwirkung entfalten kann, muß hier IP-Forwarding/Gatewaying im Kernel ausgeschaltet sein, damit Datenpakete nicht schon auf der IP-Ebene weiterwandern können. Damit müssen alle Datenpakete die Anwendungsschicht passieren, wo die Firewall-Software zur Kontrolle und Überwachung sitzt. Richtig sinnvoll wird ein Firewall natürlich erst, wenn er auf einem Rechner installiert ist, der sonst nichts anderes tut. Ein solcher sog. "Dual Homed Host" ist der einzige aus dem externen Netz erreichbare Rechner. Diese Konfiguration stellt eine den wichtigsten Sicherheitsaufgaben genügende Firewall, die sowohl Filtering beherrscht, als auch über Proxies für die wichtigsten Protokolle verfügt, dar.

Die folgende Abbildung zeigt, wie die physikalische Aufteilung des Gesamtnetzes in einzelne, untereinander abgesicherte LANs, erfolgen könnte:

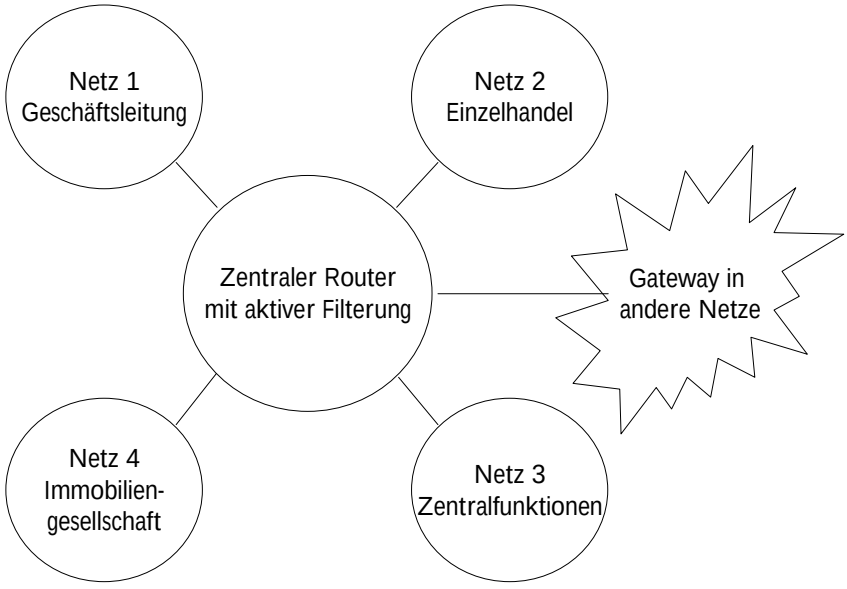

Abbildung 7: Physikalische Trennung der Geschäftszweige

Die Geschäftsleitung könnte in diesem Fall auf alle anderen Netze und die dort abgelegten Daten uneingeschränkt zugreifen, wobei Nutzer der anderen Netze wegen den Filterfunktionen des zentralen Routers z.B. nicht in das Netz der Geschäftsleitung eindringen können. Diese Trennung erlaubt eine sehr hohe Flexibilität bei der Administration der Zugangsberechtigungen ohne Schlupflöcher, da es

[52] vgl. Reiser (1998), S. 72ff
[53] http://www.tis.com/ und Chapman/Zwicky (1996), S. 516

keine Verbindungsredundanzen[54] gibt. Bei Ausfall einer Leitung ist aber das ganze Teilnetz vom übrigen Netz abgetrennt. Ein Notfallplan ist hier eine wichtige Grundlage vor (!) der Realisierung einer solchen Netzarchitektur, um im Ernstfall geordnet vorgehen und das Problem möglichst rasch beseitigen zu können.

Eine professionelle Firewall bedarf einer sehr aufwendigen Administration, die Filter müssen ständig überwacht und ggfs. geändert werden. Das o.g. Verfahren ist zwar prinzipiell für eine anspruchsvolle Firewall geeignet, die Freeware- bzw. Public Domain-Produkte ermöglichen aber meist nur eine recht schwierige und unkomfortable Konfiguration, da sie i.d.R. nicht über eine grafische Oberfläche verfügen. Dennoch ist es eine sinnvolle und äußerst flexible Alternative zu den vergleichsweise teuren Standardlösungen.

3.1 Chancen und Risiken einer Internet-Anbindung

Eine Internet-Anbindung[55] bedeutet in der zunehmenden Globalisierung den Gang der Technik, man bedient sich gerne der Vorteile der (fast) kostenlosen Dienste und Möglichkeiten, die dadurch in das Unternehmen geholt werden können. Die einzigen entstehenden Kosten werden vom Provider erhoben, der (meist unter Zuhilfenahme einer Telefongesellschaft) die Verbindung ins Internet einrichtet und i.d.R. eine Gebühr in Abhängigkeit vom Datenaufkommen verlangt. Bei Emails bleibt die Datenmenge im erträglichen Rahmen, wenn aber auch WWW- oder ftp-Dienste ermöglicht werden, wird sie sicher signifikant steigen, nebenbei steigen auch die Risiken eines unerwünschten Eindringens, auch weil zusätzliche Schnittstellen in das öffentliche Netz geöffnet werden müssen, diese Risiken gilt es zu minimieren.

Unternehmensinterne Netze wachsen in der Zukunft mit öffentlichen Netzen und Netzwerken privater Betreibergesellschaften sowie weltweiten Datenhighways zusammen. Diese Netzwerke werden von mehreren Betreibern verwaltet und sind über technische Schnittstellen miteinander verbunden. Dies wirft die Frage nach der Gesamtverantwortung für ein Netzwerk diesen Ausmaßes auf, wer stellt den reibungslosen Betrieb sicher und wer schützt die Nutzer? Wie bereits erwähnt, bilden hier Firewalls die Grundlage einer Anbindung eines Unternehmensnetzes an das Internet, um unerwünschte Dienste und Anwendungen grundsätzlich sperren zu können. Das Ziel einer Internet-Anbindung ist also nicht das Abblocken vom Netz, sondern die Nutzung der Internet-Dienste und der Wunsch, selbst solche Dienste anzubieten. Dadurch werden aber Möglichkeiten der Umgehung von Sicherheitsmechanismen Tür und Tor geöffnet, es können sowohl Viren[56] als auch unerwünschte Programme[57] "eingeschleppt" werden. Viren kann allerdings mit einem permanenten und nicht abschaltbaren

---

[54] doppelte Verbindungen
[55] Konfigurationsbeispiele in Reiser (1998), S. 92ff
[56] s. kurze Erläuterung in Reiser (1998), S. 65ff
[57] Hacker- und Systemtools

Virenscanner auf jedem Client und auf allen Servern ein Riegel vorgeschoben werden, wobei die Aktualität der Viren-Identifikationsdaten unbedingt gewährleistet sein muß. Zu bemerken hierbei ist aber, daß das Virenproblem schon mit jeglicher Netzanbindung oder mit einem Diskettenlaufwerk beginnt, also bereits bei der bestehenden Systemlandschaft akut ist.

Um Unbefugten den Zugang zu verwehren und Mißbrauch möglichst ausschließen zu können, sollten sichere Authentifizierungsverfahren eingesetzt werden. Die Fernwartungsdienste sollten in Zukunft am besten selbst durchgeführt werden, und zwar auf allen Systemen, um die volle Kontrolle über das Netz zu haben und in kritischen Situationen nicht auf fremde Hilfe angewiesen zu sein. Der Support des Systems könnte über einen ftp-Upload des Herstellers erfolgen, das Patch wird dann (nach reiflicher Überlegung) selbst installiert (oder auch nicht). Damit wird dem Administrator wieder mehr Verantwortung zukommen, Absprachen und Terminverhandlungen für Systemwartungen gehören der Vergangenheit an, Sicherheitslücken werden geschlossen. Hier ein Beispiel, wie eine solche Lösung implementiert werden könnte:

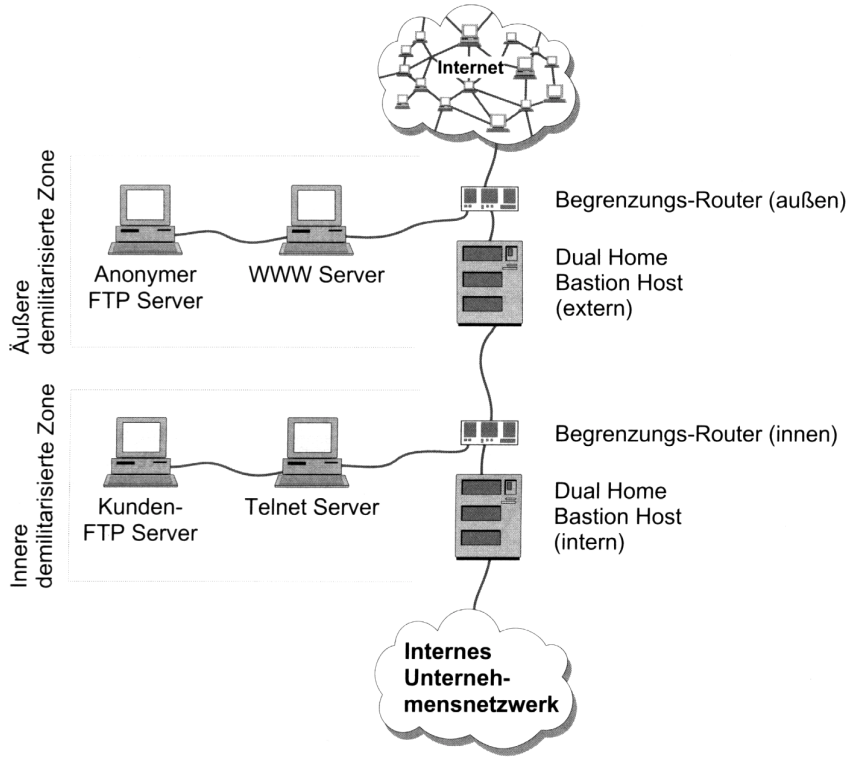

Abbildung 8: Kaskadierte Dual Home Bastion Hosts[58]

Dual Home Bastion[59] Hosts sind physikalisch zwischen dem gesicherten und dem nicht vertrauenswürdigen Netz plaziert, darauf aufbauende Firewall-Systeme sind in der Lage, das interne und externe Netz miteinander zu koppeln, ohne auf Protokollebene eine Verbindung zuzulassen (außer Bastion

[58] aus Kyas (1998), S. 254

[59] Der Bastion Host ist der einzige nach außen vertretene Rechner des Unternehmens, vgl. Chapman / Zwicky (1996), S. 105ff und Cheswick / Bellovin (1996), S. 61

Hosts mit Paketfilter), was einen wesentlich höheren Schutz bedeutet, als dies mit Begrenzungs-Routern möglich ist. Die Firmen, die eine Fremdwartung vornehmen wollen, rufen vorher an und erhalten ein Einmalpaßwort für den externen Dual Home Bastion Host, um Patches auf den ftp-Server ablegen zu dürfen. Hier ist im Prinzip auch ein Datenaustausch mit Partnerfirmen und den Filialen möglich, die jeweils nur einen bestimmten Pfad freigegeben bekommen, um z.B. die aktuelle Telefon- und Telefaxliste der Mitarbeiter zu bekommen. Wichtig hierbei ist nur, daß nicht vergessen wird, alle anderen unkontrollierten Verbindungen in ungesicherte Netze absolut zu unterbinden, sei es nun die ISDN-Karte in einem Client oder das Modem zur Fernwartung an einem Novell-Server.

3.2 Intranet

Ein Intranet wird oft als Möglichkeit für die Stärkung im Wettbewerb propagiert, weil es Kommunikation und Zusammenarbeit in bisher nicht geahnter Weise garantiert. Es baut auf dem TCP/IP-Protokoll auf, ist durch offene Schnittstellen zwischen Client und Server gekennzeichnet und kann mit jedem Browser bedient werden, was einen geringen Lern- und Einarbeitungsaufwand bedeutet. Zu einem Intranet gehören Email-Dienste, eine zentrale Terminkalenderverwaltung und eine ständig aktualisierte Datenbank mit wichtigen Informationen für alle Mitarbeiter, also eine Art "Schwarzes Brett". Die konventionelle Briefpost kann damit auf ein Minimum reduziert werden.

4. Fazit und Ausblick

Das IV-Budget ist im Verhältnis zur Abhängigkeit des Unternehmens von der elektronischen Datenverarbeitung relativ gering und innerhalb dieses Rahmens bleibt nicht viel Spielraum für die zwingend notwendige und bisher nicht gegebene Sicherheit. Dennoch sind weitere Maßnahmen notwendig, um grundlegende Vorkehrungen treffen zu können, besonders in Hinblick auf die Einwählknoten, die Option der Einrichtung eines Intranets und eine mögliche Internet-Anbindung.

Anhang

Praxisbeispiel zum Thema 'Sicherheit und der menschliche Faktor' von Bernd Hechenleitner[60]

Wie man soziale Interaktionen nutzen kann, um in ein System einzubrechen, soll nun anhand eines Beispieles aus den USA erläutert werden. Das Beispiel ist nicht etwa frei erfunden, sondern der Einbruch wurde mit den beschriebenen Methoden tatsächlich durchgeführt. Der Angriff wurde von der betroffenen Firma geplant und in Auftrag gegeben, um Daten über die Einbruchssicherheit der Firma zu erhalten. Die Angestellten wurden nicht davon unterrichtet, so daß also nur die Geschäftsleitung wußte, daß versucht werden wird, in das Computersystem einzudringen.

Abfolge des Angriffs:

Infosuche im Internet: Die Abfrage verschiedenster Datenbanken lieferte die Namen einiger Angestellter und Führungskräfte.

Recherche im Telefonbuch: Aus dem Telefonbuch ermittelten die Angreifer die Telefonnummer einer den Angreifern nahen Zweigstelle der Firma. Per Anruf erhielten die Angreifer die gebührenfreie Telefonnummer der Firma und eine Kopie des Jahresberichts. Daraus erhielten sie Namen und Positionen vieler Führungskräfte mit Informationen über Projekte, an denen diese gerade arbeiten.

Beschaffung des firmeninternen Telefonverzeichnisses: Das firmeninterne Telefonverzeichnis enthält die Namen zusätzlicher Angestellter und gibt üblicherweise einen guten Überblick über die Firmenstruktur. Um an dieses heranzukommen, waren weitere Schritte nötig.

Herausfinden der firmenüblichen Identifikation: Unter Verwendung der gebührenfreien Telefonnummer der Firma wurde in der Postabteilung angerufen. Der Anrufer gab vor, ein neuer Angestellter zu sein und wollte wissen, welche Informationen man braucht, wenn man ein Paket innerhalb der USA bzw. ins Ausland versendet. Daraus wurde die Information gewonnen, daß es zwei wichtige Identifikationsnummern gibt, Angestelltennummer und Kostenstellennummer.

Herausfinden der Angestellten- und Kostenstellennummer einer Führungskraft: Die Angreifer wählten nun diejenige Führungskraft aus, über die sie am meisten wußten. Via Firmenvermittlung kontaktierten sie dessen Sekretärin und unter der Vorgabe, aus der Public-Relations-Abteilung zu sein, wurden ein paar harmlose Fragen gestellt. Durch diesen Anruf erhielten die Angreifer die Angestelltennummer der Führungskraft. Ein weiterer Anruf im Sekretariat, bei dem der Anrufer vorgab, ein Auditor zu sein, der die korrekte Abrechnung kontrolliere, lieferte die Kostenstellennummer. Mit den ermittelten Identifikationsnummern konnte nun das firmeninterne Telefonverzeichnis einfach in der dafür

---

[60] http: / / www.tks.fh.sbg.ac.at / kry / bhechenl / humanfac.htm /

zuständigen Abteilung bestellt werden, indem sich der Anrufer als die vorher erwähnte Führungskraft ausgab und veranlaßte, daß ein firmeninternes Telefonverzeichnis per Expreß an einen „Geschäftspartner“ geschickt wurde. Es braucht wohl nicht näher erwähnt werden, wer dieser „Geschäftspartner“ war.

Ausfragen von Angestellten: Unter Verwendung des firmeninternen Telefonbuches wurden nun Dutzende von Angestellten angerufen, um deren Angestelltennummern zu erhalten, die man für zusätzliche Angriffe nutzen könnte. Der Anrufer gab dabei immer an, von der Personalabteilung zu sein und versehentlich den falschen Angestellten angerufen zu haben. Dieser sollte nun seine Angestelltennummer nennen, um die Verwirrung aufzuklären.

Herausfinden von Namen neuer Angestellter: Neue Angestellte sind am leichtesten manipulierbar, da sie mit der Firmenstruktur und der Kompetenzverteilung noch nicht so vertraut sind. Die Angreifer beschlossen, in der Personalabteilung anzurufen und vorzugeben, für die Geschäftsführung zu arbeiten, welche die neuen Angestellten persönlich begrüßen wolle. Sie würden behaupten, die Geschäftsführung sei schon etwas ungehalten, da die nötigen Informationen schon längst überfällig seien. Der Anruf in der Personalabteilung wurde von einem Anrufbeantworter entgegengenommen. Dieser lieferte neben der Information, daß die Abteilung umgezogen ist, die neue Telefonnummer sowie den Namen des Verantwortlichen. Der Name war sehr wichtig, denn dieser konnte die Glaubwürdigkeit eines Anrufes untermauern. Der nachfolgende Anruf ergab, daß der Verantwortliche das Büro bereits verlassen hatte. Dies war vorteilhaft, denn nun konnten die Angreifer behaupten, daß dieser üblicherweise die erforderlichen Informationen über die neuen Angestellten lieferte. Mit entsprechendem Nachdruck veranlaßten die den Gesprächspartner, die Namen und Abteilungen aller Angestellten zu nennen, die in dieser Woche eingestellt wurden.

Paßwortermittlung der neuen Angestellten: Unter der Vorgabe, Systembeauftragter zu sein, wurden die neuen Angestellten angerufen, um weitere Informationen einzuholen. Die Angestellten wurden aufgefordert, das verwendete Computersystem, installierte Software sowie die ihnen zugewiesenen Computeridentifikationen und ihre Paßwörter zu nennen.

Eine kleine Kuriosität am Rande: in einem Fall riet der Angreifer einem Angestellten, sein Paßwort zu ändern, da es sehr leicht zu erraten sei.

Herausfinden der Einwählnummer: Ein Anruf in der Computer-Support-Hotline der Firma lieferte die Telefonnummer eines Einwählmodems.

Einbruch: Nun waren die Angreifer in der Lage, ungehindert und unentdeckt einzubrechen und die ihnen bekannten user accounts auszuschöpfen.

Das ISO/OSI-Schichtenmodell[61]

7. Anwendungsschicht	besteht aus Anwendungen, mit denen man das Netz nutzen kann
6. Darstellungsschicht	standardisiert das Format der Darstellung von Daten im Netz
5. Kommunikations-steuerungsschicht	Verwaltet die Verbindungen zwischen den Anwendern: Setzen von Checkpoints, Aktionsmanagement
4. Transportschicht	garantiert die fehlerfreie Datenübertragung durch Fehlererkennung und -korrektur (Ende-zu-Ende Integrität)
3. Netzwerkschicht	verwaltet die Verbindungen und Routerinformationen zwischen den Rechnern im Netz für die höheren Verbindungen
2. Datensicherungs-schicht	transportiert Informationen in Bitgruppen und sorgt für die zuverlässige Übertragung der Daten über die physikalischen Verbindungen
1. Bitübertragungs-schicht	transportiert Bitströme über physikalische Medien und definiert die physikalischen Eigenschaften der Übertragungswege

Dieses Basisreferenzmodell der International Standardisation Organisation (ISO) teilt die Aufgaben einer Netzwerkverbindung von der sendenden Datenquelle bis zur empfangenden Datensenke im Dienste einer einheitlichen, offenen Kommunikation in transparente und leichter realisierbare Teilaufgaben. In diesem architektonischen Ansatz übernimmt jede der sieben Schichten ganz spezielle Aufgabengebiete und verwendet zu deren Erfüllung die darunterliegende Schicht (Ebene) als Transportmedium. Die einzelnen Schichten werden von der Datenquelle aus von Schicht 7 bis 1 absteigend und bei der Datensenke in umgekehrter Reihenfolge aufsteigend durchlaufen, wobei eine Schicht durchaus mehrere Protokolle enthalten kann. Bei der sendenden Stelle werden die Daten bei der Passage der einzelnen Schichten mit einer besonderen Kennung, dem sog. Header, ausgestattet und bis zur Schicht 1 weitergereicht. Bei der empfangenden Station werden die Daten von jeder Schicht auf den spezifischen Header untersucht, dabei werden entsprechende Kennungen entnommen. Nach der Entnahme aller Kennungen reduziert sich das Datenpaket wieder auf die reinen Informationen.

[61] s. Siyan / Hare (1995), S. 175ff, Haun / Georgiadis (1992), S. 362ff und Chapman / Zwicky (1996), S. 527ff

Protokollarchitektur von TCP/IP[62]

4. Anwendungsschicht	enthält Anwendungen und Prozesse, die aufs Netz zugreifen	SMTP, Telnet, FTP, etc.
3. Rechner-zu-Rechner-Transportschicht	stellt Ende-zu-Ende-Datendienste zur Verfügung	TCP, UDP, ICMP
2. Internet-Schicht	definiert den Aufbau von Datagrammen[63] und routet Daten	IP
1. Netzzugangsschicht	enthält Routinen für den Zugriff auf physikalische Netze	Ethernet, FDDI, ATM, etc.

TCP/IP besteht aus weniger Schichten, als das OSI-Schichtenmodell beinhaltet, die Verarbeitung der Daten erfolgt aber identisch. Jede Schicht behält ihre eigene Datenstruktur und ihre eigene Terminologie zur Beschreibung dieser Struktur.

[62] aus Chapman/Zwicky (1996), S. 530ff, Funktionsbeschreibung der einzelnen Schichten ab S. 532
[63] kleinste Übertragungseinheit im Internet

Literaturverzeichnis

Bundesamt für Sicherheit in der Informationstechnik (BSI) (1997), IT-Grundschutzhandbuch, http://www.bsi.bund.de/gshb/deutsch/menue.htm, Stand 15. Mai 1998

Chapman, D.B., Zwicky, E.D. (1996), Einrichten von Internet-Firewalls (deutsche Übersetzung von K. Karsunke und T. Merz), Bonn, 1996

Cheswick, W.R., Bellovin, S.M. (1996), Firewalls und Sicherheit im Internet (deutsche Übersetzung von T. Maus), 1996

Haun, M., Georgiadis, K., How to Network, Vaterstetten 1992

Hechenleitner, B. (1997), Sicherheit und der menschliche Faktor, http://www.tks.fh.sbg.ac.at/kry/bhechenl/humanfac.htm, Download 15. Mai 1998

Heuser, A. (1996), Kryptographie: der Schlüssel zu mehr Datensicherheit in der Informationstechnik, in: HMD, Heft 190/1996, S. 8-14

Kauffels, F.-J. (1994), Lokale Netze: Grundlagen, Standards, Perspektiven, Haar 1994

Kersten, H. (1995), Sicherheit in der Informationstechnik, 2. Auflage, München 1995

Kreutz, D. (1995), Grundbegriffe der Computersicherheit i.R. des Seminars zur Sicherheit von Informationssystemen am Institut Informatik III in Bonn, http://www.titan.informatik.uni-bonn.de/~kreutz/html/deutsch/inhaltsverzeichnis.html, Download 15. Mai 1998

Kuppinger, M. (1998), Internet- und Intranet-Sicherheit, Unterschleißheim 1998

Kyas, O. (1998), Sicherheit im Internet, 2. Auflage, Bonn 1998

Reiser, C. (1998), Internet - die Sicherheitsfragen, Wien 1998

Siyan, K., Hare, C. (1995), Internet Firewalls und Netzwerksicherheit (deutsche Übersetzung von H. Hajer und R. Kolbeck), München 1995

Stallings, W. (1995), Sicherheit in Netzwerk und Internet, Haar 1995

Newsgroups zu den behandelten Themen:

alt.security
alt.security.index
alt.security.pgp
comp.protocols.kerberos
comp.security.pgp.discuss
comp.security.firewalls
de.comp.security